UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSTGRADO


# MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE A LA OPERACIÓN DE LOS PROCESOS DE GESTIÓN COMERCIAL DE LAS EMPRESAS DEL SECTOR DE SANEAMIENTO DEL NORTE DEL PERÚ

Autores:
Ing. Lissette Angélica Moscoso Anaya
Ing. Edgard Esaú Peña Núñez
Ing. María del Carmen Soto Castrillón

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

Chiclayo, Perú
2018

# MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE A LA OPERACIÓN DE LOS PROCESOS DE GESTIÓN COMERCIAL DE LAS EMPRESAS DEL SECTOR DE SANEAMIENTO DEL NORTE DEL PERÚ

POR

Ing. Lissette Angélica Moscoso Anaya
Ing. Edgard Esaú Peña Núñez
Ing. María del Carmen Soto Castrillón

Tesis presentada a la Escuela de Postgrado de la Universidad Católica Santo Toribio de Mogrovejo, para optar el Grado Académico de **MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN**

APROBADO POR

_____

……..

Presidenta de Jurado

_____

…….

Secretaria de Jurado

_____

…….

Vocal/Asesor de Jurado

CHICLAYO, 2018

# Dedicatoria

A Dios por permitirme llegar hasta aquí. A mi hijo Rómulo, que me motiva a seguir siempre adelante. A mi abuela Victoria, quien llena mi vida de amor. A mi madre Lisbeth ejemplo continuo de lucha y perseverancia en la vida.

María del Carmen

A Dios por permitirme culminar mi maestría exitosamente. A mis padres Hildebrando y María que son mi motivación para ser mejor como persona y profesional cada día. A mis hermanos Omar y Katherine por su constante apoyo.

Edgard Esaú

A Dios ya que gracias a él he logrado concluir mi carrera. A mis padres Edgar y Luz que han sido un pilar fundamental en mi formación como profesional. A mis hermanos Liliana y Edgar, por sus palabras y compañía. A mis sobrinos porque siempre estuvieron a mi lado.

Lissette Angélica

## Epígrafe

"Nunca consideres el estudio como un deber, sino como una oportunidad para penetrar en el maravilloso mundo del saber"

- Albert Einstein.

# Agradecimiento

A nuestra asesora Mtra. María Isabel Arangurí, por su apoyo en el desarrollo de este proyecto, brindándonos sus recomendaciones y experiencia profesional. A los Mtro. Juan Dávila Ramírez, Mtro. Gregorio León Tenorio y Mtro. Ernesto Celi Arévalo, quienes nos apoyaron en la evaluación de nuestro proyecto y lo enriquecieron con sus valiosos aportes.

# ÍNDICE

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

## ÍNDICE DE DIAGRAMAS

# RESUMEN

La presente investigación centra su estudio en la necesidad de incluir la gestión de riesgos de tecnologías de la información (TI) en las empresas del sector de saneamiento del norte del Perú, el diagnóstico fue aplicado la empresa EPSEL S.A., dentro de esta organización se ha tomado como muestra de manera censal los siguientes procesos comerciales: medición, facturación, recaudación, atención al cliente, catastro y conexiones y micro medición y se consideró 03 grupos de estudio: alta dirección, gestión operativa y personal se detectó que estas no implementan gestión de riesgos o no la implementan de una manera efectiva, además se determinó que los conceptos de gestión de riesgos de TI no son conocidos a nivel de la gerencia de TI, condicionando una respuesta reactiva ante situaciones adversas en los servicios importantes soportados por TI, con la posibilidad de generar pérdidas económicas y deterioro de imagen ante la comunidad universitaria.

Se planteó como objetivo general: contribuir a la operación de los procesos de gestión comercial a través del desarrollo de un modelo de gestión de riesgos de TI adecuado a las empresas de saneamiento del norte del Perú. El modelo se validó por juicio de expertos midiendo su confiabilidad aplicando el alfa de Cronbach y la concordancia de su contenido en base a Kendall.

El modelo propuesto, en la presente tesis, se aplicó en la empresa prestadora de servicios de saneamiento de Lambayeque como caso de estudio, identificando 165 riesgos, siendo 52 riesgos categorizados como alta prioridad en base a la valoración del apetito y tolerancia, se plantearon estrategias de tratamiento con 16 proyectos aplicados a monitorear y revisar que la gestión de riesgos logra contribuir a la operación de los procesos de gestión comercial.

PALABRAS CLAVES: Gestión de riesgos, nivel de riesgo, apetito de riesgo, matriz de riesgo, riesgo total

## ABSTRACT

This research focuses its study on the need to include information technology IT risk management in the companies of the sanitation sector of northern Peru, the diagnosis applied to a sample of the company EPSEL S.A, within this organization has been taken as a sample of census the following business processes: measurement, billing, collection, customer service, cadaster and connections and micro measurement and was considered 03 study groups: senior management, operational management and personnel was detected that these are not they implement risk management or do not implement it in an effective manner; furthermore, they determined that IT risk management concepts are not known at the IT management level, conditioning a reactive response to adverse situations in the important services supported by IT, with the possibility of generating economic losses and deterioration of image before the community.

The general objective was to: contribute to the operation of commercial management processes through the development of an IT risk management model suitable for sanitation companies in northern Peru. The model was validated by expert judgment, measuring its reliability by applying Cronbach's alpha and concordance of its content based on Kendall.

The proposed model, in this thesis, was applied in the company providing sanitation services Lambayeque as a case study, identifying 165 risks, with 52 risks categorized as high priority based on the assessment of appetite and tolerance, strategies were raised of treatment with 16 projects applied to monitor and review that risk management manages to contribute to the operation of commercial management processes.



KEYWORDS: Risk management, risk level, risk appetite, risk matrix, total risk value.

.

# INTRODUCCIÓN

En el presente trabajo de investigación se desarrolló un modelo de gestión de riesgos aplicado a las empresas de sector saneamiento, ubicadas geográficamente en la región norte del Perú.

Si bien es cierto, se han definido diferentes estándares de gestión de riesgos que han servido de base para la implementación de distintos modelos de trabajo, estos no se han contextualizado para empresas del sector de saneamiento.

Con respecto, a las empresas del sector saneamiento, éstas están estrechamente vinculadas a las tecnologías de información (TI) como herramienta de apoyo y mejora en la gestión de los diferentes procesos que ejecutan; sin embargo, como resultado de la situación problemática analizada en las empresas de este sector, se puede indicar que éstas no han tomado conciencia de la necesidad, de una efectiva gestión de riesgos, no existiendo un proceso definido claramente para este tipo de gestión, que les permita identificar los riesgos a los que pueden estar expuestos sus activos y el impacto que puede causar la materialización de algún riesgo. Además de los costos que implicaría su reposición o reparación de los activos involucrados.

El daño, interrupción, alteración o falla derivada del uso de tecnologías de información, puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo

y estratégico. Según el estudio "Cost of Data Breach"[1]realizado en Junio del 2017 por el Instituto Ponemon (USA), las tres causas principales de violación y pérdida de información son: ataque malicioso o criminal (47%), falla de sistemas (25%) y error humano (28%) y generan un costo promedio de 3,62 millones de dólares a nivel mundial, que en comparación al año 2016 se ha reducido en un 10%, sin embargo estos incidentes de seguridad han supuesto para las empresas un costo promedio de 141 dólares por registro perdido o robado.

Una situación que ejemplifica lo mencionado, en el contexto internacional (El Comercio 2017)[2], ocurrió con el servicio de mensajería instantánea Whatsapp, cuando se presentó un problema de conexión a nivel mundial, dejando incomunicados por aproximadamente dos horas a más de 1.200 millones de usuarios, afectando directamente a la imagen de la empresa y de acuerdo al reporte "Supply Chain Resilience" del Business Continuity Institute, las interrupciones no planificadas tienen como principales consecuencias: el impacto en la productividad (68%) y el incremento del costo laboral(53%)[3].

De forma similar, (La Prensa Gráfica 2018)[4], informa lo ocurrido en el de marcas preferenciales en el proceso electoral de diputados y concejos conteo de votos municipales de El Salvador; la empresa Smartmatic, fue la

[1]Ponemon Institute. 2017. Cost Data Breach Study. https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

[2]El comercio. 2018. Whatsapp sufre una caída mundial basada en un profundo cambio. http://www.elcomercio.es/tecnologia/201705/04/whatsapp-caida-mundial-basada-20170504043123.html

[3]Deloitte. 2018. Lecciones tras la caída de Whatsapp https://www2.deloitte.com/do/es/pages/risk/articles/lecciones-tras-la-caida-de-whatsapp.html

[4]La prensa gráfica. 2018. "Esto es un error de estudiante de primer año de informática": 5 datos claves para entender el "error humano" de Smartmatic en la elecciones 2018. https://www.laprensagrafica.com/techlife/Esto-es-un-error-de-estudiante-de-primer-ano-de-informatica-5-datos-claves-para-entender-el-error-humano-de-Smartmatic-en-las-Elecciones-2018-20180306-0049.html

encargada de procesar y difundir los resultados de este proceso electoral, sin embargo, por un "error humano" como ellos mismos catalogaron, se vio obligada a frenar el proceso de marcas preferenciales y a dar un orden de preferencias muy diferente al que habían revelado en un inicio, impactando directamente en la credibilidad del proceso electoral y además pudiendo acarrear una sanción penal para la empresa implicada.

Nuestro país, no es exento de estas situaciones de interrupción del servicio, (RPP 2014)[5], el Aeropuerto Internacional Jorge Chávez, el 22 de mayo del 2014 sufrió la caída del sistema informático del área de migraciones, generando molestias a pasajeros, quienes formaron largas colas esperando ser atendidos, muchos de ellos corriendo el riesgo de perder sus vuelos. Si consideramos que este aeropuerto administra la llegada y salida de 54 vuelos internacionales, como informa en su página web, el incidente ocurrido generó la insatisfacción de un promedio de 1200 pasajeros de los 8100 que reciben este servicio y según la oficina de asuntos del consumidor de la Casa Blanca[6], cada uno de estos clientes le contará, a un promedio de 9-15 personas sobre su experiencia y alrededor del 13% de los clientes insatisfechos lo comentan a más de 20 personas afectando negativamente a la organización.

De todos los casos antes mencionados y considerando los resultados obtenidos por la encuesta global de seguridad de información 2017 aplicada

[5]RPP Noticias. 2014. Caída del sistema genera aglomeración de pasajeros en el Jorge Chávez. http://rpp.pe/lima/actualidad/caida-de-sistema-genera-aglomeracion-de-pasajeros-en-el-jorge-chavez-noticia-694161

[6]Oficina de asuntos del consumidor de la casa blanca. Capítulo 15. Influencia del consumidor y difusión de las innovaciones. 515. https://books.google.com.pe/books?id=Wqj9hlxqW-IC&pg=PA515&dq=oficina+de+Asuntos+del+Consumidor+de+la+casa+blanca&hl=es-419&sa=X&ved=0ahUKEwi0nsGU--fZAhUN7lMKHXpMBtEQ6AEILTAB#v=onepage&q=oficina%20de%20Asuntos%20del%20Consumidor%20de%20la%20casa%20blanca&f=false

por la firma Ernest & Young (EY)[7], que indica que, 55% a nivel mundial y el 97% en el Perú de los encuestados, no tiene o solo tiene una capacidad informal de identificación de una vulnerabilidad que podrían afectar a sus sistemas de información, grafican la importancia de establecer una cultura a gestión de riesgos de TI y con mayor razón si consideramos que en la región norte del Perú, dentro del sector de saneamiento encontramos empresas que tienen bajo su responsabilidad la gestión de servicios de saneamiento de un promedio de542, 654mil de conexiones domiciliarias.

Bajo el análisis de la situación problemática descrita, se formuló la siguiente interrogante ¿Cómo se puede contribuir a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú?

Para dar respuesta a la interrogante mencionada en el párrafo anterior se planteó la siguiente hipótesis, es posible contribuir a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú, con la implementación del modelo de gestión de riesgos de tecnologías de información.

De la hipótesis se desprende la variable independiente definida como, modelo de gestión de riesgos de tecnologías de información basado en estándares adaptados a las TI que soportan los procesos comerciales. Como variable dependiente se propuso contribuir a la operación de los procesos de gestión comercial en las empresas del sector saneamiento del norte del Perú.

Para demostrar la validez del modelo se determinaron como objetivos establecer los niveles de coincidencia, basado en la evaluación de estándares, modelos y normas de gestión de riesgos de TI, para desarrollar

[7]EY. 2017. El camino hacia la resiliencia cibernética. http://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resiliencia-cibernetica/$FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf

un modelo que permita valorar los activos críticos de tecnología de información que definen los niveles de impacto en la gestión de los procesos comerciales de las empresas de saneamiento y luego identificar la estructura que deberían tener los proyectos requeridos por las necesidades de control de los procesos críticos y finalmente validar el modelo propuesto, en cuanto a la utilidad para contribuir a los procesos de gestión comercial en las empresas de saneamiento.

Los resultados de esta investigación se desarrollaron con la finalidad de promover en las empresas del sector de saneamiento que carecen o manejan de manera incipiente buenas prácticas para la gestión de riesgos de TI, un adecuado soporte en la operación de los procesos de gestión comercial, la implementación de un modelo de gestión de riesgos adaptado a sus necesidades logró gestionar los riesgos inherentes del uso de las tecnologías de información en este tipo de empresa. Si bien hoy en día existen estándares e incluso diferentes metodologías para gestionar riesgos, es importante mencionar, que muchos de estos plantean una vasta variedad de escenarios de los cuales solo una parte se adecuará a este sector, motivo por el cual se consideró importante desarrollar un modelo de gestión de riesgos que adecuado a la realidad de este sector empresarial. Así mismo, gestionar a tiempo los riesgos de TI permitió disminuir las pérdidas económicas generadas por la materialización de riesgos, que puedan conllevar a la paralización de las actividades del negocio e incluso a la pérdida de la información, más aun considerando que este tipo de empresas es supervisada por el estado y cualquier alteración o falla en la información que se remite al ente supervisor conlleva a la aplicación de multas que pueden alcanzar hasta 200 unidades impositivas tributarias (UIT).Finalmente, considerando que las empresas de saneamiento tienen índole social y su misión es contribuir a mejorar la calidad de vida de la población, la implementación de este modelo, apoyó a la operación de los procesos de

gestión comercial, así como a mantener la reputación empresarial y la calidad del servicio prestado a la sociedad.

# CAPÍTULO I: MARCO TEÓRICO CONCEPTUAL

Antecedentes del problema

Para dar un sustento a la propuesta aquí planteada, se ha considerado fundamentar a través de los antecedentes seleccionados como investigaciones previas relacionados con el tema.

NATO Alliance Ground Surveillance Management Agency (2013)[8], el artículo detalla y aporta los pasos para implementar una estándar de gestión de riesgos, en los que considera la configuración y puesta de un comité de implementación, proporcionar conocimientos, soporte técnico, gestionar así como organizar sistemas y procesos. Desarrollar un marco de gestión de trabajo, publicar y anunciar, aprobar la gestión e implementar un proceso de gestión de riesgos. Así mismo identifica los pros y contras de implementar un proceso de gestión de riesgos.

Según Vanegas y Pardo (2014)[9],presenta la armonización de modelos de riesgos de TI MOGRIT (CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE) y algunas estándares enfocados en brindar soporte a los riesgos (ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006, y

[8]NATO Alliance Ground Surveillance Management Agency (NAGSMA). 2013. Bélgica. Implementando un estándar de gestión de riesgos.
[9]Vanegas G, 2014, "Hacia un modelo para la gestión de riesgos de TI en MiPyMES: MOGRIT"

UNE 71504:2008) y realiza un análisis comparativo, de alto y bajo nivel, que permite conocer las características más comunes y representativas de cada uno de ellos. Con los resultados obtenidos, se establecieron los beneficios, es decirla manera en la que los modelos comparados y su implementación pueden ser armonizados, y de esta manera dar soporte a los procesos de gestión dentro de las actividades de desarrollo de una organización. En este sentido, el artículo provee una perspectiva más clara de las diferencias, similitudes y posibles integraciones entre modelos y estándares de riesgos de TI, para MiPyMEs que desarrollan software. Los investigadores concluyeron que gracias al análisis realizado se pudo evidenciar que la mayoría de estándares y modelos descritos en el artículo están relacionados entre sí, aunque algunos estándares presentan procesos más detallados, con un nivel más profundo que otros modelos. Asimismo, observaron que hay estándares y modelos con similitudes en la definición de sus procesos, tales como actividades similares entre sí. Por otra parte, también encontraron algunas actividades que complementaban y mejoraban las descripciones de otras actividades, dando como resultado la característica en la que un modelo es capaz de soportar a otro modelo. Obtuvieron una metodología, la cual era soportada por las actividades que están descritas en los procesos de gestión de riesgos definidos en normas y estándares certificados, que son avalados por organismos internacionales como la ISO, IEC, ISACA e ICONTEC, entre otros, siendo este el principal aporte al desarrollo del trabajo de investigación propuesto.

Celi, Ernesto (2014)[10], en su artículo de investigación denominado "Un modelo para la gestión de TI en las empresas microfinancieras: caso Lambayeque, Perú", propone un modelo de gestión de riesgos de TI, que

[10]Celi E., 2014, Lambayeque. "Un modelo para la gestión de TI en las empresas microfinancieras: caso Lambayeque, Perú"

identifica, evalúa y trata los activos de TI, sus amenazas, debilidades y niveles de riesgo relacionadas con las categorías: disponibilidad, integridad y confidencialidad de la información, que exige la Superintendencia de Banca y Seguros (SBS) para este tipo de organizaciones. Permitiendo establecer pautas para evaluar la magnitud de los riesgos y contar con indicadores clave para monitorizar periódicamente las actividades de gestión de riesgos de TI en las entidades financieras tomadas como muestra, mediante la evaluación de brechas de efectividad de los controles de seguridad de la información. El producto tangible del modelo de gestión de riesgos es la matriz de riesgos y a través de ella lograron disponer de un registro permanentemente actualizado de los principales activos de TI a proteger, de modo que se garantice la continuidad operativa vía los planes de mitigación de los riesgos inmersos en cada activo permitiendo una adecuada sinergia con los procedimientos de continuidad del negocio. Concluyeron, que se ha podido demostrar que la metodología de gestión de riesgos de TI que propusieron, permite identificar los niveles de riesgos de tal forma que sirve de información para la toma de decisiones en relación a la inversión, para la implementación de los controles que sirvan de salvaguardas en la protección de su procesos, contra posibles amenazas y vulnerabilidades. Se considerará como aporte al trabajo de investigación la matriz de riesgos obtenida de la implementación de la metodología de gestión de riesgos que se propuso.

Según Molina (2015)[11], en su investigación ha descrito los conceptos relacionados con la gestión de los riesgos de la seguridad de la información, estándares, metodologías y herramientas que proporcionan las guías

[11] Molina, M. 2015. Madrid. Propuesta de un plan de gestión de riesgos de tecnología superior politécnica. http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

necesarias para reducir el nivel de vulnerabilidad que tienen los activos ante una amenaza. Es de vital importancia que una organización, dedicada a brindar servicios tecnológicos y mantener respaldada mucha información confidencial de forma segura, cuente con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, vieron la necesidad de desarrollar un análisis de riesgo tecnológico de orden cualitativo aplicado en el centro que administra y brinda los servicios de red y sistemas de la Escuela Superior Politécnica del Litoral siguiendo la metodología MAGERIT. Primero procedieron a describir la situación actual de la organización, luego a identificar los activos con sus respectivas vulnerabilidades, para proseguir a realizar la medición de riesgos existentes y sugerir las salvaguardas necesarias que podrían formar parte del plan de implantación, que genera aporte a este estudio, por lo que identifica el nivel de riesgo en que se encuentran los activos, mediante el nivel de madurez de la seguridad implementada y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

Murillo y Rivas (2015)[12], realizan una propuesta metodológica para la gestión del riesgo en microempresas comercializadoras de electrodomésticos ubicadas en la ciudad de Bogotá, basándose en el estándar ISO 31000: 2011 y OHSAS18001:2007. Partiendo con el análisis de riesgos y la contextualización del sector. Tras la entrada al país de las grandes superficies, las microempresas se ven obligadas a cambiar sus estrategias que les permita mantenerse vigentes en el mercado, rentables y

[12] Murillo Ch. y S. Rivas, 2015, Colombia. Propuesta metodológica para la gestión del riesgo en microempresas comercializadoras de electrodomésticos basada en los modelos ISO 31000:2011 y OHSAS 18001:2007. https://repositorio.escuelaing.edu.co/bitstream/001/226/1/EC-Especializaci%C3%B3n%20en%20Gestion%20Integrada%20QHSE-1072493699.pdf

competitivas. Se han tomado como referencia diversos casos en los que la implementación de un Sistema Integrado de Gestión, permite a las organizaciones desarrollar sus actividades con una mayor eficiencia y eficacia a partir de la gestión por procesos, donde no sólo se reducen costos y tiempo, sino que además se mejora la efectividad y productividad de la organización, pues permite monitorear los procesos, para determinar si realmente son eficientes o ajustarlos en caso de ser necesario, reduciendo considerablemente el riesgo y el gasto de recursos. Se logró establecer los principales factores de riesgo internos y externos qué afectan el crecimiento, rentabilidad y sostenibilidad de las microempresas mediante el análisis de la severidad de los mismos permite priorizar la implementación de controles para dichos riesgos.

La investigación de Arangurí, Imán y León(2016)[13], propone una alternativa de solución, por lo que define que el modelo aplicado por el estándar de riesgos ISO 31000, las normas ISO/IEC 27000, 27001, 27002, 27003 y 27005 y las metodologías de OCTAVE, MAGERIT permitió gestionar los riesgos de TI asegurando la continuidad de los procesos, sin afectar las operaciones económicas y operativas en las universidades privadas de la región Lambayeque, haciendo los riesgos más visibles, el aporte de esta investigación es la secuencia lógica que proponen como modelo de gestión de riesgos, la cual se usó de referencia para el desarrollo de la presente tesis.

La tesis Chillogallo y Zambrano (2016)[14], propone elaborar y validar un modelo de gestión de riesgos de tecnologías de información para la Fiscalía

[13]Arangurí, M., R. Iman y G. León, 2016, Chiclayo. Modelo de gestión de riesgos de TI basados en estándares adaptados a las TI que soportan los procesos para contribuir a la generación de valor en las universidades privadas de la región Lambayeque.
[14]Chillogallo, E., V. Zambrano, 2016, Quito. Elaboración de un modelo de gestión de riesgos de tecnologías de información para la fiscalía general del estado.

General del Estado (FGE), teniendo en cuenta el análisis de la situacional de la entidad en torno a la gestión de riesgos, comparando modelos y metodologías para el análisis y gestión de riesgos de tecnologías de información para elaborar y aplicar el modelo. Aporta al presente trabajo de investigación con la propuesta metodológica de gestión de riesgos que desarrollaron para la FGE, y en particular para la dirección de TI.

El trabajo de investigación de López (2017)[15], propone desarrollar un modelo de gobierno y gestión de TI para industrias farmacéuticas ecuatorianas, tomando como referencia las mejores prácticas de manufactura y gobierno de TI, que constituye una guía clara para que los procesos relacionados con TI estén controlados y gestionados, a fin de generar valor para la industria sirviendo como aporte para el desarrollo de la presente tesis.

En este apartado se hará referencia de cada uno de los conceptos que han sido aplicados, en el desarrollo de la presente tesis y define el sustento teórico del método.

1.1. Gestión de riesgos de tecnologías de información

a. Gestión de riesgos

COBIT 5 (2012), menciona que "Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y posibilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo o transfiriendo el

[15]Coronel, K., 2017, Ecuador. Modelo de gobierno y gestión de TI para industrias farmacéuticas ecuatorianas, tomando como referencia las mejores prácticas de manufactura y gobierno de TI. Caso de estudio: Laboratorios industriales farmacéuticos ecuatorianos (LIFE)

riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa".

El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales.

El desarrollo y uso de metodologías integradas y ágiles ayudan a minimizar el impacto que puede causar en las dimensiones de la seguridad.

b. Tratamiento de Riesgos

Después que se ha identificado el riesgo, es necesario saber cómo se debe manejar y para ello existen 4 maneras de hacerlo:

- Evitar: Es generalmente conceptual porque implica oportunidades. Esta forma de evitar el riesgo suele ser inviable.
- Transferir: La organización puede transferir la responsabilidad para un evento hacia un tercero.
- Mitigar: Es cuando la organización puede reducir la expectativa de costo de un riesgo, al reducir la posibilidad de que el evento ocurra.
- Aceptar: Si la empresa retiene el riesgo sin establecer un fondo, entonces se dice que la empresa acepta el riesgo.

c. Perfil de riesgo de TI

En la gestión de TI, es necesario tener en cuenta tres aspectos básicos: implantación eficaz de las TI, procesos de gobierno del riesgo y la cultura consciente sobre el riesgo, para lograr la efectiva gestión de los riesgos.

Un perfil de riesgo debe determinar e identificar los siguientes componentes:

- Nivel potencial e inherente de riesgo: Consiste en estimar el nivel de exposición a los riesgos que tiene la empresa.
- Controles provenientes de las TI: La implementación de TI trae consigo una serie de controles relacionados con los activos o con los procesos de TI, que permite mitigar los riesgos, obteniendo un nivel de riesgo.
- Apetito de riesgo[16]: COSO (Committee of Sponsoring Organizations of the Treadway) define el apetito del riesgo como el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad.
- Tolerancia al riesgo[17]: Es la cantidad máxima de un riesgo que una empresa puede aceptar para lograr su objetivo. Es decir es aquel riesgo que tiene que ser capaz de soportar.
- Capacidad de riesgo[18]: Es la cantidad y tipo de riesgo máximo que una organización es capaz de soportar en la persecución de sus objetivos sin afectar su existencia.

## 1.2. Estándares

### a. ISO 31000

[16]Instituto de Auditores Internos. 2013. España. Definición e implantación de apetito de riesgo. 15-16. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

[17]Instituto de Auditores Internos. 2013. España. Definición e implantación de apetito de riesgo. 16. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

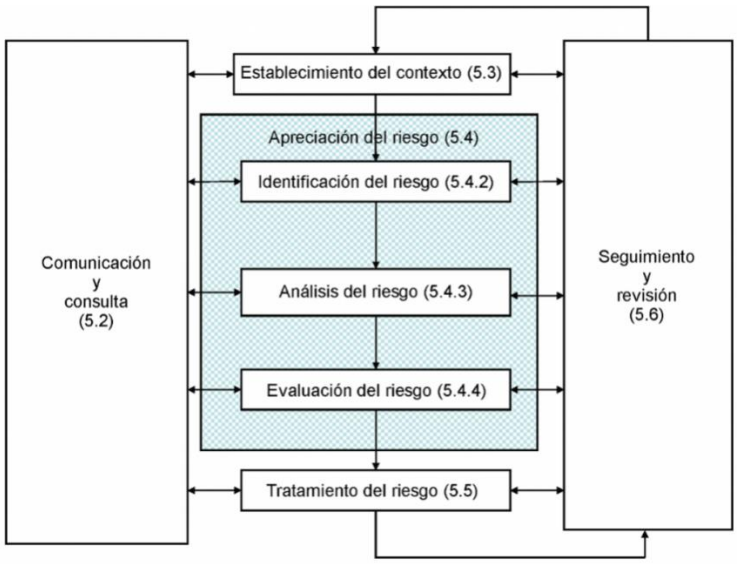
[18]Instituto de Auditores Internos. 2013. España. Definición e implantación de apetito de riesgo. 16. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

Esta norma internacional, describe este proceso sistemático y lógico en detalle, comunica y consulta a las partes interesadas, supervisa y examina el riesgo y de los controles que están modificando el riesgo con el fin de garantizar que no se requiere el tratamiento del riesgo.

Las prácticas de gestión y los procesos de muchas organizaciones incluyen los componentes de riesgo de gestión, y muchas organizaciones ya han adoptado un proceso formal de gestión de riesgo para particulares tipos de riesgo o circunstancias. En tales casos, una organización puede decidir llevar a cabo una revisión crítica de sus prácticas y procesos existentes a la luz de esta norma internacional.

El proceso de gestión de riesgos se muestra en la figura 1:

Figura 1: Proceso de gestión del riesgo - ISO 31000




Fuente: ISO 31000:2009

Establecer el contexto.

El proceso de gestión de riesgo que se está aplicando, debe ser establecido.

La gestión de riesgo, debe llevarse a cabo con plena consideración de la necesidad de justificar los recursos utilizados en la realización de gestión de riesgos. Los recursos necesarios, las responsabilidades y autoridades, y los registros que deben mantenerse especificados.

Identificación de Riesgos.

El objetivo de este paso, es generar una lista completa de los riesgos basados en los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos. Es importante identificar los riesgos asociados a que no ejercen una oportunidad. La identificación completa es fundamental, porque el riesgo de que no se identifica en esta etapa no sean incluidas en el análisis posterior.

Análisis de Riesgos.

El análisis de riesgos implica el desarrollo de la comprensión de los riesgos. El análisis de riesgos proporciona una entrada a los riesgos, la evaluación y las decisiones sobre si los riesgos necesitan ser tratados y en el tratamiento del riesgo se busca aplicar las estrategias adecuadas como métodos de control. El análisis de riesgos también puede aportar en la toma de decisiones, las elecciones deben ser realizados y las opciones de participación de los diferentes tipos y niveles de riesgo.

Evaluación de Riesgos.

El propósito de la evaluación de riesgos, es ayudar en la toma de decisiones, tomando como base en el análisis de riesgos que necesitan tratamiento y determinado la prioridad para la aplicación del tratamiento.

Evaluación de los riesgos supone la comparación del nivel de riesgo identificado durante el proceso de análisis con criterios de riesgo establecidos cuando se establece el contexto. Basándose en esta comparación se determina la necesidad del tratamiento que puede ser considerado.

Tratamiento del Riesgo.

El tratamiento del riesgo consiste en seleccionar una o más opciones de modificación de los riesgos, y la aplicación de esas opciones.

El tratamiento del riesgo implica un proceso cíclico de:

- Evaluación de un tratamiento del riesgo.
- Decidir si los niveles de riesgo residual son aceptables.
- Si no son aceptables, generar un nuevo tratamiento del riesgo.
- La evaluación de la eficacia de ese tratamiento.

Las opciones de tratamiento de los riesgos no son necesariamente excluyentes o apropiadas en todas las circunstancias.

Las opciones pueden incluir:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.

- Aceptar o aumentar el riesgo con el fin de perseguir una oportunidad.
- Transferir el riesgo con la otra parte o partes (incluidos los contratos y la financiación de riesgo).
- Mitigar el riesgo.

b. ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar

que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

Importancia

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales: Cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.
- Obtener una ventaja comercial: Si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
- Menores costos: La filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.
- Una mejor organización: En general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

## 1.3. Metodologías de gestión de riesgos de información

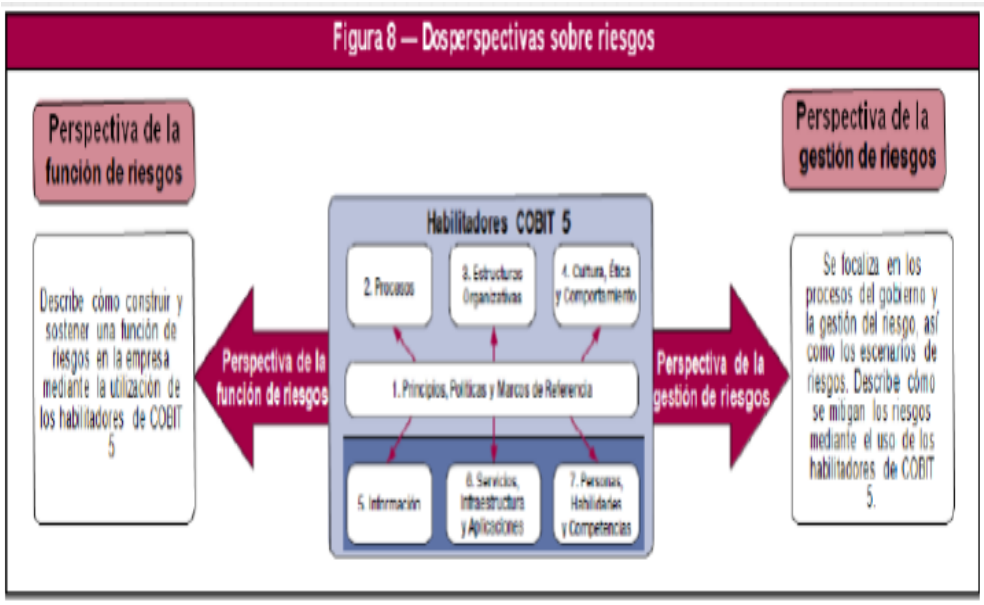
COBIT 5

COBIT 5 en un contexto de riesgo presenta dos perspectivas:

- ✓ Función de riesgo y
- ✓ Gestión de riesgos.

Gineo Pablo (2015), la perspectiva de función de riesgo se centra en lo que se necesita para construir y mantener la función de riesgo en la empresa, mientras la perspectiva de la gestión de riesgos se centra en los procesos básicos de gobierno y gestión del riesgo para optimizar el riesgo y en cómo identificar, analizar, responder y reportar sobre el riesgo a diario.

Figura 2: Dos perspectivas sobre riesgos




Fuente: COBIT 5

Procesos principales de la gestión de riesgos:

Figura 3: Procesos principales del riesgo

| Figura 33—Procesos principales del riesgo | |
|---|---|
| Procesos COBIT 5 | Razonamiento |
| EDM03 Asegurar la optimización del riesgo | Este proceso abarca el entendimiento, la articulación y la comunicación del apetito y tolerancia al riesgo de la empresa, y asegura la identificación y gestión del riesgo asociado al valor de la empresa que está relacionado con el uso de TI y su impacto. Las metas de este proceso son:<br>• Definir y comunicar los umbrales de riesgo y asegurar que se conozcan los riesgos clave relacionados con TI.<br>• Gestionar de una manera efectiva y eficiente a los riesgos críticos de la empresa relacionados con TI.<br>• Asegurar que los riesgos de la empresa relacionados con TI no excedan su apetito de riesgo. |
| APO12 Gestionar el riesgo | Este proceso abarca la continua identificación, evaluación y reducción del riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa. La gestión de riesgos de la empresa relacionado con TI debería ser integrada al ERM global. Se deberían balancear los costos y beneficios de gestionar el riesgo de la empresa relacionado con TI mediante:<br>• La recolección de datos apropiados asociados al análisis de riesgos.<br>• Manteniendo el perfil de riesgo de la empresa y articulando los riesgos.<br>• Definiendo el portafolio de acciones de la gestión de riesgos y respondiendo al riesgo |

Fuente: COBIT 5

Procesos base para el soporte de la gestión de riesgos con Cobit 5.

Figura 4: Procesos clave de soporte de la función de riesgos

| Figura 19—Procesos clave de soporte de la función de riesgos | | |
|---|---|---|
| Identificación del proceso | Descripción | Productos específicos de riesgo |
| EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno. | El gobierno y la gestión de los riesgos requieren el establecimiento de un marco adecuado de gobierno para implementar estructuras, principios, procesos y prácticas. | Principios guía del gobierno del riesgo. |
| EDM02 Asegurar la entrega de beneficios. | Este proceso se focaliza en el manejo del valor que genera la función de riesgos. | Acciones para mejorar la entrega de valor del riesgo. |
| EDM05 Asegurar la transparencia hacia las partes interesadas. | La función de riesgos de una empresa, requiere de la medición transparente del desempeño y la conformidad, con metas y métricas aprobadas por las partes interesadas. | Evaluación de los requisitos del informe de riesgos. |
| APO02 Gestionar la estrategia. | La estrategia de gestión de riesgos de TI debe estar bien definida y alineada con el enfoque ERM. | Estrategia de la gestión de riesgos. |
| APO06 Gestionar presupuestos y costos. | La función de riesgos debe presupuestarse. | Requisitos financieros y presupuestarios. |
| APO07 Gestionar los recursos humanos. | La gestión de riesgos requiere una cantidad adecuada de personas, habilidades y experiencia. | Marco de competencias de recursos humanos. |
| APO08 Gestionar las relaciones. | Mantener las relaciones entre la función de riesgos y el negocio. | Plan de comunicación de la gestión de riesgos. |
| APO11 Gestionar la calidad. | La calidad es un componente que no debe omitirse en la gestión efectiva de riesgos. Los entregables de la función de riesgos debieran ser tratados siguiendo el sistema de gestión de calidad de la empresa. | Revisión de la calidad de los entregables de la función de riesgos. |
| BAI08 Gestionar el conocimiento. | La función de riesgos requiere el conocimiento necesario para apoyar al personal en sus actividades. | • Clasificación de la información de la función de riesgos.<br>• Control de acceso sobre dicha información.<br>• Reglas para desechar la información. |

Fuente: COBIT 5

CRAMM

Fue desarrollado por el gobierno británico en 1997. CRAMM[19] es el acrónimo de CCTA Risk Analysis and Management Methodology.A su vez la CCTA es el acrónimo de la Central Computer and Telecommunications Agency. Traduciendo al español CRAMM es la Metodología para el Análisis y Administración del Riesgo de la CCTA (Agencia Central de Computación y Telecomunicación). CRAMM es consistente con los estándares y políticas de seguridad del gobierno británico y del BS7799 (el código de prácticas para la administración de seguridad de la información).

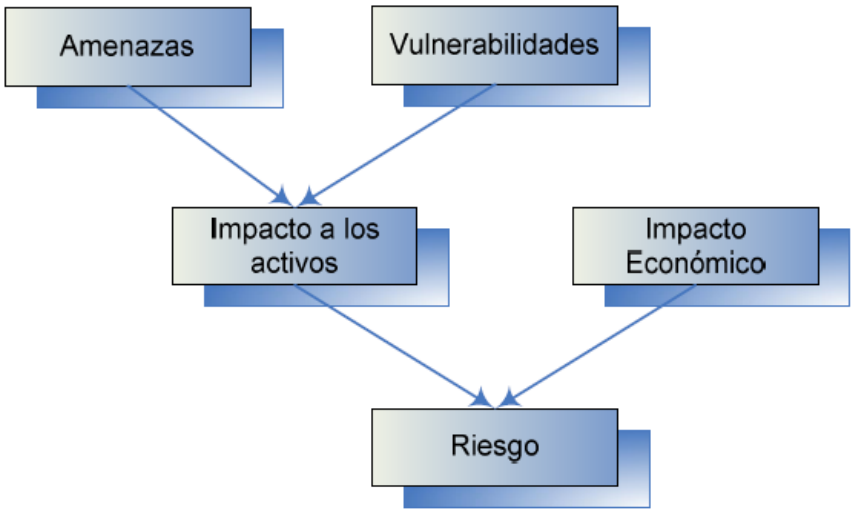
El método para el análisis de riesgo usado por CRAMM consiste en evaluar los siguientes tres factores:

- Las amenazas que pueden afectar a los activos.
- Las vulnerabilidades que pueden ser aprovechadas por esas amenazas.
- El costo en caso del impacto hacia el activo.

Y a partir de esto se determina el nivel de riesgo o se establece una medida del riesgo. Este concepto se ilustra en la figura 5.

[19]Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México-Edición Única. 23-25. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

Figura 5: El riesgo según CRAMM



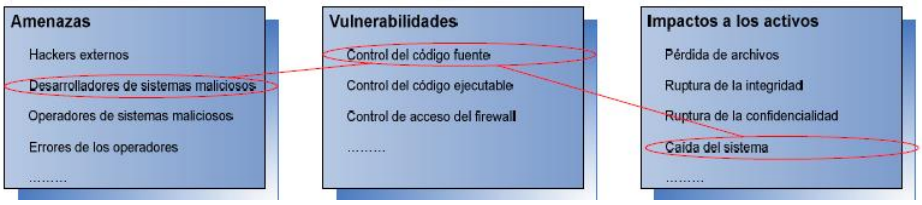

Fuente: Tecnológico de Monterrey

El análisis de riesgo en sí mismo consiste en cinco pasos:

1. Identificar los activos, amenazas y vulnerabilidades: Cada activo potencial de ser impactado tiene que ser identificado. Listas de todas las amenazas imaginables, de todas las vulnerabilidades relevantes y todos los activos potencialmente afectados son establecidas.

2. Identificar los posibles impactos a los activos: Una lista de todas las combinaciones de amenazas y vulnerabilidades que potencialmente puedan causar un impacto a un activo son identificadas, los cuales se ilustran en la figura 6.

Figura 6: Impactos potenciales. Combinación de amenaza, vulnerabilidad e impacto- CRAMM




Fuente: Tecnológico de Monterrey

3. Evaluación de los activos y medición de las amenazas y vulnerabilidades: Cada activo potencialmente afectado tiene que ser evaluado de acuerdo a los costos de pérdida o daño del activo. Todos los valores son transcritos a una escala de 1 a 10. La fuerza de las amenazas y el nivel de vulnerabilidades debe ser cuantificado. Los posibles valores para las amenazas y las vulnerabilidades son: bajo, medio y alto.
4. Calcular el riesgo: Para este cálculo se usa una tabla tridimensional donde la fuerza de la amenaza, el nivel de vulnerabilidad y el valor del activo son los parámetros de entrada, al final da el requerimiento de seguridad (dígase nivel de riesgo) en un rango de uno a cinco.
5. Revisión de los resultados: En este punto se revisan los datos. El común tiene que ser usado para ver si los resultados parecen razonables. Usualmente, un ajuste de los datos de entrada es necesario.

Después del análisis de riesgos, las mejores salvaguardas pueden ser seleccionadas y el análisis de riesgo puede ser hecho nuevamente, contando con las nuevas salvaguardas, para así determinar si se ha podido reducir el riesgo a un nivel aceptable.

MAGERIT

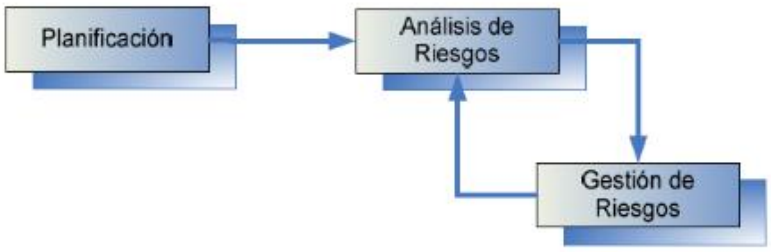
Metodología española para la gestión y análisis de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica. La razón de ser de MAGERIT[20] está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos, que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Esta metodología se puede resumir en la figura 7.

[20]Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México-Edición Única. 28-29. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

Figura 7: Administración de riesgos según MAGERIT




Fuente: Tecnológico de Monterrey

OCTAVE

OCTAVE[21], es el acrónimo de Operationally Critical Threat, Asset, and Vulnerability Evaluation (en español: Evaluación de Amenazas, Activos y Vulnerabilidades de Operaciones Criticas). Es una evaluación de riesgos estratégica y una técnica de planeación para la seguridad.

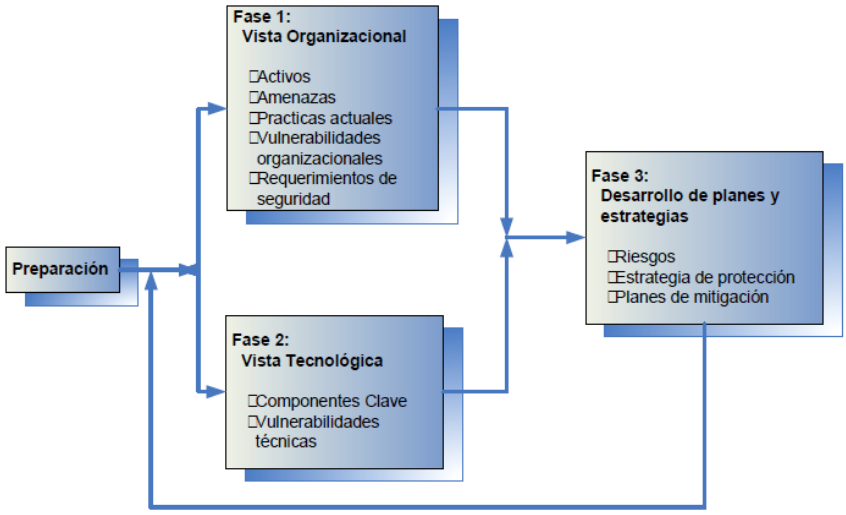
OCTAVE, se enfoca en el riesgo organizacional y en su estrategia. Busca balancear el riesgo operacional, las mejores prácticas de seguridad y la tecnología.

Esta metodología consta de tres pasos los cuales permiten construir una imagen de las necesidades de seguridad, los que se ilustran en la figura 8. Estos pasos son:

- Construir los perfiles de amenazas basados en los activos.
- Identificar las vulnerabilidades de la infraestructura.
- Desarrollar las estrategias y planes de seguridad.

[21]Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México-Edición Única. 29-30. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

Figura 8: Proceso de administración de riesgos de OCTAVE




Fuente: Tecnológico de Monterrey

Construir los perfiles de amenazas basados en los activos.

Esta etapa es una evaluación organizacional; se determina que información mantiene relación con los activos críticos con la finalidad de identificar que es importante para la organización y que es lo que actualmente se está haciendo para proteger estos activos. Posteriormente se seleccionan aquellos activos que sean más importantes para la organización y se describen los requerimientos de seguridad para cada activo crítico. Finalmente, se identifican las amenazas para cada activo crítico, creando un perfil de amenaza para ese activo.

Identificar las vulnerabilidades de la infraestructura.

Este paso es una evaluación de la infraestructura informática. Se examinan los caminos de acceso de la red, identificando los tipos de tecnología de información relacionados con cada activo.

Finalmente, se determina el grado de resistencia de cada tipo hacia los ataques de red.

Desarrollar las estrategias y planes de seguridad.

Durante esta etapa de evaluación, se identifican los riesgos a los que se están expuestos los activos críticos y se decide qué hacer con ellos. Se desarrolla una estrategia de protección para la organización y un plan de mitigación hacia los riesgos de los activos críticos basado en la información generada.

NIST 800-30

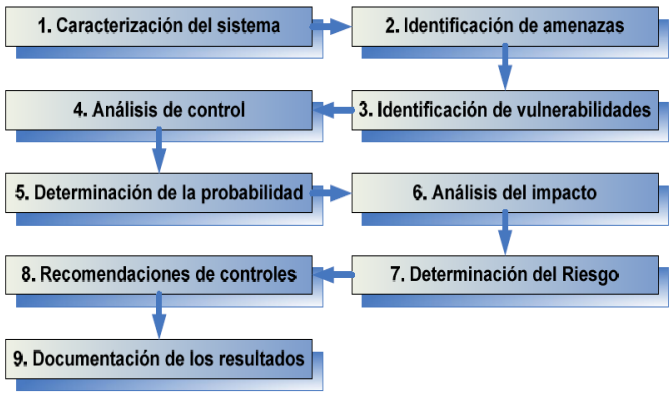
El Instituto Nacional de Estándares y Tecnología (NIST: Nacional Institute of Standards and Technology)[22] de Estados Unidos. El propósito es proporcionar una guía para la realización de evaluaciones de riesgo de los sistemas de información y las organizaciones federales, amplificando la orientación en la Publicación Especial 800-39. Las evaluaciones de riesgo se utilizan para identificar, estimar, y priorizar riesgo para las operaciones de la organización (es decir, la misión, funciones, imagen, y reputación), estas pueden llevar a cabo la jerarquía en los tres niveles de la gestión de riesgos, incluyendo Nivel 1 (nivel de organización), Nivel 2 (nivel de proceso de negocio de misión), y Nivel 3 (nivel de sistema de información); son parte de un proceso de gestión del riesgo global, proporcionando a los directivos con la información necesaria para determinar las formas de actuación en respuesta a los riesgos identificados.

[22]Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México-Edición Única. 32-36. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

En particular, NIST 800-30 proporciona una guía para la realización de cada uno de los pasos en el proceso de evaluación de riesgos (es decir, la preparación para la evaluación, la realización de la evaluación, la comunicación de los resultados de la evaluación, y el mantenimiento de la evaluación) y cómo las evaluaciones de riesgo y otra organización los procesos de gestión de riesgos se complementan y se informan mutuamente.

Estos pasos se esquematizan en la figura 9.

Figura 9: Evaluación de riesgos – NIST




Fuente: Tecnológico de Monterrey

## 1.4. Definición de términos básicos

Riesgos:

Según Cobit 5, el riesgo se define como el potencial de los objetivos empresariales no alcanzados o como cualquier oportunidad que puede mejorar los objetivos de la empresa.

Activos:

Ítem, objeto o entidad que tiene valor real o potencial para una organización.

Amenaza:

Eventos que pueden desencadenar un incidente en la organización produciendo daños materiales o pérdidas inmateriales.

Vulnerabilidad:

Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia. [UNE-ISO Guía 73:2010]

Impacto:

Consecuencia – Resultado de un suceso que afecta a los objetivos. [UNEISO Guía 73:2010]

Consecuencia que sobre un activo tiene la materialización de un riesgo. [Magerit: 1997]

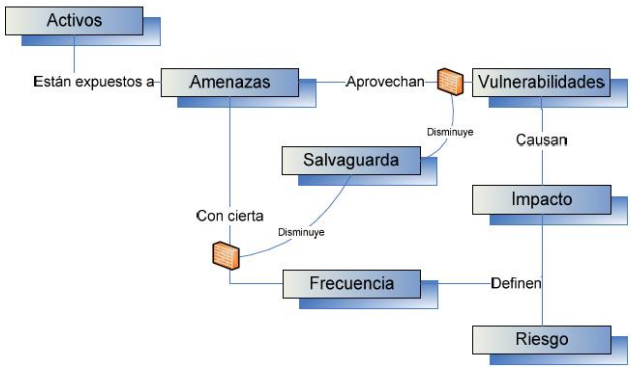
Salvaguarda:

Procedimiento o mecanismo tecnológico que reduce el riesgo. Control: Medida que modifica un riesgo. [UNE-ISO Guía 73:2010]

Interrelación de los conceptos básicos

Esquemáticamente podemos relacionar estos conceptos en la figura 10.

Figura 10: Relación entre activos, amenazas y riesgos




Fuente: Tecnológico de Monterrey

En resumen, los activos están expuestos a amenazas que aprovechan vulnerabilidades que al ser explotadas producen un impacto que multiplicado por la frecuencia de ocurrencia nos permite determinar el nivel de riesgo. Las salvaguardas, nos permiten reducir tanto el impacto como la frecuencia de que se materialicen los riesgos.

# CAPÍTULO II: MATERIALES Y MÉTODOS

## 2.1.Tipo de estudio y Diseño de Contrastación de Hipótesis

El tipo de estudio: Observacional, Transversal y Prospectiva.

Para el cumplimiento de los objetivos de la presente tesis, se identificó como diseño de contrastación el de tipo pre test – post test; el mismo que permite probar el planteamiento de la hipótesis. Para esto se mide la variable dependiente a ser utilizada (pre test), luego se efectúa una nueva medición de la variable dependiente, en la información, de las tecnologías de información que dan soporte a los procesos comerciales de las empresas de saneamiento del norte del Perú (post test), finalmente, la aplicación de la variable independiente el Modelo de Gestión de Riesgos basado en estándares adaptados a las TI utilizadas.

Diseño de Contrastación Pre-Test y Post-Test

Se detalla lo que se propone lograr en el resultado del método de diseño pre test – post test.

G O1 X O2

Donde:

- ✓ G: Caso de estudio seleccionado.

- ✓ O1: La aplicación de la encuesta pretest consistirá en una encuesta a los directores y gestores de TI, con la finalidad de evaluar el estado actual de la gestión de riesgos de TI.
- ✓ X: Modelo de gestión de riesgos de TI.
- ✓ O2: La aplicación de la encuesta postest consistirá aplicar la misma encuesta a los directores y gestores de TI, con la finalidad de evaluar la contribución del modelo a la continuidad del negocio.

## 2.2.Población

Empresas del Sector de Saneamiento del Norte del Perú catalogadas como empresas grandes según SUNASS.

## 2.3.Muestra

Respecto a la población de empresas de saneamiento del norte del Perú, la investigación se desarrolló, tomando como muestra a la empresa EPSEL S.A., y dentro de esta organización se ha tomado de manera censal los siguientes procesos comerciales:

- Medición.
- Facturación.
- Recaudación.
- Atención al Cliente.
- Catastro y Conexiones.
- Micro medición.

## 2.4.Muestreo

Para la presente investigación se utilizará un muestreo no probabilístico causal-accidental, y se considerarán 03 grupos de estudio:

- Alta dirección.

- Gestión Operativa.
- Personal.

## 2.5.Técnicas e instrumentos de recolección de datos

Tabla 1- Técnicas e instrumentos de recolección de datos

| Variable | Técnicas | Instrumentos |
|---|---|---|
| Contribuir a la continuidad de la operación de los procesos comerciales | Encuestas | ✓ Cuestionario (En el anexo N° 01 se puede observar la importancia de los activos que contribuyen a la continuidad de la operación de los procesos comerciales). |
| | Entrevistas | ✓ Cuestionarios (En el anexo N° 02 se puede observar el cuestionario evaluar el nivel de Gestión de Riesgos a nivel de Gobierno). |

Fuente: Propia

## 2.6.Plan de procesamiento para análisis de datos

Para la obtención de la información se utilizó la aplicación de encuestas y se uso entrevistas, así también el análisis documental, técnico importante para la revisión de documentación estratégica.

**Encuestas:**

Serán aplicadas a los usuarios del sistema comercial.

**Entrevistas:**

Hetero-administradas serán aplicadas a los especialistas del área de TI y a la plana directiva de las EPS.

**Análisis documental:**

**Revisión de documentos estratégicos:** Plan estratégico de TI.

**Revisión de documentos administrativos:** Políticas de seguridad de información, políticas de accesos, plan de contingencia y reportes de incidencias de TI.

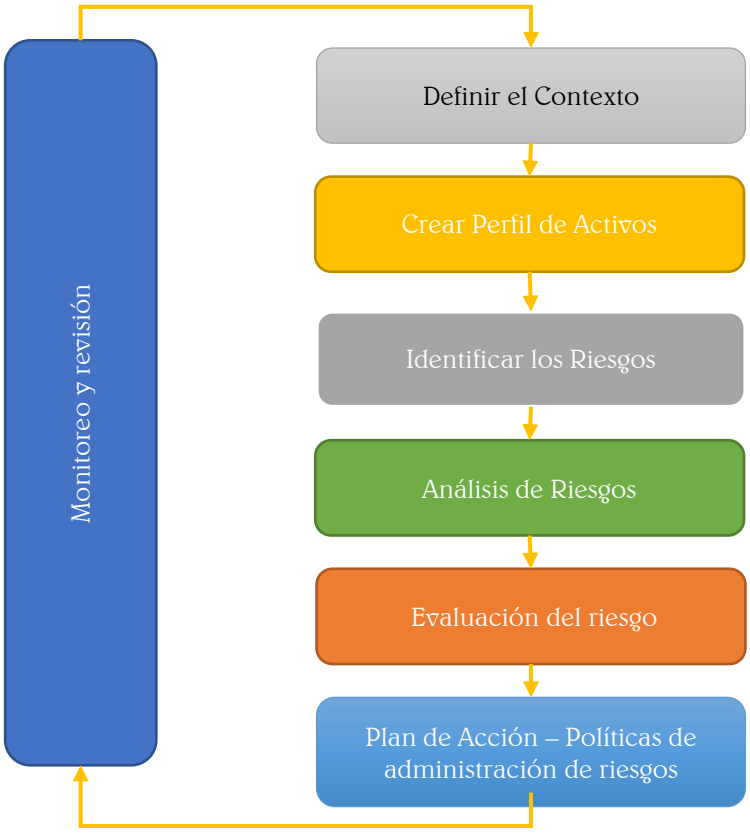
Para el plan de procesamiento utilizaremos las herramientas informática SPSS y/o Excel.

Asimismo, los principales indicadores, serán detallados a través de gráficos estadísticos.

# CAPÍTULO III: RESULTADOS Y DISCUSIÓN

En este capítulo se analizó el estándar ISO 31000:2011y metodologías referentes a la gestión de riesgos de tecnologías de la información: Magerit, Octave, Nist y COBIT 5, determinando las siguientes fases coincidentes, las cuales se adaptaron a la realidad de las empresas del sector de saneamiento del norte del Perú.

Figura 11: Modelo de gestión de riesgos propuesto




Fuente: Propia

### Fase N° 01: Definición del contexto

Esta fase tiene como base fundamental la fase N° 01 de la norma ISO 31000:2009 donde define los parámetros básicos internos y externos para la gestión del riesgo.

Para poder evaluar los riesgos se debe incluir su definición y la clasificación de los criterios de riesgo interno y externo.

### Proceso 1: Definición del contexto interno

Este proceso tiene como objetivo identificar los parámetros de fuente y detalle en cada criterio del contexto interno.

1. Descripción:

   Definir parámetros básicos internos para alcanzar los objetivos estratégicos de la organización.

2. Herramientas:
   a. Formato de definición de contexto interno. (Tabla 2).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Manual de organización y funciones (MOF).
   b. Cuadro de asignación de personal (CAP).
   c. Plan Estratégico.
   d. Organigrama.
   e. Misión.
   f. Valores.
   g. Patrimonio.
   h. Inventario de activos.
5. Información de salida:
   a. Listado de definición de contexto interno.

6. Procedimiento:
    a. Identificar fuente y detalle del factor interno cultural.
       Características de las entidades prestadoras de servicios de saneamiento de la región.
    b. Identificar fuente y detalle del factor interno normativo.
       Identificar normas, estándares de referencia adoptados por la organización.
    c. Identificar fuente y detalle del factor interno partes internas involucradas y la relación del personal con los procesos de la empresa.
    d. Identificar fuente y detalle del factor interno recursos.
       Inventarios de activos de infraestructura tecnológica de la organización.
    e. Identificar fuente y detalle del factor interno estructura.
       Se define como está organizado las funciones de la organización.
    f. Identificar fuente y detalle del factor interno metas y objetivos.
       Lo que se quiere lograr en un tiempo establecido para la organización.
    g. Identificar fuente y detalle del factor interno valores.
       Características que nos identifica como organización.

| LOGO | Fase: 01 | Proceso: 01 | Actividad: - | CÓDIGO DECI N°___ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Definición del contexto interno | | | | |
| **Objetivo:** Identificar los parámetros de fuente y detalle en cada criterio del contexto interno. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 2 - Formato de definición del contexto interno

| Criterio | Fuente | Detalle |
|---|---|---|
| Cultural | Plan estratégico | EPSEL S.A. tiene como objeto la prestación de los servicios de saneamiento de agua potable y alcantarillado sanitario. |
| Normativo | Oficina de Desarrollo Empresarial | ▪ MOF.<br>▪ CAP.<br>▪ ROF.<br>▪ Plan Estratégico.<br>▪ PIA. |
| Partes Internas Involucradas | Personal administrativo | ▪ Medición.<br>▪ Facturación.<br>▪ Recaudación.<br>▪ Atención al Cliente.<br>▪ Catastro y Conexiones.<br>▪ Micro medición. |
| Recursos | CAP | ▪ Personal |
| Metas y Objetivos | Plan estratégico | ▪ Misión<br>▪ Visión |
| Valores | Plan estratégico | ▪ Trabajo en Equipo.<br>▪ Honestidad.<br>▪ Protección del Medio Ambiente. |
| Criterio N | Fuente N | Detalle N |
| Criterio N+1 | Fuente N+1 | Detalle N+1 |
| … | … | … |
| … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

### Proceso 2: Definición del contexto externo

Este proceso tiene como objetivo identificar los parámetros de fuente y detalle en cada criterio del contexto externo.

1. Descripción:

   Definir parámetros básicos externos para alcanzar los objetivos estratégicos de la organización.

2. Herramientas:
   a. Formato de definición de contexto externo. (Tabla 3).

3. Responsable:
   a. Equipo de análisis.

4. Información de entrada:
   a. Convenios.
   b. INEI.
   c. NTP Seguridad.
   d. NTP Desarrollo.
   e. Gobiernos locales.
   f. Cuadro de asignación de personal (CAP).
   g. Marco normativo.
   h. Constitución Política.
   i. Entidades Financieras

5. Información de salida:
   a. Listado de definición de contexto externo.

6. Procedimiento:
   a. Identificar fuente y detalle del factor externo ambiente del negocio.

Convenios con otras empresas para afectar el desempeño de la organización.

b. Identificar fuente y detalle del factor externo normativo y político.
   Normas y leyes que por su incumplimiento puede afectar a la organización.
c. Identificar fuente y detalle del factor interno financiero.
   Aspectos relacionados con la economía.

| LOGO | Fase: 01 | Proceso: 02 | Actividad: - | CÓDIGO DECE N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Definición del contexto externo | | | | |
| **Objetivo:** Identificar los parámetros de fuente y detalle en cada criterio del contexto externo. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 3- Formato de definición del contexto externo

| Criterio | Fuente Sugerida | Detalle |
|---|---|---|
| Ambiente del Negocio | Convenios | Convenio de operaciones reciprocas con las entidades del estado. |
| Normativo y Político | Portal de Transparencia de Epsel | ▪ Ley Orgánica de Municipalidades, Ley N° 27972.<br>▪ Ley de la Actividad Empresarial del Estado, Ley N° 24948.<br>▪ Ley General de sociedades, Ley N°26887.<br>▪ Ley General del Sistema Nacional de Presupuesto, Ley 28411.<br>▪ Plan Nacional de Saneamiento 2006 – 2015, D.S. N° 007 – 2006 – vivienda.<br>▪ Ley de Creación de la Superintendencia Nacional de Servicios de Saneamiento, Decreto Ley N° 25965.<br>▪ Ley General del Ambiente, Ley N° 28611.<br>▪ Ley General de Servicios de Saneamiento Ley N° 26338 y su Reglamento.<br>▪ Estatutos de la empresa, reglamento aprobado por D.S N° 09-95-PRES vigente, se cambia la denominación de EMAPAL por el de EPSEL S.A integrando a las municipalidades distritales. |
| | Portal Institucional de SUNASS | ▪ Resolución Directiva N ° 064.<br>▪ Resolución Directiva N° 011. |
| Financiero | Entidades financieras | ▪ Gobierno francés.<br>▪ Banco Continental.<br>▪ BCP.<br>▪ Interbank.<br>▪ Banco de la Nación. |
| Criterio N | Fuente Sugerida N | Detalle N |
| Criterio N+1 | Fuente Sugerida N+1 | Detalle N+1 |
| … | … | … |
| … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

### Fase N° 02: Generar perfil de activos

La norma ISO 31000:2009, en su fase de establecimiento del contexto, cita que es importante articular los objetivos de la organización, estableciendo el alcance y los criterios de riesgo, se ha considerado que para las empresas de saneamiento del norte del Perú, es importante definir este alcance apoyándose en la fase 1 del Método OCTAVE que busca recopilar información de toda la organización para determinar los perfiles de activos críticos de la organización. Para ello se deben ejecutar los siguientes procesos:

### Proceso 1: Identificar los conocimientos de dirección

Este proceso tiene como finalidad captar el conocimiento desde el punto de vista de la alta dirección para identificar los activos críticos, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales.

**Actividad 1:** Identificar de los activos críticos

1. Descripción:

   Esta actividad tiene como objetivo que los miembros de la alta dirección definan qué activos son críticos para ellos y la organización, que de haberse afectados se produzca un impacto negativo en la continuidad del proceso comercial.

2. Herramientas:
   a. Entrevista para la alta dirección. (Entrevista N° 01).
   b. Formato de ingreso de activos críticos. (Tabla 4).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Manual de organización y funciones (MOF).
   b. Cuadro de asignación de personal (CAP).

5. Información de salida:
    a. Listado de activos críticos para la alta dirección de las empresas de saneamiento del norte del Perú.
6. Procedimiento:
    a. Determinar en base al MOF y CAP, el personal de alta dirección con quienes se ejecutará esta actividad.
    b. Aplicar la entrevista dirigida a la alta dirección. (Entrevista Nº 01) Nota: Es importante que los miembros de alta dirección asignen una puntuación por grado de importancia a los activos que sean listados. La escala a utilizar es: 1 a 5, siendo 5 el más importante.
    c. Proceder a llenar la información en el formato de activos críticos. (Tabla 4).

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 01 | CÓDIGO IDAC N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Identificación de activos críticos | | | | |
| **Objetivo:** Definir qué activos son críticos para la organización, que de haberse afectados se produzca un impacto negativo en la continuidad del proceso comercial. | | | | **TIPO** | |
| **Actores** | | **Elaborado Por:** | | **Fecha Elaboración** | ___/___/_____ |
| **Revisado Por:** | | **Aprobado Por:** | | **Fecha Aplicación** | ___/___/_____ |

Tabla 4- Activos críticos

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| N°1 | S_PF | Servicios de Información | Proceso de Facturación | Proceso de cálculo de montos por los servicios de agua y alcantarillado de acuerdo a los consumos registrados en el proceso de medición y a la tarifa establecida para cada conexión, así como otros cargos a facturar (cuotas de convenio, intereses, cortes y rehabilitaciones, etc.). |
| | SW_SGC | Software | Sistema de Gestión Comercial | Sistema de gestión comercial SICDESA, que automatiza todos los procesos comerciales. |
| | SI_SBD | Soporte de Información | Servidor de Base de Datos | Servidor que contiene el programa que gestiona la base de datos que almacena toda la información comercial. |
| | Código N | Categoría N | Activo Crítico N | Descripción N |
| | Código N+1 | Categoría N+1 | Activo Crítico N+1 | Descripción N+1 |
| | … | … | … | … |
| | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

**Actividad 2:** Describir de las áreas de preocupación

1. Descripción:

   Con esta actividad desde el punto de vista de la alta dirección, se busca determinar qué situaciones pueden amenazar a los activos críticos, identificados en la actividad anterior, que están implicados en la operación de los procesos comerciales de las empresas de saneamiento del norte del Perú.

2. Herramientas:
   a. Identificación amenazas por activo. (Tabla 5).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Listado de activos críticos.
5. Información de salida:
   a. Listado de amenazas por activo. (Tabla 5).
6. Procedimiento:
   a. Evaluar la entrevista Nº 01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de amenazas por activo. (Tabla 5).

| | | | | | |
|---|---|---|---|---|---|
| LOGO | Fase: 02 | Proceso: 01 | Actividad: 02 | CÓDIGO IAAC N°__ | Pág. ___/ ___ |
| | Identificación de amenazas por activo crítico | | | | |
| **Objetivo:** Determinar qué situaciones pueden amenazar a los activos críticos. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 5 - Identificación amenazas por activo

| Proceso | Código | Activo Crítico | Situación |
|---|---|---|---|
| N° | S_PF | Proceso de Facturación | Modificaciones de la normativa vigente.<br>Restricción de tiempo de servicio y presión.<br>Agua no facturada. |
| | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegio de acceso.<br>Inconsistencia de registro de información. |
| | SI_SBD | Servidor de Base de Datos | Modificación de la información.<br>Caída del servicio por agotamiento de recurso. |
| | Código N | Activo Crítico N | Situación N |
| | Código N+1 | Activo Crítico N+1 | Situación N+1 |
| | … | … | … |
| | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Actividad 3:** Definir de requisitos de seguridad para los activos críticos.

1. Descripción:

   En esta actividad, se busca obtener los requisitos de seguridad para cada activo crítico, desde el punto de vista de la alta dirección de las empresas de saneamiento del norte del Perú. Estos requisitos estarán definidos en base a los criterios de continuidad, integridad y disponibilidad de la información, pilares de la seguridad informática y pueden ser de índole legal, regulatorios, contractual y aquellos que hayan sido establecidos por la empresa o que el personal considere crítico.

2. Herramientas:
   a. Requisito de seguridad por activo crítico. (Tabla 6).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Listado de activos crítico.
   b. Extraer información de la encuesta realizada.
5. Información de salida:
   a. Requerimiento de seguridad en base a criterios de integridad, confidencialidad y disponibilidad de los activos críticos.
6. Procedimiento:
   a. Evaluar la entrevista N° 01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de requerimiento de seguridad por activo crítico. (Tabla 6).

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 03 | CÓDIGO DRSA N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 6 - Requisito de seguridad por activo crítico

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_PF | La información relacionada a la evolución de los montos facturados y su distribución tarifaria y geográfica solo debe ser accedida por el personal que toma de decisiones en relación a este proceso. | La información relacionada al proceso de facturación debe ser coherente mes a mes para poder tomar las decisiones pertinentes. | La información requerida y generada en este proceso debe estar siempre a disposición de las gerencias y personal que toma decisiones. | | |
| Activo Crítico N | Confidencialidad N | Integridad N | Disponibilidad N | Apetito N | Tolerancia N |
| Activo Crítico N+1 | Confidencialidad N+1 | Integridad N+1 | Disponibilidad N+1 | Apetito N+1 | Tolerancia N+1 |
| … | … | … | … | … | … |
| … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Actividad 4:** Identificar las estrategias actuales de protección

1. Descripción:

   Esta actividad, desde el punto de vista de la alta dirección tiene como objetivo identificar cuáles son las estrategias de protección con las que actualmente cuentan los activos identificados.

2. Herramientas:

   Cuadro de las estrategias actuales de activos críticos por área. (Tabla 7).

3. Responsable:
   a. Equipo de análisis.

4. Información de entrada:
   a. Listado de activos críticos.
   b. Extraer información de la encuesta realizada.

5. Información de salida:
   a. Estrategias actuales de protección y vulnerabilidades organizacionales.

6. Procedimiento:
   a. Evaluar la Encuesta N°01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de estrategias de protección y vulnerabilidades organizacionales por activo (Tabla 7).

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 04 | CÓDIGO IEOA N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Identificación de estrategias de protección y vulnerabilidades organizacionales por activo crítico | | | | |
| **Objetivo:** Identificar las estrategias actuales de protección. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 7- Estrategias de protección y vulnerabilidades organizacionales por activo

| Código de Activo | Activo | Estrategias actuales de protección |
|---|---|---|
| S_PM | Proceso de Medición | Muestreo de padrones de toma de lectura. |
| S_PF | Proceso de Facturación | Muestreo de recibos facturados. |
| Código de Activo N | Activo N | Estrategias actuales de protección N |
| Código de Activo N+1 | Activo N+1 | Estrategias actuales de protección N+1 |
| … | … | … |
| … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Proceso 2:** Identificar los conocimientos en el área de gestión operativa

Este proceso, tiene como finalidad captar el conocimiento desde el punto de vista de los gestores operativos comerciales para identificar los activos críticos, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales.

**Actividad 1:** Identificar de los activos críticos

Los administradores de las áreas operativas completan la encuesta en la que definen qué activos son críticos para ellos y la organización. Priorizando los activos identificando los cinco más críticos.

1. Descripción:

   Esta actividad tiene como objetivo que los gestores operativos comerciales definan qué activos son críticos para ellos y la organización, que de verse afectados, se produzca un impacto negativo a la operación de los procesos de gestión comercial.
2. Herramientas:
   a. Encuesta para la gestión operativa. (Encuesta N° 01).
   b. Formato de ingreso de activos críticos. (Tabla 4).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Manual de organización y funciones (MOF).
   b. Cuadro de asignación de personal (CAP).
5. Información de salida:
   a. Listado de activos críticos para la gestión operativa de las empresas de saneamiento del norte del Perú.

6. Procedimiento:
    a. Determinar en base al MOF y CAP, el personal de gestión operativa con quienes se ejecutará esta actividad.
    b. Aplicar la encuesta dirigida a la gestión operativa (Encuesta N° 01) Nota: Es importante que los miembros de la gestión operativa asignen una puntuación por grado de importancia a los activos que sean listados. La escala a utilizar es: 1 a 5, siendo 5 el más importante.
    c. Proceder a llenar la información en el formato de activos críticos (Tabla 4).

**Actividad 2:** Describir de las áreas de preocupación

1. Descripción:

    Con esta actividad, desde el punto de vista de los gestores operativos comerciales, se busca determinar qué situaciones pueden amenazar a los activos críticos, identificados en la actividad anterior, que están implicados en la operación de los procesos comerciales de las empresas de saneamiento del norte del Perú.
2. Herramientas:
    a. Identificación amenazas por activo. (Tabla 5).
3. Responsable:
    a. Equipo de análisis.
4. Información de entrada:
    a. Listado de activos críticos.
5. Información de salida:
    a. Listado de amenazas por activo. (Tabla 5).
6. Procedimiento:
    a. Evaluar la encuesta N° 01 aplicada en la actividad anterior.
    b. Proceder a llenar la información en el formato de amenazas por activo (Tabla 5).

**Actividad 3:** Definir de los requisitos de seguridad para los activos críticos

1. Descripción:

   En esta actividad busca obtener los requisitos de seguridad para cada activo crítico, desde el punto de vista de los gestores operativos comerciales de las empresas de saneamiento del norte del Perú. Estos requisitos, estarán definidos en base a los criterios de continuidad, integridad y disponibilidad de la información, pilares de la seguridad informática y pueden ser de índole legal, regulatorios, contractual y aquellos que hayan sido establecidos por la empresa o que el personal considere crítico.

2. Herramientas:
   a. Requisito de seguridad por activo crítico. (Tabla 6).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Listado de activos crítico.
   b. Extraer información de la encuesta realizada.
5. Información de salida:
   a. Requerimiento de seguridad en base a criterios de integridad, confidencialidad y disponibilidad de los activos críticos.
6. Procedimiento:
   a. Evaluar la encuesta N° 01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de requerimiento de seguridad por activo crítico. (Tabla 6).

**Actividad 4:** Identificar las estrategias actuales de protección

1. Descripción:

   Esta actividad desde el punto de vista de los gestores operativos comerciales, tiene como objetivo identificar cuáles son las estrategias de protección con las que actualmente cuentan, los activos identificados, así también determinar sus vulnerabilidades.

2. Herramientas:
   a. Cuadro de las estrategias actuales de activos crítico por área (Tabla 7).
3. Responsable:
   a. Equipo de análisis:
4. Información de entrada:
   a. Listado de activos críticos.
   b. Extraer información de la encuesta realizada.
5. Información de salida:
   a. Estrategias actuales de protección y vulnerabilidades organizacionales.
6. Procedimiento:
   a. Evaluar la encuesta N°01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de estrategias de protección y vulnerabilidades organizacionales por activo (Tabla 7).

**Proceso 3:** Identificar los conocimientos del personal

Este proceso tiene como finalidad captar el conocimiento desde el punto de vista del personal para identificar los activos críticos, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales.

**Actividad 1:** Identificar de los activos críticos

1. Descripción:

   Esta actividad tiene como objetivo que los miembros del personal definan qué activos son críticos para ellos y la organización, que de haberse afectados se produzca un impacto negativo, en la continuidad del proceso comercial.

2. Herramientas:
   a. Entrevista para el personal (Entrevista Nº 01).
   b. Formato de ingreso de activos críticos (Tabla 4).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Manual de organización y funciones (MOF).
   b. Cuadro de asignación de personal (CAP).
5. Información de salida:
   a. Listado de activos importantes para el personal de las empresas de saneamiento del norte del Perú.
6. Procedimiento:
   a. Determinar en base al MOF y CAP, para el personal con quienes se ejecutará esta actividad.
   b. Aplicar la entrevista dirigida al personal (Entrevista Nº 01).

      Nota: Es importante que los miembros del personal asignen una puntuación por grado de importancia a los activos que sean listados. La escala a utilizar es: 1 a 5, siendo 5 el más importante.

   c. Proceder a llenar la información en el formato de activos críticos (Tabla 4).

**Actividad 2:** Describir de las áreas de preocupación

1. Descripción:

   Con esta actividad, desde el punto de vista del personal se busca determinar, qué situaciones pueden amenazar a los activos críticos, identificados en la actividad anterior, que están implicados en la operación de los procesos comerciales de las empresas de saneamiento del norte del Perú.

2. Herramientas:
   a. Identificación amenazas por activo (Tabla 5).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Listado de activos críticos.
5. Información de salida:
   a. Listado de amenazas por activo (Tabla 5).
6. Procedimiento:
   a. Evaluar la encuesta N° 01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de amenazas por activo (Tabla 5).

**Actividad 3:** Definir de requisitos de seguridad para los activos críticos

1. Descripción:

   Esta actividad, busca obtener los requisitos de seguridad para cada activo crítico, desde el punto de vista del personal de las empresas de saneamiento del norte del Perú. Estos requisitos estarán definidos en base a los criterios de continuidad, integridad y disponibilidad de la información, pilares de la seguridad informática y pueden ser de índole legal, regulatorios, contractual y aquellos que hayan sido establecidos por la empresa o que el personal considere crítico.

2. Herramientas:
   a. Requisito de seguridad por activo crítico (Tabla 6).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Listado de activos críticos.
   b. Extraer información de la encuesta realizada.
5. Información de salida:
   a. Requerimiento de seguridad en base a criterios de integridad, confidencialidad y disponibilidad de los activos críticos.
6. Procedimiento:
   a. Evaluar la encuesta Nº 01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de requerimiento de seguridad por activo crítico (Tabla 6).

**Actividad 4:** Identificar las estrategias actuales de protección

1. Descripción:

   Esta actividad, desde el punto de vista del personal tiene como objetivo identificar, cuáles son las estrategias de protección con las que actualmente cuentan los activos identificados.
2. Herramientas:
   a. Cuadro de las estrategias actuales de activos críticos por área (Tabla 7).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Listado de activos críticos.
   b. Extraer información de la encuesta realizada.
5. Información de salida:
   a. Estrategias actuales de protección y vulnerabilidades organizacionales.

6. Procedimiento:
   a. Evaluar la encuesta N°01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de estrategias de protección y vulnerabilidades organizacionales por activo (Tabla 7).

**Proceso 4:** Identificar activos a gestionar

Este proceso tiene como objetivo determinar los activos de mayor importancia, de acuerdo al puntaje obtenido desde los distintos puntos organizacionales: dirección, gestión operativa y personal.

**Actividad 1:** Ponderar y priorizar la gestión de activos más críticos

1. Descripción:

   En este proceso se recoge las listas de activos, requisitos de seguridad y áreas de interés identificados en los procesos 1, 2 y 3, y se procede a asignar un valor ponderado por activo para cada una de las áreas, para finalmente determinar el puntaje final e identificar los activos críticos para la organización.
2. Herramientas:
   a. Cuadro de ponderación de activos (Tabla 8).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Lista de activos críticos.
5. Información de salida:
   a. Ponderación de activos.
6. Procedimiento:
   a. Evaluar la entrevista N° 01 y la encuesta N° 01 aplicada.
   b. Proceder a llenar la información en el formato de ponderación de activo (Tabla 8).

| LOGO | Fase: 02 | Proceso: 04 | Actividad: 01 | CÓDIGO POAC N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Ponderación de activos críticos | | | | |
| **Objetivo:** Ponderar y priorizar la gestión de activos más críticos. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 8- Ponderación de activos

| | | | Puntuación | | | | |
|---|---|---|---|---|---|---|---|
| Código | Categoría | Activo Crítico | Dirección | Operativa | Personal | Gestor de Riesgo | Promedio |
| S_PM | Servicios de Información | Proceso de Medición | 5 | 5 | 4 | 4 | 4.5 |
| S_PF | Servicios de Información | Proceso de Facturación | 5 | 5 | 4 | 5 | 4.75 |
| SW_SGC | Software | Sistema de Gestión Comercial. | 5 | 5 | 5 | 5 | 5 |
| SI_SBD | Soporte de Información | Servidor de Base de Datos | 5 | 5 | 5 | 5 | 5 |
| Código N | Categoría N | Activo Crítico N | Dirección N | Operativa N | Personal N | Gestor de Riesgo N | Promedio N |
| Código N+1 | Categoría N+1 | Activo Crítico N+1 | Dirección N+1 | Operativa N+1 | Personal N+1 | Gestor de Riesgo N+1 | Promedio N+1 |
| … | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

## Fase N° 03: Identificar los riesgos

Al identificar los riesgos, se busca determinar las acciones o circunstancias que podrían causar una pérdida potencial y comprender cómo, dónde y por qué puede ocurrir dicha pérdida; identificando los activos, amenazas, medidas de seguridad, vulnerabilidades y sus consecuencias.

**Proceso 1:** Crear perfil de amenaza

Esta fase, tiene como objetivo generar una lista de riesgos basada en aquellas situaciones que puedan afectar los activos implicados en la operación de los procesos comerciales.

Para poder gestionar los activos se ha utilizado MARGERIT versión 3.0 donde se clasifican, se desarrolla la dependencia entre ellos en un diagrama y se valoró en base a los criterios de la seguridad de la información: disponibilidad, integridad y confidencialidad. Con la finalidad de determinar el impacto que tendría la materialización de algún riesgo.

**Actividad 1:** Clasificación de activos

1. Descripción:

   En esta actividad, se procede a clasificar los activos críticos, identificados en la fase 2, en las categorías establecidas por el Método MAGERIT (servicios de información, software, hardware y soporte de información).
2. Herramientas:
   a. Lista de clasificación de activos (Tabla 9).
3. Responsable:
   a. Equipo analista.
4. Información de entrada:
   a. Lista de activos obtenidas de la Fase 2.

5. Información de salida:
   a. Clasificación de activos.
6. Procedimiento:
   a. Evaluar la lista de activos obtenidas en la fase 2.
   b. Clasificar los activos siguiendo las siguientes consideraciones:
      ✓ **[S] Servicios de Información:** Los datos son el corazón que permite a una organización prestar sus servicios, el cual serán transferidos de un lugar a otro por los medios de transmisión de datos.
      ✓ **[SW] Software:** Tareas que han sido automatizadas para su desempeño por un equipo informático; los cuales gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
      ✓ **[HW] Hardware:** Son bienes materiales, físicos, destinados a dar soporte a los servicios que presta la organización del sector de saneamiento, siendo depositarios temporales o permanentes de los datos de soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.
      ✓ **[SI] Soporte de Información:** Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, durante largos períodos de tiempo.
   c. Proceder a llenar la información en los formatos correspondientes de acuerdo a la clasificación que le corresponda de amenazas por activo (Tabla 9).

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 01 | CÓDIGO LCAC N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Lista de clasificación de activos críticos | | | | |
| **Objetivo:** Clasificar los activos. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 9- Lista de clasificación de activos

| Ítem | Activos | Código | Categoría | | | |
|---|---|---|---|---|---|---|
| | | | [S] | [SW] | [HW] | [SI] |
| 1 | Proceso de Medición | [S_PM] | X | | | |
| 2 | Proceso de Facturación | [S_PF] | X | | | |
| 3 | Sistema de Gestión Comercial | [SW_SGC] | | X | | |
| 4 | SICAP | [SW_SICAP] | | X | | |
| 5 | Impresoras | [HW_IMP] | | | X | |
| 6 | Estación de Trabajo | [HW_PC] | | | X | |
| 7 | Servidor Web | [SI_SWEB] | | | | X |
| 8 | Servidor DNS | [SI_SDNS] | | | | X |
| 9 | Servidor de Base de Datos | [SI_SBD] | | | | X |
| 10 | Activos N | Código N | [S] N | [SW] N | [HW] N | [SI] N |
| 11 | Activos N+1 | Código N+1 | [S] N+1 | [SW] N+1 | [HW] N+1 | [SI] N+1 |
| … | … | … | … | … | … | … |
| … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Actividad 2:** Dependencia de activos

1. Descripción:

   En este apartado se identifican los activos y se establece una relación de dependencia. Para establecer la relación de dependencia de activos se debe tener en cuenta:

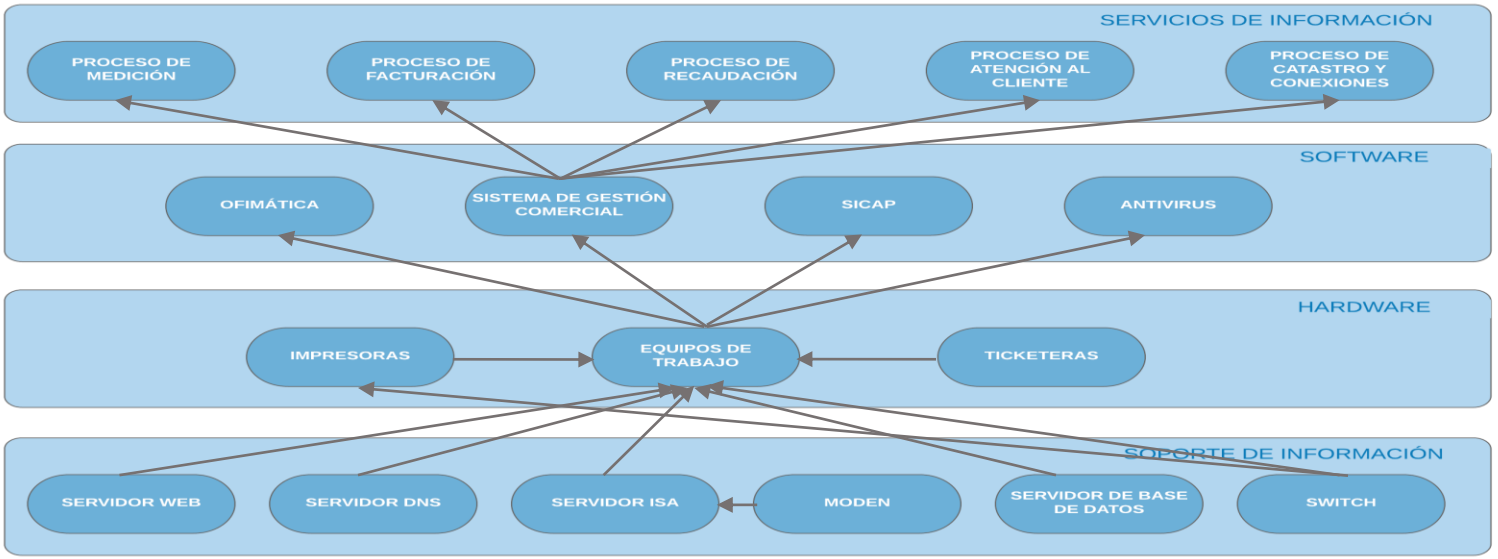
   ✓ Identificación de activos: Se propone establecer las categorías identificadas mediante la encuesta y entrevista: servicios de información, software, hardware y soporte de información correspondiente a las empresas del sector de saneamiento del norte del Perú.

   ✓ Establecer las líneas de dependencia: Esta actividad, permite establecer las líneas de soporte entre categorías con respecto a los activos, apoyando en la determinación de los activos críticos y el impacto que representaría de manifestarse el riesgo.

2. Herramientas:
   a. Diagrama de dependencia de activos (Diagrama 1).
3. Responsable:
   a. Equipo analista.
4. Información de entrada:
   a. Lista de clasificación de activos.
5. Información de salida.
   a. Dependencia de activos.
6. Procedimiento:
   a. Evaluar la entrevista N° 01 y la Encuesta N° 01 aplicada en la fase anterior.
   b. Proceder a relacionar la lista de clasificación activos en el diagrama de dependencia (Diagrama 1).

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 02 | CÓDIGO DDAC N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Diagrama de dependencias de activos críticos | | | | |
| **Objetivo:** Establecer una relación de dependencia. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Diagrama 1: Dependencias de activos




| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Actividad 3:** Valoración de activos

1. Descripción:

   La valoración de activos debe ser identificada desde una visión TOP-DOWN, para asignar el valor de acuerdo al grado de importancia teniendo en cuenta los criterios de disponibilidad, integridad y confidencialidad con una valoración cuantitativa y cualitativa.

   Para el proceso de valoración, se recomienda usar la Escala de Likert, que permite medir grados de conformidad con respecto a los criterios mencionados. Además de establecer rangos de valoración que en el caso se estableció del 1 al 5, permitiéndonos tener la amplitud suficiente para la valoración.

2. Herramientas:
   a. Valoración de criterio de confidencialidad (Tabla 10).
   b. Valoración de criterio de disponibilidad (Tabla 11).
   c. Valoración de criterio de integridad (Tabla 12).
   d. Tabla de valoración de los niveles de criticidad de activos (Tabla 13).
   e. Cuadro de valoración de activos (Tabla 14).
3. Responsable:
   a. Equipo analista.
4. Información de entrada:
   a. Lista de clasificación de activos.
5. Información de salida:
   a. Lista de activos valorizados.
6. Procedimiento:
   a. Valorar los activos tomando en cuenta los siguientes criterios:
      ✓ **Confidencialidad (C):** Información debe ser accedida sólo por las personas autorizadas (Tabla 10).

✓ **Disponibilidad (D):** Acceso a la información cuando se necesita (Tabla 11).

✓ **Integridad (I):** Exactitud y totalidad de la información (Tabla 12).

b. Proceder a llenar la información en el formato de valorización de activo (Tabla 14).

Tabla 10- Valoración de criterio de confidencialidad

| CONFIDENCIALIDAD (C) | |
|---|---|
| **Valor** | **Criterio** |
| 1 | De carácter público, no requiere control y no tiene impacto negativo en la empresa. |
| 2 | De menor importante, no afecta los procesos comerciales, requiere control mínimo, no tiene impacto negativo en la empresa. |
| 3 | Cuasi importante para la gestión comercial de la empresa requiere nivel bajo de control, impacta levemente a la empresa. |
| 4 | Importante para la gestión comercial de la empresa requiere nivel medio de control, impacta negativamente a la empresa. |
| 5 | De vital importancia para la gestión comercial de la empresa, requiere nivel alto de control, impacta seria y negativamente a la empresa. |

Fuente: Propia

Tabla 11- Valoración de criterio de disponibilidad

| DISPONIBILIDAD (D) | |
|---|---|
| **Valor** | **Criterio** |
| 1 | Información cuya inaccesibilidad no afecta la operación de los procesos comerciales. |
| 2 | Información cuya inaccesibilidad permanente de al menos 10% del tiempo durante la jornada laboral podría impedir la ejecución |

| DISPONIBILIDAD (D) | |
|---|---|
| Valor | Criterio |
| | de los procesos comerciales la empresa |
| 3 | Información cuya inaccesibilidad permanente de al menos 50% del tiempo durante la jornada laboral podría impedir la ejecución de los procesos comerciales de la empresa |
| 4 | Información cuya inaccesibilidad permanente de al menos 80% del tiempo durante la jornada laboral podría impedir la ejecución de los procesos comerciales de la empresa |
| 5 | Información cuya inaccesibilidad permanente de al menos el 95% del tiempo durante la jornada laboral podría ocasionar un perjuicio significativo para la empresa |

Fuente: Propia

Tabla 12- Valoración de criterio de integridad

| INTEGRIDAD (I) | |
|---|---|
| Valor | Criterio |
| 1 | Irrelevante para la correcta operación de los procesos comerciales. |
| 2 | Se puede recuperar de una forma bastante fácil. |
| 3 | Se puede recuperar guardando la relación pertinente con una molestia razonable. |
| 4 | Es factible recuperar la integridad del activo en un tiempo razonable. |
| 5 | No es posible recuperar el activo y sus relacionados. |

Fuente: Propia

**Nivel de valoración =** Confidencialidad + Integridad + Disponibilidad

Aplicando en dicha ecuación la siguiente valoración clasificada de la siguiente manera:

Tabla 13- Valoración de los niveles de criticidad de activos

| Rango | Valor | Descripción | | Criterio |
|---|---|---|---|---|
| 0 | 1 | Muy Bajo | MB | Irrelevante en la operación de los procesos comerciales |
| 1 – 3 | 2 | Bajo | B | Afecta levemente la operación de los procesos comerciales al menos un 10% del tiempo de la jornada laboral, no implica pérdida de información. |
| 4 – 6 | 3 | Medio | M | Afecta la operación de los procesos comerciales al menos un 50% del tiempo de la jornada laboral, no implica pérdida de información. |
| 7 – 9 | 4 | Alto | A | Afecta la operación de los procesos comerciales al menos un 80% del tiempo de la jornada laboral, puede implicar pérdida de información. |
| Igual o mayor a 10 | 5 | Muy Alto | MA | Paraliza la operación de los procesos comerciales al menos un 95% del tiempo de la jornada laboral, e implica pérdida de información. |

Fuente: Propia

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 03 | CÓDIGO VDAC N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Valoración de activos críticos | | | | |
| **Objetivo:** Valorar los activos. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 14 - Valoración de activos

| ACTIVO | | | | CRITERIOS | | | | |
|---|---|---|---|---|---|---|---|---|
| N° Ítem | Etiqueta Categoría | Código activo | Descripción del activo | Valoración confidencialidad | Valoración de Integridad | Valoración de Disponibilidad | TOTAL | |
| 1 | [S] | [S_PM] | Proceso de Medición | 5 | 5 | 5 | 15 | MA |
| 2 | [S] | [S_PF] | Proceso de Facturación | 5 | 5 | 5 | 15 | MA |
| 3 | [SW] | [SW_SGC] | Sistema de Gestión Comercial | 5 | 5 | 5 | 15 | MA |
| 4 | [SI] | [SI_SBD] | Servidor de Base de Datos | 5 | 5 | 5 | 15 | MA |
| 5 | Etiqueta Categoría N | Código activo N | Descripción del activo N | Valoración confidencial N | Valoración de Integridad N | Valoración de Disponibilidad N | Total N | Total N |
| 6 | Etiqueta Categoría N+1 | Código activo N+1 | Descripción del activo N+1 | Valoración confidencial N+1 | Valoración de Integridad N+1 | Valoración de Disponibilidad N+1 | Total N+1 | Total N+1 |
| … | … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Actividad 4:** Identificación de las amenazas y vulnerabilidades

1. Descripción:

   Esta actividad, tiene como objetivo identificar las vulnerabilidades y amenazas que se ciernen contra cada uno de los activos valorizados en la actividad anterior.

   Una vulnerabilidad, es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

2. Herramientas:
   a. Tabla de criterios de valoración de amenaza (Tabla 15).
   b. Tabla de Matriz de valorización de la amenaza (Tabla 16).
   c. Tabla de la valoración de la amenaza (Tabla 17).
   d. Tabla de criterios de valoración de vulnerabilidad (Tabla 18).
   e. Tabla de cruce de severidad – exposición (Tabla 19).
   f. Tabla de identificación de las vulnerabilidades (Tabla 20).
   g. Tabla de valorización de la vulnerabilidad (Tabla 21).
3. Responsable:
   a. Equipo de análisis.
4. Información de entrada:
   a. Lista de activos.
5. Información de salida:
   a. Valoración de vulnerabilidad.

6. Procedimiento:
   a. Analizar la información obtenida en la fase 1, para adicionar las amenazas que no estén consideradas en el listado de la tabla 17.
   b. Proceder a llenar la tabla 17 catalogando los activos valorizados en la actividad anterior de acuerdo a las amenazas a las que pueden estar expuestos.

      Para asignar los valores relacionados a la motivación y capacidad se debe considerar a la tabla 15, y el valor final de la amenaza se obtendrá usando la tabla 16 - Matriz de valorización de la amenaza.
   c. Sobre las amenazas que afectan a cada activo se procederá a llenar la tabla 20- Identificación de las vulnerabilidades, que tiene por finalidad determinar que vulnerabilidades tienen cada uno de los activos identificados frente a los riesgos determinados.
   d. En base a la valorización considerada en la tabla 18 criterios de valoración de vulnerabilidad, se procede a llenar la tabla 21 - Valorización de la vulnerabilidad, para asignar el valor de la vulnerabilidad se deberá usar el tabla 19 -Cruce de severidad - exposición.

Tabla 15 - Criterios de valoración de amenaza

| Valor | Capacidad | Motivación |
|---|---|---|
| 1 | Poca o nula capacidad de realizar el ataque. Cumple con menos del 30% del perfil del responsable del proceso y con menos el 20% de los accesos al proceso. | Poca o nula motivación. No se está inclinando a actuar. |
| 2 | (1) Capacidad moderada. Se tiene el conocimiento y habilidades para realizar el ataque, pero pocos recursos. Cumple con menos del | Nivel moderado de motivación. Se actuará si se le pide o provoca. |

| Valor | Capacidad | Motivación |
|---|---|---|
| | 60% del perfil del responsable del proceso y con menos el 40% de los accesos al proceso.<br>(2) Tiene suficientes recursos, pero conocimiento y habilidades limitadas. Cumple con menos del 40% del perfil del responsable del proceso y con menos el 60% de los accesos al proceso. | |
| 3 | Altamente capaz. Se tienen los conocimientos, habilidad y recursos necesarios para realizar un ataque. Cumple con menos del 80% del perfil del responsable del proceso y con al menos el 70% de los accesos al proceso. | Altamente motivado. Casi seguro que intentará el ataque |

Fuente: Propia

Tabla 16- Matriz de valorización de la amenaza

| Capacidad | Motivación | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 4 |
| 3 | 3 | 4 | 5 |

Fuente: Propia

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 17- Valoración de la amenaza

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| 1 | Fuego | SI_SBD | 3 | 1 | 3 |
| 2 | Daños por agua | SI_SBD | 3 | 1 | 3 |
| 3 | Desastres naturales | SI_SBD | 1 | 1 | 1 |
| 4 | Corte de suministro eléctrico | SI_SBD | 2 | 2 | 3 |
| 5 | Condiciones inadecuadas de temperatura o humedad | SI_SBD | 1 | 1 | 1 |
| 6 | Fallo de servicios de comunicaciones | SI_SBD | 2 | 2 | 3 |
| 7 | Amenazas N | Activos N | Capacidad N | Motivación N | Valor amenaza N |
| … | … | …. | …. | …. | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

Tabla 18- Criterios de valoración de vulnerabilidad

| Valor | Severidad | Exposición |
|---|---|---|
| 1 | **Severidad Menor:** Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene poco potencial de pérdida o daño en el activo. Tiene un nivel de acceso a la operación del proceso menor al 10% del total de privilegios requeridos y afecta solo a 1 de los 6 procesos comerciales. | **Exposición Menor:** Los efectos de vulnerabilidad son mínimos. No incrementa la posibilidad de que vulnerabilidades adicionales sean explotadas. |
| 2 | **Severidad Moderada:**<br><br>**(1)** Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo; Tiene un nivel de acceso a la operación del proceso menor al 50% del total de privilegios requeridos y afecta a por lo menos 3 de los 6 procesos comerciales considerados.<br><br>**(2)** Se requiere pocos recursos para explotar la vulnerabilidad y tiene un potencial moderado de pérdida o daño en el activo. Tiene un nivel de acceso a la operación del proceso menor al 30% del total de privilegios requeridos y afecta a por lo menos 3 de los 6 procesos comerciales considerados. | **Exposición Moderada:** La vulnerabilidad puede afectar a más de un elemento o componente del sistema. La explotación de la vulnerabilidad aumenta la posibilidad de explotar vulnerabilidades adicionales. |
| 3 | **Severidad Alta:** Se requieren pocos recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo. Tiene un nivel de acceso a la operación del proceso de más del 80% del total de privilegios requeridos y afecta a por lo menos 4 de los 6 procesos comerciales considerados. | **Exposición Alta:** La vulnerabilidad afecta a la mayoría de los componentes del sistema. La explotación de la vulnerabilidad aumenta significativamente la posibilidad de explotar vulnerabilidades adicionales. |

Fuente: Propia

Tabla 19- Cruce de severidad – exposición

| Severidad | Exposición | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 4 |
| 3 | 3 | 4 | 5 |

Fuente: Propia

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidades. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 20- Identificación de las vulnerabilidades

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores. |
| 50 | R50 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de seguridad. |
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores. |
| 52 | R52 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en las políticas de copias de seguridad. |
| 53 | Código del Riesgo N | Código de Activo N | Activo N | Amenaza N | Vulnerabilidad N |
| 54 | Código del Riesgo N+1 | Código de Activo N+1 | Activo N+1 | Amenaza N+1 | Vulnerabilidad N+1 |
| … | …. | … | … | … | … |
| … | …. | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 21- Valorización de la vulnerabilidad

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores | 2 | 3 | **4** |
| 50 | R50 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de seguridad | 2 | 3 | **4** |
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 3 | **5** |
| 52 | R52 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en las políticas de copias de seguridad | 3 | 3 | **5** |
| 53 | Código Riesgo N | Código de Activo N | Activo N | Amenaza N | Vulnerabilidad N | Severidad N | Exposición N | Valor Vulnerabilidad N |
| 54 | Código Riesgo N+1 | Código de Activo N+1 | Activo N+1 | Amenaza N+1 | Vulnerabilidad N+1 | Severidad N+1 | Exposición N+1 | Valor Vulnerabilidad N+1 |
| … | … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

FASE N° 04: Análisis de riesgos

La norma ISO 31000:2009, en su fase de apreciación del riesgo, indica que el análisis del riesgo permite tomar las decisiones, acerca de si es necesario tratar los riesgos y permite determinar los métodos de tratamiento más apropiados además de proporcionar los elementos para tomar decisiones cuando es necesario hacer algún tipo de elección y los diferentes niveles de riesgo.

Para ello se expresa las consecuencias (impacto) y la posibilidad, así como la manera en que ambas se combinan para determinar el nivel de riesgo de cada una de las amenazas identificadas, para los activos críticos de la organización, finalmente clasificarlas en un cuadro de prioridad.

Proceso 1: Determinación de posibilidad

1. Descripción:

   En este proceso se determina el valor de la posibilidad de que un riesgo se materialice a causa de una determinada vulnerabilidad.

2. Herramientas:
   a. Tabla de definición de posibilidad (Tabla 22).
3. Responsable:
   a. Equipo analista.
4. Información de entrada:
   a. Listado de vulnerabilidad de los activos.
5. Información de salida:
   a. Valoración de vulnerabilidades.
6. Procedimiento:
   a. Para cada vulnerabilidad detectada para los activos críticos, se procede a asignar un valor de posibilidad de acuerdo a la tabla 22.
   b. Proceder a llenar la información en la tabla 24 de la matriz del nivel de riesgo en lo que corresponde al valor de la posibilidad.

Tabla 22- Definición de la posibilidad de ocurrencia

| Valor | Criterio de Posibilidad | Descripción |
|---|---|---|
| 1 | Casi imposible | Es casi inconcebible que el suceso ocurra – 0%de ocurrencias históricamente en la región. |
| 2 | Raro | Poco posible que ocurra (no se sabe que haya ocurrido alguna vez) – 0% de ocurrencias históricamente en la empresa. |
| 3 | Posible | Posible que ocurra (ha ocurrido raramente) – Menos del 10% del total de incidencias en la empresa. |
| 4 | Muy posible | Posible que ocurra algunas veces (no ha ocurrido con frecuencia) – Menos del 50% del total de incidencias en la empresa. |
| 5 | Casi cierto | Posible que ocurra muchas veces (ha ocurrido con frecuencia) Más del 80% del total de incidencias en la empresa. |

Fuente: Propia

**Proceso 2:** Análisis de impacto

1. Definición:

   Esta actividad nos permite medir los efectos adversos resultantes de la materialización de un riesgo para cada uno de los riesgos identificados para cada activo crítico.

2. Herramientas:

   a. Cuadro de definición de la magnitud del impacto (Tabla 23).

3. Responsable:

   a. Equipo analista.

4. Información de entrada:

a. Lista de vulnerabilidades de los activos.

5. Información de salida:
   a. Matriz de evaluación de riesgos.
6. Procedimiento:
   a. Para cada vulnerabilidad detectada para los activos críticos, se procede a asignar un valor de impacto de acuerdo a la tabla 23.
   b. Proceder a llenar la información en la tabla 24 de la matriz del nivel de riesgo en lo que corresponde al valor del impacto.

**Proceso 3:** Determinación del riesgo

1. Descripción:

   Este proceso, se encarga de determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza.

   Aplicando unas escalas de la magnitud del impacto podremos saber qué tanto influye en los procesos (Bajo, medio, alto).
2. Herramientas:
   a. Tabla de criterio de impacto (Tabla 23).
   b. Tabla de criterio de posibilidad (Tabla 22).
   c. Tabla de matriz del nivel de riesgo (Tabla 24).
3. Responsable:
   a. Equipo analista.
4. Información de entrada.
   a. Lista de vulnerabilidades de los activos.
5. Información de salida:
   a. Matriz del nivel de riesgo.

6. Procedimiento:

a. Calcular el nivel de riesgo que resulta del producto del valor de amenaza, vulnerabilidad, posibilidad y el impacto, asignados en las actividades anteriores.
b. Proceder a llenar la información en el formato de matriz de riesgo (Tabla 23).

Tabla 23 - Criterio de impacto

| Valor | Criterio | Definición del impacto |
|---|---|---|
| 1 | Insignificante | No requiere un esfuerzo extra para restablecer la operación de los procesos comerciales. |
| 2 | Menor | Puede implicar un tiempo de recuperación menor al 10% del tiempo de la jornada laboral y en la pérdida de algunos bienes, material o recursos. |
| 3 | Moderada | Puede implicar un tiempo de recuperación menor al 50% del tiempo de la jornada laboral y en la pérdida de bienes, material o recursos. |
| 4 | Mayor | Puede implicar un tiempo de recuperación menor al 80% del tiempo de la jornada laboral y en la pérdida de costosa de bienes, material o recursos. |
| 5 | Catastrófico | Puede implicar un tiempo mayor al 80.1% del tiempo de la jornada laboral, la paralización total de los procesos comerciales y en la pérdida de costosa de bienes, materiales o recursos. |

Fuente: Propia

| LOGO | Fase: 04 | Proceso: 03 | Actividad: - | CÓDIGO MDNRN°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 24- Matriz del nivel de riesgo

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores | 3 | 4 | 2 | 5 | 10 | 120 |
| 50 | R50 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de seguridad | 3 | 4 | 2 | 5 | 10 | 120 |
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 5 | 2 | 5 | 10 | 150 |
| 52 | R52 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en las políticas de copias de seguridad | 3 | 5 | 2 | 5 | 10 | 150 |
| 53 | Código del Riesgo N | Código de Activo N | Activo N | Amenaza N | Vulnerabilidad N | Valor Amenaza (1) N | Valor Vulnerabilidad (2) N | Posibilidad (3) N | Impacto (4) N | Riesgo (3)x(4) (5) N | Riesgo Total (1)x(2)x(5) N |
| 54 | Código del Riesgo N+1 | Código de Activo N+1 | Activo N+1 | Amenaza N+1 | Vulnerabilidad N+1 | Valor Amenaza (1) N+1 | Valor Vulnerabilidad (2) N+1 | Posibilidad (3) N+1 | Impacto (4) N+1 | Riesgo (3)x(4) (5) N+2 | Riesgo Total (1)x(2)x(5) N+1 |
| … | … | … | … | … | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

FASE N° 05: Evaluación del riesgo

La Norma ISO 31000:2009, en el proceso de evaluación de la fase de apreciación de riesgo, busca determinar en base a los resultados del análisis de riesgos, cuáles deben ser tratados y la prioridad para implementar el tratamiento.

Proceso 1: Elaboración de la matriz de clasificación del riesgo

1. Descripción:

   Este proceso tiene como objetivo clasificar a los riesgos según su prioridad de tratamiento con análisis adicionales.

   A través de una tabla de clasificación de riesgos según posibilidad e impacto, establecer si el riesgo se evita, se asume, se transfiere.

2. Herramientas:
   a. Cuadro de matriz de clasificación de riesgos (Tabla 25).
3. Responsable:
   a. Equipo analista.
4. Información de entrada:
   a. Matriz de nivel de riesgo.
5. Información de salida:
   a. Cuadro de priorización de riesgos.
6. Procedimiento:
   a. En base a la matriz de nivel de riesgo, se deberá obtener el valor del producto de la posibilidad y el impacto, para cada evento de amenaza, con estos valores se debe llenar la tabla 26 - Matriz de clasificación de riesgos.
   b. Con los valores calculados en el numeral anterior se procede a ubicar el evento en la matriz de clasificación de riesgos. Proceder a llenar la información en el formato de amenazas por activo de la tabla 17. Finalmente de acuerdo a la semaforización de la matriz de clasificación se procederá a

asignar en la tabla 27 priorización del riesgo, el valor de la prioridad de cada riesgo.

Leyenda 1: Leyenda de prioridad

| | | |
|---|---|---|
| | Prioridad 4 | 1 – 3 |
| | Prioridad 3 | 4 – 6 |
| | Prioridad 2 | 8 - 12 |
| | Prioridad 1 | 15 - 25 |

Fuente: Propia

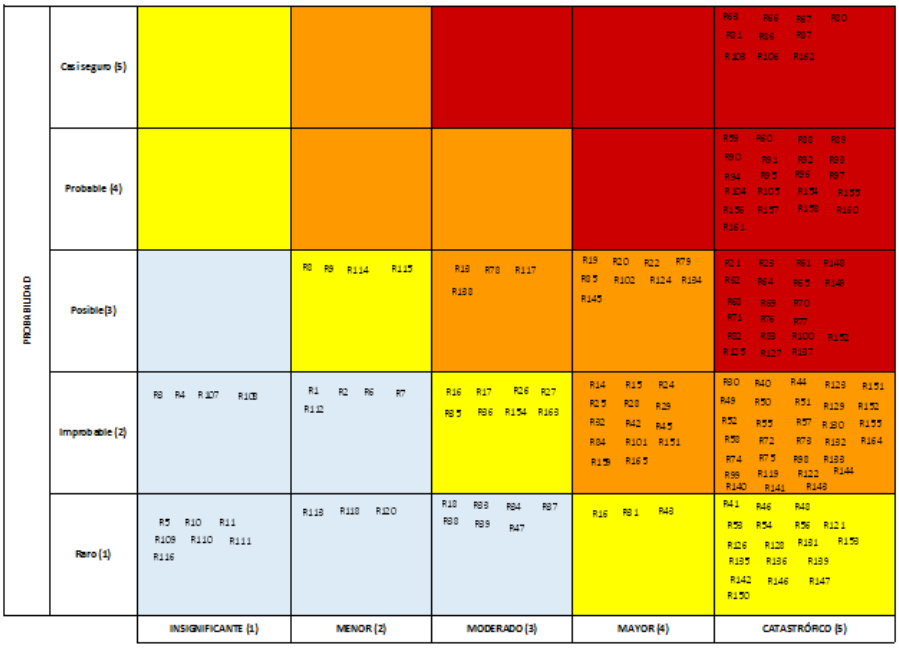
Tabla 25- Matriz de clasificación de riesgos

| | | | | | | |
|---|---|---|---|---|---|---|
| POSIBILIDAD | Casi seguro (5) | Moderada | Alta | Extrema | Extrema | Extrema |
| | | Asumir Reducir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir |
| | Probable (4) | Moderada | Alta | Alta | Extrema | Extrema |
| | | Asumir Reducir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir |
| | Posible(3) | Baja | Moderada | Alta | Alta | Extrema |
| | | Asumir | Asumir Reducir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir |
| | Improbable (2) | Baja | Baja | Moderada | Alta | Alta |
| | | Asumir | Asumir | Asumir Reducir | Reducir Evitar Compartir o transferir | Reducir Evitar Compartir o transferir |
| | Raro (1) | Baja | Baja | Baja | Moderada | Moderada |
| | | Asumir | Asumir | Asumir | Asumir Reducir | Asumir Reducir |
| | | INSIGNIFICANTE (1) | MENOR (2) | MODERADO (3) | MAYOR (4) | CATASTRÓFICO (5) |
| | | IMPACTO | | | | |

Fuente: Propia

| LOGO | Fase: 05 | Proceso: 01 | Actividad: - | CÓDIGO MDCR N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Matriz de clasificación de riesgos | | | | |
| **Objetivo:** Elaborar la matriz de clasificación del riesgo. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 26– Ejemplo de Matriz de clasificación de riesgos




Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: - | CÓDIGO PRDR N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgos. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 27- Priorización del riesgo

| N | Código de riesgo | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 49 | R49 | 2 | 5 | 10 | Alta |
| 50 | R50 | 2 | 5 | 10 | Alta |
| 51 | R51 | 2 | 5 | 10 | Alta |
| 52 | R52 | 2 | 5 | 10 | Alta |
| 53 | R53 | 1 | 5 | 5 | Moderada |
| 54 | R54 | 1 | 5 | 5 | Moderada |
| 55 | R55 | 2 | 5 | 10 | Alta |
| 56 | R56 | 1 | 5 | 5 | Moderada |
| 57 | R57 | 2 | 5 | 10 | Alta |
| 58 | R58 | 2 | 5 | 10 | Alta |
| 59 | R59 | 4 | 5 | 20 | Extrema |
| 60 | R60 | 4 | 5 | 20 | Extrema |
| 61 | R61 | 3 | 5 | 15 | Extrema |
| 62 | R62 | 3 | 5 | 15 | Extrema |
| 63 | R63 | 5 | 5 | 25 | Extrema |
| 64 | R64 | 3 | 5 | 15 | Extrema |
| 65 | Código de riesgo N | Posibilidad [P] N | Impacto [I] N | ([P]x[I]) N | Prioridad N |
| … | … | … | … | … | … |
| … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

**Proceso 2:** Valorización del riesgo

Este proceso, nos permite evaluar los riesgos determinados para cada activo en relación a los criterios de apetito y tolerancia determinado por la empresa, y así determinar si se trata de un riesgo aceptable o debe ser tratado.

**Actividad 1:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo

1. Descripción:

   Esta actividad proporciona por cada riesgo, límites de tolerancia, capacidad y apetito del riesgo para determinar si puede ser aceptable.

   Según la ISO (Guide 73:2009, 2009) define los siguientes conceptos:

   ✓ **Apetito:** Cantidad de riesgo que está dispuesta a asumir la organización.

   ✓ **Tolerancia:** Cantidad de riesgo que podría llegar a asumir la organización.

   ✓ **Capacidad:** Es el riesgo máximo asumible sin comprometer los objetivos.

2. Herramientas:
   a. Matriz de valoración de riesgos (Tabla 28).
3. Responsable:
   a. Equipo analista.
4. Información de entrada.
   a. Cuadro de priorización de riesgo.
5. Información de salida:
   a. Matriz de valoración de riesgos.
6. Procedimiento:
   a. Evaluar la entrevista N°01 aplicada en la actividad anterior.
   b. Proceder a llenar la información en el formato de amenazas por activo (Tabla 5).

| LOGO | Fase: 05 | Proceso: 02 | Actividad: 01 | CÓDIGO MDVR N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 28- Matriz de valorización de riesgos

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 | R10 | HW_IMP | Impresoras | Fuga de información | Ausencia de un plan de seguridad. | 1 | Baja | 5 | 10 | Aceptable |
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 53 | R53 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 54 | R54 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Políticas de copias de seguridad deficiente | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 59 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de Plan de Gestión de Configuración | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 60 | Código del Riesgo N | Código de Activo N | Activo N | Amenaza N | Vulnerabilidad N | Riesgo N | Prioridad N | Apetito N | Tolerancia N | Nivel N |
| 61 | Código del Riesgo N+1 | Código de Activo N+1 | Activo N+1 | Amenaza N+1 | Vulnerabilidad N+1 | Riesgo N+1 | Prioridad N+1 | Apetito N+1 | Tolerancia N+1 | Nivel N+1 |
| … | … | … | … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

FASE N° 06: Plan de acción - políticas de administración de riesgos

Esta fase busca establecer los parámetros para administrar los riesgos identificados de acuerdo a los niveles establecidos, con el fin de aplicar medidas necesarias que permitan crear una base confiable para la toma de decisiones, asignar y utilizar eficazmente los recursos para el tratamiento de los riesgos y asegurar de esta forma la continuidad en la operación de los procesos comerciales.

Proceso 1: Definición del plan de seguridad

Este proceso tiene, como finalidad diseñar planes de seguridad de acuerdo a las decisiones que se tomen en base al resultado de la fase de evaluación de riesgos. Para obtener este plan será necesario elaborar un conjunto armónico de programas de seguridad que traduzcan las decisiones de tratamiento de los riesgos en acciones concretas, buscando llevar el impacto riesgo a los niveles residuales determinados por la empresa mediante el establecimiento y la ejecución de los proyectos de seguridad que se identifiquen.

Actividad 1: Identificación de proyectos de seguridad

1. Descripción:

   Esta actividad, tiene como objetivo realizar acciones o proyectos que ayuden en el tratamiento del riesgo, donde se implementen estrategias de respuesta al riesgo que reduzca la posibilidad que ocurra o disminuya el impacto en los objetivos estratégicos de la organización.
2. Herramientas:
   a. Inventario de proyectos (Tabla 29).
3. Responsable:
   a. Equipo analista.

4. Información de entrada:
    a. Matriz de valoración de riesgos.
5. Información de salida:
    a. Formato de inventario de proyectos.
    b. Fichas de proyecto.
6. Procedimiento:
    a. Evaluar la matriz de valoración de riesgos y determinar de acuerdo al nivel de cada riesgo el tipo de acción que le corresponde y el proyecto que se debe evitar, transferir, mitigar y aceptar el riesgo según COBIT 5.
    b. Proceder a llenar la tabla 29 - Inventario de proyectos.
    c. Para cada proyecto se llenara la ficha del proyecto que se muestra en la tabla 30.
    d. Proceder a actualizar la tabla 29 - Inventario de proyectos, con la información del costo de cada proyecto.

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Inventario de proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad. | | | | **TIPO** | |
| **Actores** | | **Elaborado Por:** | | **Fecha Elaboración** | ___/___/_____ |
| **Revisado Por:** | | **Aprobado Por:** | | **Fecha Aplicación** | ___/___/_____ |

Tabla 29- Inventario de proyectos

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de Plan de Gestión de Configuración | 400 | Extrema | Reducir | Implementar plan de gestión de configuración de todos los equipos | S/.10,800.00 |
| 4 | R60 | SI_SBD | Servidor de Base de Datos | Fuga de información | Ausencia de un plan de seguridad. | 400 | Extrema | Reducir | Implementar plan de seguridad | S/.112,500.00 |
| 5 | R61 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 180 | Extrema | Reducir | Definir e implementar política de supervisión por muestreo para los diferentes procesos comerciales. | S/.1,500.00 |
| 6 | R62 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de un plan de supervisión | 180 | Extrema | Reducir | Implementar un plan de supervisión | S/.8,100.00 |
| 7 | Código Riesgo N | Código activo N | Activo N | Amenaza N | Vulnerabilidad N | Valor Riesgo N | Nivel N | Acciones N | Proyecto N | Costo N |
| 8 | Código Riesgo N+1 | Código activo N+1 | Activo N+1 | Amenaza N+1 | Vulnerabilidad N+1 | Valor Riesgo N+1 | Nivel N+1 | Acciones N+1 | Proyecto N+1 | Costo N+1 |
| … | … | … | … | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO FIPR N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto. | | | | **TIPO** | |
| **Actores** | | **Elaborado Por:** | | **Fecha Elaboración** | ___/___/_____ |
| **Revisado Por:** | | **Aprobado Por:** | | **Fecha Aplicación** | ___/___/_____ |

Tabla 30- Ficha de proyecto - "Implementar un plan de seguridad"

| **Proyecto N° 02: "Implementar plan de seguridad"** | |
|---|---|
| **Alcance** | El proyecto de implementación de un plan de seguridad contribuye a mejorar la seguridad en los activos de las EPS. |
| **Objetivo** | - Disminuir la difusión de software dañino.<br>- Reducir fuga de información.<br>- Prevenir la perdida de equipos.<br>- Reducir la manipulación de los datos que impacte negativamente en la gestión del proceso comercial. |
| **Riesgo/Clasificación** | R23 / R60 / R70 / R89 / R149 / R162 / R164 / R165 / R166 / R167 / R168 / R172. |
| **Estimación de Tiempos** | 6 meses. |
| **Requerimientos** | 1. Formar un comité de gestión de seguridad.<br>2. Obtener el compromiso de alta dirección.<br>3. Identificar la lista de activos de la entidad.<br>4. Evaluar los riesgos que podría tener cada activo de la entidad.<br>5. Definir la priorización de los riesgos de los activos.<br>6. Establecer medidas de protección de los activos en base a los riesgos identificados. |

**PROYECTO**

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Selección | Propuesta |
|---|---|---|---|---|
| Organismo supervisor de las contrataciones del estado - OSCE | 100% | S/ 126,496.00 | SI | Ver Anexo 07 |

| | |
|---|---|
| **Unidad Responsable** | Oficina de Informática. |
| **Activos afectados** | - Impresoras. - Estación de Trabajo. - Servidor de base de datos. - Servidor DHCP. - SICAP. |

Fuente: Propia

**Actividad 2:** Determinación del Plan de Ejecución

Su principal objetivo, es ordenar temporalmente los programas de seguridad.

1. Descripción:

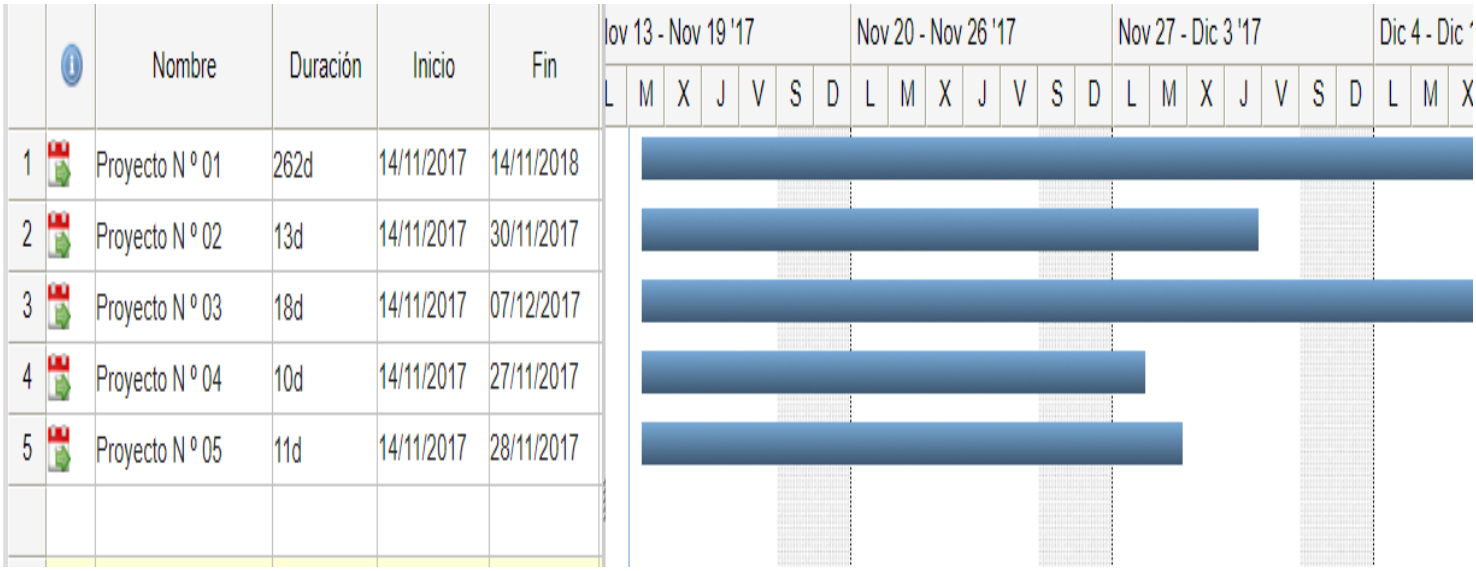
   Esta actividad busca ordenar los proyectos de seguridad inventariados en el punto anterior, para esto toma en cuenta factores como:

   a. Criticidad o gravedad del impacto de los riesgos que se afrontan, siendo las situaciones críticas las de mayor prioridad.
   b. Costo: el costo de ejecución de programa, así como la disponibilidad del recurso humanos para la dirección o ejecución (según se determine) de las tareas programadas
   c. Otros factores: como el presupuesto anual de la empresa, la evolución del marco legal, reglamentario o contractual, etc.

2. Herramientas:
   a. Cronograma de ejecución (Plan Director 1)
3. Responsable:
   a. Equipo analista.
4. Información de entrada:
   a. Inventario de proyectos.
5. Información de salida:
   a. Cronograma de ejecución de proyectos de seguridad.
6. Procedimiento:
   a. Evaluar el inventario de proyectos de seguridad (Tabla 29).
   b. Planificar la ejecución de los proyectos de seguridad priorizando de acuerdo a la criticidad, costo, presupuesto u otros.
   c. Llenar la tabla 31 - Cronograma del plan de ejecución.

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO CDPE N°__ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Cronograma del plan de ejecución | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 31- Formato de cronograma



| | Nombre | Duración | Inicio | Fin |
|---|---|---|---|---|
| 1 | Proyecto N º 01 | 262d | 14/11/2017 | 14/11/2018 |
| 2 | Proyecto N º 02 | 13d | 14/11/2017 | 30/11/2017 |
| 3 | Proyecto N º 03 | 18d | 14/11/2017 | 07/12/2017 |
| 4 | Proyecto N º 04 | 10d | 14/11/2017 | 27/11/2017 |
| 5 | Proyecto N º 05 | 11d | 14/11/2017 | 28/11/2017 |



Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

Fase N° 07: Monitorización y revisión

Esta fase tiene como objetivo evaluar periódicamente los cambios que pueden surgir al gestionar los riesgos, debido a que pueden darse cambios en los procesos, nuevas estrategias, modificación en los activos, entre otros.

Esta fase es importante para asegurar el cumplimiento de los objetivos estratégicos que se apoyan en la tecnología de información.

Proceso 1: Definición de lista de control

1. Descripción:

   Para evaluar los proyectos que darán tratamiento a los riesgos identificados, es necesario determinar el listado de indicadores en base a los cuales se efectuará la evaluación en mención, para este fin, en este proceso se elaborará el listado de indicadores por cada proyecto incluido en el plan de ejecución.

2. Herramientas:
   a. Cuadro de control de indicadores por proyecto.

3. Responsable:
   a. Equipo analista.

4. Información de entrada:
   a. Cronograma de ejecución de proyecto.

5. Información de salida:
   a. Listado de indicadores por proyecto

6. Procedimiento:
    a. Evaluar la tabla 31, cronograma del plan de ejecución de proyectos de seguridad.
    b. Determinar los indicadores a evaluar por cada uno de los proyectos incluidos en el plan de ejecución.
    c. Proceder a llenar la información en la tabla 32, lista de indicadores de control de indicadores a evaluar por proyecto.

| LOGO | Fase: 07 | Proceso: 01 | Actividad: - | CÓDIGO LIEP N° ___ | Pág. ___/ ___ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 32: Lista de control de indicadores a evaluar por proyecto

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control | | | | |
|---|---|---|---|---|---|---|---|---|
| Capacitación de uso de equipos | R21 | Número de incidentes en falla de equipos por error humano | Mensual | | | | | |
| Capacitación de uso y configuración de servidores | R125 | Cantidad de Incidentes por falla de configuración de servidores<br>Tiempo Promedio de Servicio Web fuera de línea | Mensual | | | | | |
| Capacitación en ingeniería social | R106 | Cantidad de incidentes de acceso no autorizado<br>Cantidad de ataques externos detectados | Mensual | | | | | |
| Proyecto N | Riesgos Tratados N | Indicadores a Evaluar N | Periodicidad de Evaluación N | Fecha de Control N | Fecha de Control N | Fecha de Control N | Fecha de Control N | Fecha de Control N |
| Proyecto N+1 | Riesgos Tratados N+1 | Indicadores a Evaluar N+1 | Periodicidad de Evaluación N+1 | Fecha de Control N+1 | Fecha de Control N+1 | Fecha de Control N+1 | Fecha de Control N+1 | Fecha de Control N+1 |
| … | … | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … |

Fuente: Propia

| | | |
|---|---|---|
| | | |
| **Ejecutor** | **Revisor** | **V°B°** |

**Proceso 2:** Seguimiento de los proyectos

1. Descripción:

   Para evaluar periódicamente los cambios que pueden surgir al gestionar los riesgos, se hará seguimiento a los proyectos implementados y a los riesgos que están siendo tratados, mediante la implementación del proyecto, para ello en base a la lista de indicadores y a la frecuencia de evaluación se elabora la ficha de monitoreo del proyecto.

2. Herramientas:

   a. Ficha de monitoreo del proyecto.

3. Responsable:

   a. Equipo analista.

4. Información de entrada:

   a. Cronograma de ejecución de proyecto.
   b. Lista de indicadores a evaluar.

5. Información de salida:

   a. Ficha de monitoreo del proyecto de ejecución.

6. Procedimiento:

   a. Evaluar la tabla 31, cronograma del plan de ejecución de proyectos de seguridad.
   b. Evaluar la tabla 32, lista de indicadores de control de indicadores a evaluar por proyecto y riesgo, determinando a que proyectos y riesgos les corresponden un proceso de evaluación ya sea porque se ha cumplido el plazo establecido para ser evaluado o porque se haya dado algún cambio en los procesos, nuevas estrategias, modificación en los activos u otros.
   c. Proceder a llenar la información en la tabla 33, ficha de monitoreo.

| | | | | | |
|---|---|---|---|---|---|
| LOGO | Fase: 07 | Proceso: 02 | Actividad: - | CÓDIGO<br>FDMO N° ___ | Pág. ___/ ___ |
| | Ficha de monitoreo | | | | |
| **Objetivo:** Monitorear y revisar periódicamente los cambios que pueden surgir al gestionar los riesgos. | | | | TIPO | |
| Actores | | Elaborado Por: | | Fecha Elaboración | ___/___/_____ |
| Revisado Por: | | Aprobado Por: | | Fecha Aplicación | ___/___/_____ |

Tabla 33- Ficha de monitoreo

| | | | |
|---|---|---|---|
| RIESGO | … colocar código(s) de riesgo | | |
| CÓDIGO ACTIVO | … colocar código de activo(s) afectados | | |
| PROYECTO DE SALVAGUARDA APLICADO | … colocar nombre del proyecto de salvaguarda | | |
| ESTADO DEL RIESGO | … colocar el estado en el que se encuentra el riesgo al momento del monitoreo (Ej. Mitigado) | | |
| MONITOREO Y REVISIÓN | | | |
| Fecha | DD /MM /AAAA | N° de Monitoreo/<br>Fecha Monitoreo Anterior | n<br>DD /MM /AAAA |
| INDICADORES | | | |
| 1. Listado de indicadores a evaluar. | | | |
| VALORES DE ENTRADA (De revisión anterior) | 1. | VALORES DE SALIDA | 1. |
| RECOMENDACIONES | | | |
| 1. Lista de recomendaciones. | | | |
| Responsable - Cargo | Nombre - Cargo | | |
| Fecha de Próxima Revisión | DD /MM /AAAA | | |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

## Discusión

De acuerdo al objetivo general planteado, en la presente tesis de contribuir a la operación de los procesos de gestión comercial las empresas de saneamiento del norte del país, se desarrolló un modelo de gestión de riesgos de TI basado en el estándar ISO 31000 y las metodologías Magerit, OCTAVE y NIST, adaptado para el mencionado sector.

Para la validación del modelo se diseñó para el mismo dos instrumentos:

Por juicio de expertos, para lo cual 2 profesionales expertos validaron la estructura y contenido del modelo propuesto en la presente tesis, obteniendo la aceptación del mismo (ver Anexo N° 03).

Para medir el nivel de confiabilidad del modelo, se procesó los resultados del juicio de expertos, aplicando el Método de Alfa de Crombach, obteniendo un nivel de confiabilidad del 90.9% como lo refiere los resultados del cálculo siguiente:

Tabla 34 - Estadística de confiabilidad

| Estadísticas de confiabilidad | |
|---|---|
| Alfa de Cronbach | N de elementos |
| 0.909 | 7 |

Fuente: Propia

Teniendo como referencia al criterio de George y Mallery (2003, p. 231) sugieren las recomendaciones siguientes para evaluar los coeficientes de alfa de Cronbach:

- Coeficiente alfa >0.9 es excelente.

- Coeficiente alfa >0.8 es bueno.
- Coeficiente alfa >0.7 es aceptable.
- Coeficiente alfa >.6 es cuestionable
- Coeficiente alfa >.5 es pobre.
- Coeficiente alfa <.5 es inaceptable.

La medida obtenida del coeficiente de confiabilidad es: excelente.

Prueba de concordancia de Kendall, para la validación de contenidos:

Para determinar el grado de acuerdo en la validez de los contenidos entre un grupo de expertos (m=3) y el número de ítems (7).

No basta con saber si W está más cercano a 0 o 1; sino que además debemos saber si W es distinta de 0 para rechazar la hipótesis de concordancia casual.

$$W = \frac{12S}{m^2(n^3 - n) - mT}$$

Tabla 35 – Estadística de confiabilidad de Kendall.

| Calculo de coeficiente de Kendall | |
|---|---|
| n | 7 |
| m | 3 |
| W | 0.04 |
| chi-cuadrado | 0.71 |
| gl (grados de libertad) | 6 |

| Calculo de coeficiente de Kendall | |
|---|---|
| Valor de p | 0.994 |

Fuente: Coeficiente de Kendall

Si el valor es de 1, significa un fuerte nivel de concordancia entre los evaluadores mientras que el valor de 0 muestra un nivel de desacuerdo total. La tendencia a 1 es lo deseado pudiéndose realizar nuevas rondas si en la primera no es alcanzada significación en la concordancia. Tomando en consideración lo mencionado, el modelo propuesto en el presente trabajo de investigación, obtuvo un valor de concordancia de 0.994 indicado que existe una alto nivel de concordancia entre los evaluadores.

Finalmente, de la combinación de los resultados de los dos métodos aplicados para la evaluación, se puede indicar existe una alto nivel de concordancia entre los 03 evaluadores y por el valor obtenido con la aplicación del método de Alfa de Cronbanch, el modelo alcanza un nivel de excelente.

Luego de la validación del modelo se procede a contrastar la hipótesis analizando los siguientes indicadores:

**Indicador 1: Porcentaje de activos críticos de tecnología de información y niveles de impacto definidos dentro de la gestión de los procesos comerciales de las empresas de saneamiento.**

Al evaluar la situación problemática que motivó el desarrollo de la presente investigación, se determinó que las empresas de saneamiento, carecían de un inventario de activos críticos de tecnología de información relacionados a la

operación de los procesos de gestión comercial, y estos no tenían definido niveles de impacto en la operación de los procesos.

La ejecución del modelo propuesto en la presente tesis, aplicado al caso de estudio de la empresa de saneamiento de Lambayeque, bajo un enfoque de simplicidad y flexibilidad, mostró como resultado ( Tabla N°11 ) la identificación de 18 activos críticos que de acuerdo a su clasificación se agruparon en 03 activos de hardware, 05 de servicios de información, 04 software y 06 de soporte de información 6, lográndose identificar la dependencia que existe entre ellos así como los requerimientos de confidencialidad, disponibilidad e integridad y las estrategias actuales con las de protección con las que cuenta cada uno de estos activos.

### Indicador 2: Número de riesgos detectados por activo

Como resultado de la evaluación de la situación actual de gestión de riesgos en la empresas del sector saneamiento situadas en el norte del Perú los miembros de los grupos de interés involucrados, manifiestan tener información de la existencia de estándares y metodologías de gestión de riesgos de TI, sin embargo resultan alta complejidad y requieren asignar personal exclusivo para su aplicación y monitoreo.

Para medir el indicador de número de riesgos detectados por activo crítico, se implementó para el caso de estudio el modelo propuesto debidamente validado por juicio de expertos (ver Anexo N°03) lográndose la identificación de 165 riesgos de los cuales, a través de la aplicación de 06 plantillas de trabajo, se logró determinar que 52 eran de tratamiento prioritario por ser calificados como extremos y los cuales afectan a la operación de los procesos gestión comercial soportados por TI.

### Indicador 3: Cantidad de proyectos propuestos para el tratamiento de los riesgos

En la evaluación de la situación problemática del contexto actual de gestión de riesgos en la empresas del sector saneamiento situadas en el norte del Perú los miembros de los grupos de interés involucrados, se determinó que para enfrentar alguna amenaza, se adoptaban respuestas de carácter reactivo que generaban altos costos de corrección y no se contaban con proyectos organizados que hayan sido propuestos y presupuestados con anticipación.

La ejecución del modelo propuesto en la presente tesis, aplicado al caso de estudio de la empresa de saneamiento de Lambayeque, mostró como resultado (Tabla N° 57) la identificación de 165 riesgos, de los cuales 52 fueron considerados de alta prioridad, por exceder los límites de tolerancia planteados por la empresa, que serían mitigados a través de la ejecución de 16 proyectos en el proceso de tratamiento de los mismos.

## CAPÍTULO IV: Aplicación del modelo de gestión de riesgos de TI al caso de estudio

A continuación se presentará el desarrollo de la aplicación del modelo de gestión de riesgos de TI en la empresa prestadora de servicios de saneamiento de Lambayeque EPSEL S.A., y se adjuntan en el anexo N° 06, los documentos que confirman la veracidad y conformidad de los datos considerados en la aplicación del modelo.

| LOGO | Fase: 01 | Proceso: 01 | Actividad: -- | CÓDIGO DECIN° ___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Definición del contexto interno | | | | |
| Objetivo: Identificar los parámetros de fuente y detalle en cada criterio del contexto interno. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | LMOSCOSO | Fecha Elaboración | 09/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 02/11/2018 |

Tabla 36 -Cuadro de definición del contexto interno

| Criterio | Fuente | Detalle |
|---|---|---|
| Cultural | SUNASS | La Superintendencia Nacional de Servicios de Saneamiento tiene por finalidad garantizar a los usuarios la prestación de los servicios de saneamiento en las mejores condiciones de calidad, contribuyendo a la salud de la población y al mejoramiento del medio ambiente. |
| Normativo | Reglamento de prestación de servicios de agua potable y alcantarillado de la entidad prestadora de servicios de saneamiento de Lambayeque sociedad anónima EPSEL S.A. | ▪ Ley Orgánica de Municipalidades, Ley N° 27972.<br>▪ Ley de la Actividad Empresarial del Estado, Ley N° 24948.<br>▪ Ley General de sociedades, Ley N°26887.<br>▪ Ley General del Sistema Nacional de Presupuesto, Ley 28411.<br>▪ Plan Nacional de Saneamiento 2006 – 2015, D.S. N° 007 – 2006 – vivienda.<br>▪ Ley de Creación de la Superintendencia Nacional de Servicios de Saneamiento, Decreto Ley N° 25965.<br>▪ Ley General del Ambiente, Ley N° 28611.<br>▪ Ley General de Servicios de Saneamiento, Ley N° 26338 y su Reglamento.<br>▪ Estatutos de la empresa, reglamento aprobado por D.S N° 09-95-PRES vigente, se cambia la denominación de EMAPAL por el de EPSEL S.A integrando a las municipalidades distritales. |
| Partes Internas Involucradas | Personal administrativo | ▪ Medición.<br>▪ Facturación.<br>▪ Recaudación. |

| LOGO | Fase: 01 | Proceso: 01 | Actividad: -- | CÓDIGO DECIN° ___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Definición del contexto interno | | | | |
| **Objetivo:** Identificar los parámetros de fuente y detalle en cada criterio del contexto interno. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | LMOSCOSO | Fecha Elaboración | 09/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 02/11/2018 |

| Criterio | Fuente | Detalle |
|---|---|---|
| | | ▪ Atención al Cliente.<br>▪ Catastro y Conexiones.<br>▪ Micro medición. |
| Recursos | Servicios de Información | ▪ Proceso de medición.<br>▪ Proceso de facturación.<br>▪ Proceso de cobranza.<br>▪ Proceso de atención al cliente.<br>▪ Proceso de catastro y conexiones. |
| | Software | ▪ Ofimática.<br>▪ Sistema de gestión comercial.<br>▪ SICAP.<br>▪ Antivirus. |
| | Hardware | ▪ Impresoras.<br>▪ Equipo de trabajo.<br>▪ Ticketeras. |
| | Soporte de Información | ▪ Servidor Web.<br>▪ Servidor DNS.<br>▪ Servidor ISA.<br>▪ Modem.<br>▪ Servidor de base de datos.<br>▪ Switch. |
| Estructura | Organigrama | ▪ **Órganos de Dirección y Control**: Conformado por la Junta de Accionistas, el Directorio, la Gerencia General y el Órgano de Control Institucional.<br>▪ **Órganos Operativos**: Conformado por la Gerencia Operacional, Gerencia Comercial y Gerencia de Proyectos y Obras. Estas tres gerencias se encargas de los procesos de negocio de EPSEL S.A.<br>▪ **Órganos de Apoyo**: Conformado por la Gerencia de Administración y Finanzas, Oficina de Recursos Humanos, Oficina de |

<table>
<tr><td rowspan="2">LOGO</td><td>Fase: 01</td><td>Proceso: 01</td><td>Actividad: --</td><td rowspan="2">CÓDIGO<br>DECIN° ___</td><td rowspan="2">Pág. __ /____</td></tr>
<tr><td colspan="3">Definición del contexto interno</td></tr>
<tr><td colspan="4">Objetivo: Identificar los parámetros de fuente y detalle en cada criterio del contexto interno.</td><td>TIPO</td><td>TABLA</td></tr>
<tr><td>Actores</td><td>Gerencia Comercial<br>Equipo de Análisis</td><td>Elaborado Por:</td><td>LMOSCOSO</td><td>Fecha Elaboración</td><td>09/10/2017</td></tr>
<tr><td>Revisado Por:</td><td>JSEGURA</td><td>Aprobado Por:</td><td>JSEGURA</td><td>Fecha Aplicación</td><td>02/11/2018</td></tr>
</table>

| Criterio | Fuente | Detalle |
|---|---|---|
| | | Comunicación Social y la Oficina de Informática. Esta gerencia y las 3 oficinas están a cargo de la gestión administrativa y soporte del negocio.<br>▪ **Órganos de Asesoramiento y Asistencia Técnica**: Conformado por la Oficina de Asesoría Legal, Oficina de Desarrollo Empresarial y Oficina de Coordinación de Plan Maestro Optimizado. |
| **Metas y Objetivos** | Plan estratégico | ▪ **Misión**: Contribuir a mejorar la calidad de vida de la población de Lambayeque, brindando servicios de saneamiento eficientes y de calidad que ayuden a preservar el medio ambiente obteniendo niveles de rentabilidad que permitan su desarrollo empresarial y de su personal.<br>▪ **Visión**: Ser una organización eficiente, rentable, sólida, entre las más importantes del sector, con recursos humanos altamente capacitados que trabajen en equipo, actuando con permanente esfuerzo para lograr un crecimiento sostenible y brindar servicios de calidad orientados a la satisfacción del cliente.<br>▪ **Objetivo estratégicos:**<br>o Suministrar y mejorar y ampliar la cobertura de los servicios de agua potable y alcantarillado.<br>o Gestionar la calidad de los servicios de agua potable y alcantarillado.<br>o Lograr óptimos resultados económicos y financieros. |

| LOGO | Fase: 01 | Proceso: 01 | Actividad: -- | CÓDIGO DECIN° ___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Definición del contexto interno | | | | |
| Objetivo: Identificar los parámetros de fuente y detalle en cada criterio del contexto interno. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | LMOSCOSO | Fecha Elaboración | 09/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 02/11/2018 |

| Criterio | Fuente | Detalle |
|---|---|---|
| | | ○ Lograr una óptima gestión empresarial.<br>○ Fortalecer las competencias del talento humano. |
| Valores | Plan estratégico | ▪ **Trabajo en Equipo:** Unamos capacidades para alcanzar nuestros objetivos.<br>▪ **Honestidad:** Seamos honestos con nosotros mismos y con los demás.<br>▪ **Protección del Medio Ambiente:** Respeto a las leyes sobre salud pública y protección del Medio Ambiente.<br>▪ **Servicio de Calidad a los Clientes:** Porque sabemos que desean nuestros clientes, trabajamos para ellos.<br>▪ **Responsabilidad:** Asumamos los retos diarios y preparémonos para el futuro.<br>▪ **Respeto por la persona y dignidad humana:** Es nuestro compromiso social y responsabilidad de la Empresa. |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 01 | Proceso: 02 | Actividad: -- | CÓDIGO DECE N°__ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Definición del contexto externo | | | | |
| Objetivo: Identificar los parámetros de fuente y detalle en cada criterio del contexto externo. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial<br>Of. Comunicación Social<br>Equipo de análisis | Elaborado Por: | LMOSCOSO | Fecha Elaboración | 09/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 02/11/2017 |

Tabla 37– Cuadro de definición del contexto externo

| Criterio | Fuente Sugerida | Detalle |
|---|---|---|
| Ambiente del Negocio | Convenios | Convenio de operaciones reciprocas con las entidades del estado. |
| Normativo y Político | Portal de Transparencia de Epsel | ▪ Ley Orgánica de Municipalidades, Ley N° 27972.<br>▪ Ley de la Actividad Empresarial del Estado, Ley N° 24948.<br>▪ Ley General de sociedades, Ley N°26887.<br>▪ Ley General del Sistema Nacional de Presupuesto, Ley 28411.<br>▪ Plan Nacional de Saneamiento 2006 – 2015, D.S. N° 007 – 2006 – vivienda.<br>▪ Ley de Creación de la Superintendencia Nacional de Servicios de Saneamiento, Decreto Ley N° 25965.<br>▪ Ley General del Ambiente, Ley N° 28611.<br>▪ Ley General de Servicios de Saneamiento Ley N° 26338 y su Reglamento.<br>▪ Estatutos de la empresa, reglamento aprobado por D.S N° 09-95-PRES vigente, se cambia la denominación de EMAPAL por el de EPSEL S.A integrando a las municipalidades distritales. |
| | Portal Institucional de SUNASS | ▪ Resolución Directiva N ° 064.<br>▪ Resolución Directiva N° 011. |
| Financiero | Entidades financieras | ▪ Gobierno francés.<br>▪ Banco Continental.<br>▪ BCP.<br>▪ Interbank.<br>▪ Banco de la Nación. |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 01 | CÓDIGO IDAC AD N°__ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de activos críticos de la alta dirección | | | | |
| **Objetivo:** Definir qué activos son críticos para la organización, que de verse afectados se produzca un impacto negativo en la operación de los procesos de gestión comercial, desde el punto de vista de la alta dirección. | | | | TIPO | TABLA |
| **Actores** | Gerencia comercial Equipo de análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 09/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/11/2017 |

Tabla 38– Cuadro de identificación de activos críticos de la alta dirección

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| N°1 | S_PM | Servicios de Información | Proceso de Medición | Proceso de toma y registro de lecturas, cálculo de consumo de conexiones que usan medidor y crítica de lecturas de acuerdo a la normatividad vigente. |
| | S_PF | Servicios de Información | Proceso de Facturación | Proceso de cálculo de montos por los servicios de agua y alcantarillado de acuerdo a los consumos registrados en el proceso de medición y a la tarifa establecida para cada conexión, así como otros cargos a facturar (cuotas de convenio, intereses, cortes y rehabilitaciones, etc.). |
| | S_PC | Servicios de Información | Proceso de Cobranza | Proceso que contempla los subprocesos de recaudación y acciones de cobranza (cortes y rehabilitaciones). |
| | S_PAT | Servicios de Información | Proceso de Atención al Cliente | Proceso de atención al cliente que contempla acciones de atención de reclamos, servicios colaterales y consultas. |
| | S_CC | Servicios de Información | Proceso de Catastro y Conexiones | Proceso de registro y actualización de datos de ubicación y características de la conexión. |
| | SW_SGC | Software | Sistema de Gestión Comercial | Sistema de gestión comercial SICDESA, que automatiza todos los procesos comerciales. |
| | SI_SBD | Soporte de Información | Servidor de Base de Datos | Servidor que contiene el programa que gestiona la base de datos que almacena toda la información comercial. |

Fuente: Propia

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 02 | CÓDIGO IAAC AD N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de amenaza por activo crítico de la alta dirección | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar los activos críticos desde el punto de vista de la alta dirección. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 10/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 08/11/2017 |

Tabla 39- Cuadro de identificación amenaza por activo de la alta dirección

| Proceso | Código | Activo Crítico | Situación de Amenaza |
|---|---|---|---|
| N°1 | S_PM | Proceso de Medición | Tiempo insuficiente para ejecutar el proceso (Alta rotación de personal, Carencia de mano de obra operativa capacitada, Lentitud en el procesamiento de la información en el sistema comercial).<br>Manipulación de la información. |
| | S_PF | Proceso de Facturación | Modificaciones de la normativa vigente.<br>Restricción de tiempo de servicio y presión.<br>Agua no facturada. |
| | S_PC | Proceso de Cobranza | Actos mal intencionados por parte del personal.<br>Informalidad de pago. |
| | S_PAT | Proceso de Atención al Cliente | Altos niveles de llegada de clientes en fechas específicas.<br>Brindar información errada (afecta a la imagen institucional).<br>Escape de información.<br>Manipulación de la información. |
| | S_CC | Proceso de Catastro y Conexiones | Conexiones clandestinas.<br>Manipulación de la información.<br>Alteración de la información. |
| | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegio de acceso.<br>Inconsistencia de registro de información. |
| | SI_SBD | Servidor de Base de Datos | Modificación de la información.<br>Caída del servicio por agotamiento de recurso. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 03 | CÓDIGO DRSA AD N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista de la alta dirección. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 10/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 08/11/2017 |

Tabla 40-Cuadro de requisito de seguridad por activo crítico de la alta dirección

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_PM | La información de la evolución de los consumos solo debe estar a disposición del personal autorizado. | La determinación de los consumos facturados debe guardar coherencia y ajustarse a la normatividad vigente. | La información de evolución de consumos debe estar a disposición para la toma de decisiones. | 15% de la jornada laboral | 35% de la jornada laboral |
| S_PF | La información relacionada a la evolución de los montos facturados y su distribución tarifaria y geográfica solo debe ser accesada por el personal que toma de decisiones en relación a este proceso. | La información relacionada al proceso de facturación debe ser coherente mes a mes para poder tomar las decisiones pertinentes. | La información requerida y generada en este proceso debe estar siempre a disposición de las gerencias y personal que toma decisiones. | 1% de la jornada laboral | 10% de la jornada laboral |
| S_PC | La información de gestión relacionada a la cobranza y saldos pendientes de pago solo debe ser accedida por el personal encargado de la toma de decisiones. | La emisión e interpretación de la información generada en la operación de este proceso debe ser coherente y estar de acuerdo a las normas y directivas de la empresa. | La información requerida y generada en este proceso debe estar siempre a disposición de las gerencias y personal que toma decisiones. | 10% de la jornada laboral | 25% de la jornada laboral |

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 03 | CÓDIGO DRSA AD N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista de la alta dirección. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 10/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 08/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_PAT | La información de gestión generada durante este proceso debe ser accesada solo por las partes interesadas, evitando la fuga de información a personal no autorizado. | Es importante la consistencia de la información generada durante el proceso de atención al cliente, ya que en base a esta se generan las estrategias de acción respecto a la problemática del área o a los indicadores de incremento de conexión o cantidad de reclamos. | Cumplir con la ejecución de los procesos de acuerdo a las normativas y directivas vigentes, contando la disposición de la información cuando sea necesaria para la toma de decisiones pertinente. | 25% de la jornada laboral | 50% de la jornada laboral |
| S_CC | La información de gestión relacionada a las características de la conexión, tarifas, tipos de servicio, debe estar a disposición del personal autorizado. | Es importarte que la información gestionada en los procesos de catastro y conexiones guarde coherencia y se ajuste a la realidad en campo, por lo cual debe estar constantemente supervisada. | La información de gestión procesada por catastro y conexiones debe estar disponible para la toma de decisiones. | 25% de la jornada laboral | 50% de la jornada laboral |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 02 | Proceso: 01 | Actividad: 04 | CÓDIGO IEOA AD N°____ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de estrategias de protección y vulnerabilidades organizacionales por activo crítico de la alta dirección | | | | |
| **Objetivo:** Identificar cuáles son las estrategias de protección actuales desde el punto de alta dirección. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 10/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 08/11/2017 |

Tabla 41- Cuadro de estrategias de protección y vulnerabilidades organizacionales por activo de la alta dirección

| Código Activo | Activo | Estrategias Actuales de protección |
|---|---|---|
| S_PM | Proceso de Medición | Muestreo de padrones de toma de lectura. |
| S_PF | Proceso de Facturación | Muestreo de recibos facturados. |
| S_PC | Proceso de Cobranza | Supervisión de acciones de corte y rehabilitación programadas. |
| S_PAT | Proceso de Atención al Cliente | Ninguna. |
| S_CC | Proceso de Catastro y Conexiones | Ninguna. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 01 | CÓDIGO IDAC GO N° ___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de activos críticos en el área de gestión operativa | | | | |
| **Objetivo:** Definir qué activos son críticos para la organización, que de verse afectados se produzca un impacto negativo en la operación de los procesos de gestión comercial, desde el punto de vista de los gestores operativos comerciales. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 11/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 09/11/2017 |

Tabla 42- Cuadro de identificación de activos importantes en el área de gestión operativa

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| N°2 | S_PM | Servicios de Información | Proceso de Medición | Proceso de toma y registro de lecturas, cálculo de consumo de conexiones que usan medidor y crítica de lecturas de acuerdo a la normatividad vigente. |
| | S_PF | Servicios de Información | Proceso de Facturación | Proceso de cálculo de montos por los servicios de agua y alcantarillado de acuerdo a los consumos registrados en el proceso de medición y a la tarifa establecida para cada conexión, así como otros cargos a facturar (cuotas de convenio, intereses, cortes y rehabilitaciones, etc.). |
| | S_PC | Servicios de Información | Proceso de Cobranza | Proceso que contempla los subprocesos de recaudación y acciones de cobranza (cortes y rehabilitaciones). |
| | S_PAT | Servicios de Información | Proceso de Atención al Cliente | Proceso de atención al cliente que contempla acciones de atención de reclamos, servicios colaterales y consultas. |
| | S_CC | Servicios de | Proceso de | Proceso de registro y |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 01 | CÓDIGO IDAC GO N° ___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de activos críticos en el área de gestión operativa | | | | |
| **Objetivo:** Definir qué activos son críticos para la organización, que de verse afectados se produzca un impacto negativo en la operación de los procesos de gestión comercial, desde el punto de vista de los gestores operativos comerciales. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 11/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 09/11/2017 |

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| | | Información | Catastro y Conexiones | actualización de datos de ubicación y características de la conexión. |
| | SW_SGC | Software | Sistema de Gestión Comercial. | Sistema de gestión comercial SICDESA, que automatiza todos los procesos comerciales. |
| | SI_SBD | Soporte de Información | Servidor de Base de Datos | Servidor que contiene el programa que gestiona la base de datos que almacena toda la información comercial |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 03 | CÓDIGO IAAC GO N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de amenazas por activo crítico por la gestión operativa | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde de punto de vista de los gestores operativos. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 11/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 09/11/2017 |

Tabla 43- Cuadro de identificación amenaza por activo en el área de gestión operativa

| Proceso | Código | Activo Crítico | Situación de Amenaza |
|---|---|---|---|
| N°1 | S_PM | Proceso de Medición | Tiempo insuficiente para ejecutar el proceso.<br>Error de toma de lectura en campo.<br>Errores en la aplicación de la normatividad vigente.<br>Constantes fallas eléctricas.<br>Pérdida de comunicación con la sede central.<br>Caída del servicio de internet.<br>Manipulación de la información. |
| | S_PF | Proceso de Facturación | Modificaciones de la normativa vigente.<br>Restricción de tiempo de servicio y presión.<br>Fallas eléctricas.<br>Errores de distribución (Carencia de personal capacitado). |
| | S_PC | Proceso de Cobranza | Actos mal intencionados por parte del personal.<br>Centros de pago no autorizados.<br>Sobrecarga de clientes por temporadas.<br>Envió de información de cobranza en bancos fuera de tiempo.<br>Fallos eléctricos. |
| | S_PAT | Proceso de Atención al Cliente | Altos niveles de llegada de clientes en fechas específicas.<br>Brindar información errada (afecta a la imagen institucional).<br>Escape de información.<br>Manipulación de la información. |
| | S_CC | Proceso de Catastro y Conexiones | Suplantación de identidad.<br>Manipulación de la información. |
| | SW_SGC | Sistema de Gestión Comercial. | Acceso no autorizado.<br>Errores de configuración.<br>Errores de monitorización.<br>Errores de mantenimiento.<br>Fallas en el proceso de calidad.<br>Indisponibilidad del personal.<br>Suplantación de Identidad.<br>Abuso de privilegio de acceso.<br>Inconsistencia de registro de información. |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 03 | CÓDIGO IAAC GO N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de amenazas por activo crítico por la gestión operativa | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde de punto de vista de los gestores operativos. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 11/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 09/11/2017 |

| Proceso | Código | Activo Crítico | Situación de Amenaza |
|---|---|---|---|
| | | | Análisis de tráfico.<br>Caída de servicio por agotamiento de recursos. |
| | SI_SBD | Servidor de Base de Datos | Modificación de la información.<br>Corrupción de la información.<br>Destrucción de información.<br>Intercepción de información.<br>No contar con la información confiable, integra y disponible. |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 03 | CÓDIGO IAAC GO N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de amenazas por activo crítico por la gestión operativa | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde de punto de vista de los gestores operativos. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 11/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 09/11/2017 |

Tabla 44- Cuadro de requisito de seguridad por activo crítico en el área de gestión operativa

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_PM | La información de los padrones de lectura solo sea debe ser accedido por el personal autorizado. | El cálculo del consumo a facturar es la base de todo el ciclo comercial, por esto debe estar acorde a las normas vigentes y no debe sufrir alteraciones. | Durante el ciclo de comercial, la información relacionada a consumo y lecturas debe estar disponible para las acciones de seguimiento y control que correspondan. | 15% de la jornada laboral | 35% de la jornada laboral |
| S_PF | Solo el personal autorizado debe tener información a los importes facturados de la empresa debido a que esta información es susceptible a ser utilizada para fraude. | La información de entrada a este proceso (consumos, conexiones, tarifas) debe ser consistente. | La información de facturación debe estar siempre disponible tanto para los usuarios internos como para los externos. | 1% de la jornada laboral | 10% de la jornada laboral |
| S_PC | Evitar la fuga de información de saldos porque esta puede ser mal utilizada. | Es importante que la información de saldos pendientes se coherente y no presente problemas que conlleven a la ejecución de acciones de cobranza erradas. | La información relacionada a saldos pendientes de cobranza debe estar siempre disponible para no detener el flujo de ingreso de dinero a caja. | 10% de la jornada laboral | 25% de la jornada laboral |
| S_PAT | Esta información debe ser accedida solo por el personal autorizado de acuerdo a las funciones que le competan. | Para gestionar correctamente la información generada por este proceso se debe asegurar que los datos registrados sean coherentes con lo solicitado por el cliente. | El proceso de atención al cliente está normado por el ente regulador SUNASS que exige plazos de atención cuyo cumplimiento depende de que la información esté disponible de manera constante. | 25% de la jornada laboral | 50% de la jornada laboral |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 03 | CÓDIGO IAAC GO N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de amenazas por activo crítico por la gestión operativa | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde de punto de vista de los gestores operativos. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 11/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 09/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_CC | Esta información debe ser accedida solo por el personal autorizado de acuerdo a las funciones que le competan. | Para gestionar correctamente la información generada por este proceso se debe asegurar que los datos registrados sean coherentes los que se cuentan en campo. | La información generada por este proceso es la base de todo el ciclo de gestión comercial por esta razón es necesario que la información esté disponible de manera constante. | 25% de la jornada laboral | 50% de la jornada laboral |
| SW_SGC | La información de Sistema de gestión de comercial, solo debe ser accedida para los perfiles configurados.<br>3. Acceso no autorizado de los usuarios. | El procesamiento de la información debe ser veraz por que será utilizada para otros procesos. | La información debe estar disponible, porque servirá de apoyo para en los demás procesos de cobranzas, facturación y asegurar la continuidad. | 1% de la jornada laboral<br>70% de equipos instalados | 10% de la jornada laboral<br>50% de equipos instalados |
| SI_SBD | El acceso al servidor de base de datos debe ser por personal autorizado. | La información que se registrara en la base de datos debe estar bien digitada y veraz, para brindar información integra. | La disponibilidad del servidor de base de datos es importante, para poder realizar todos los procesos de la EPS asegurando la continuidad del negocio. | 1% de la jornada laboral | 10% de la jornada laboral |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 02 | Proceso: 02 | Actividad: 04 | CÓDIGO IEOA GO N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Estrategias de protección y vulnerabilidades organizacionales por activo en el área de gestión operativa | | | | |
| **Objetivo:** Identificar cuáles son las estrategias actuales de protección desde el punto de vista de los gestores operativos. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 11/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 14/11/2017 |

Tabla 45- Cuadro de estrategias de protección y vulnerabilidades organizacionales por activo en el área de gestión operativa

| Código de Activo | Activo | Estrategias Actuales de protección |
|---|---|---|
| S_PM | Proceso de Medición | Muestreo de padrones de toma de lectura. |
| S_PF | Proceso de Facturación | Muestreo de recibos facturados. |
| S_PC | Proceso de Cobranza | Supervisión de acciones de corte y rehabilitación programadas. |
| S_PAT | Proceso de Atención al Cliente | Ninguna. |
| S_CC | Proceso de Catastro y Conexiones | Ninguna. |
| SW_SGC | Sistema de Gestión Comercial | Tablas de auditoría. |
| SI_SBD | Servidor de Base de Datos | Copias de seguridad diaria y semanal. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 01 | CÓDIGO IDAC PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de Activos Críticos del Personal | | | | |
| **Objetivo:** Identificar los activos críticos desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 16/11/2017 |

Tabla 46- Cuadro de identificación de activos críticos del personal

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| N°3 | S_PM | Servicios de Información | Proceso de Medición | Proceso de toma y registro de lecturas, cálculo de consumo de conexiones que usan medidor y crítica de lecturas de acuerdo a la normatividad vigente. |
| | S_PF | Servicios de Información | Proceso de Facturación | Proceso de cálculo de montos por los servicios de agua y alcantarillado acuerdo a los consumos registrados en el proceso de medición y a la tarifa establecida para cada conexión, así como otros cargos a facturar (cuotas de convenio, intereses, cortes y rehabilitaciones, etc.) |
| | S_PC | Servicios de Información | Proceso de Cobranza | Proceso que contempla los subprocesos de recaudación y acciones de cobranza (cortes y rehabilitaciones) |
| | S_PAT | Servicios de Información | Proceso de Atención al Cliente | Proceso de atención al cliente que contempla acciones de atención de reclamos, servicios colaterales y consultas. |
| | S_CC | Servicios de Información | Proceso de Catastro y Conexiones | Proceso de registro y actualización de datos de ubicación y características de la conexión. |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 01 | CÓDIGO IDAC PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de Activos Críticos del Personal | | | | |
| **Objetivo:** Identificar los activos críticos desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 16/11/2017 |

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| | SW_SGC | Software | Sistema de Gestión Comercial | Sistema de gestión comercial SICDESA, que automatiza todos los procesos comerciales. |
| | SW_SICAP | Software | SICAP | Sistema de Captura de Datos para que las EPS ingresen, entre otra información periódica, las variables de gestión. |
| | SW_OFI | Software | Ofimática | Software para procesamiento de textos y hojas de cálculo (Ms Office, StartOffice, OpenOffice). |
| | SW_AV | Software | Antivirus | Software para detectar o eliminar virus informáticos. |
| | HW_IMP | Hardware | Impresoras | Dispositivo periférico para impresión de formatos, reportes, documentos. |
| | HW_PC | Hardware | Estación de Trabajo | Computadora personal. |
| | HW_LBAR | Hardware | Ticketeras | Dispositivo periférico para impresión de refrendo de pago. |
| | SI_SWEB | Soporte de Información | Servidor Web | Servidor configurado para alojar la página web y los sistemas bajo este formato. |
| | SI_SDNS | Soporte de Información | Servidor DNS | Servidor que contiene la configuración del dominio y traduce nombres de dominio a IPs y viceversa. |
| | SI_SISA | Soporte de Información | Servidor ISA | Servidor que contiene el firewall y la configuración de las políticas de acceso a |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 01 | CÓDIGO IDAC PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de Activos Críticos del Personal | | | | |
| **Objetivo:** Identificar los activos críticos desde el punto de vista del personal. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 12/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 16/11/2017 |

| Proceso | Código | Categoría | Activo Crítico | Descripción |
|---|---|---|---|---|
| | | | | internet. |
| | SI_MODEM | Soporte de Información | Modem | Dispositivo que recibe el servicio de internet de la empresa a cargo. |
| | SI_SWITCH | Soporte de Información | Switch | Dispositivo para la conexión de red. |
| | SI_SBD | Soporte de Información | Servidor de Base de Datos | Servidor que contiene el programa que gestiona la base de datos que almacena toda la información comercial. |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 02 | CÓDIGO IAAC PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de Amenaza por Activos Críticos del Personal | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde el punto de vista del personal. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 16/11/2017 |

Tabla 47- Cuadro de identificación amenaza por activo del personal

| Proceso | Código | Activo Crítico | Situación de Amenaza |
|---|---|---|---|
| N°1 | S_PM | Proceso de Medición | Tiempo insuficiente para ejecutar el proceso (Alta rotación de personal, carencia de mano de obra operativa capacitada, lentitud en el procesamiento de la información en el sistema comercial).<br>Error de toma de lectura en campo.<br>Errores de digitación.<br>Errores en la aplicación de la normatividad vigente.<br>Constantes fallas eléctricas.<br>Pérdida de comunicación con la sede central.<br>Caída del servicio de internet.<br>Manipulación de la información. |
| | S_PF | Proceso de Facturación | Modificaciones de la normativa vigente.<br>Restricción de tiempo de servicio y presión<br>Fallas eléctricas.<br>Error al imprimir el recibo generado.<br>Errores de distribución (Carencia de personal capacitado). |
| | S_PC | Proceso de Cobranza | Actos mal intencionados por parte del personal.<br>Centros de pago no autorizados.<br>Sobrecarga de clientes por temporadas.<br>Envío de información de cobranza en bancos Fuera de tiempo.<br>Fallos eléctricos.<br>Pago con billetes falsos (equipos insuficientes). |
| | S_PAT | Proceso de Atención al Cliente | Altos niveles de llegada de clientes en fechas específicas.<br>Error de digitación.<br>Brindar información errada (afecta a la imagen institucional).<br>Escape de información.<br>Manipulación de la información. |
| | S_CC | Proceso de Catastro y Conexiones | Suplantación de identidad.<br>Errores en el registro de la información.<br>Error en la toma de información en campo. |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 02 | CÓDIGO IAAC PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de Amenaza por Activos Críticos del Personal | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde el punto de vista del personal. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 16/11/2017 |

| Proceso | Código | Activo Crítico | Situación de Amenaza |
|---|---|---|---|
| | | | (Carencia de personal capacitado).<br>Manipulación de la información. |
| | SW_SGC | Sistema de Gestión Comercial | Acceso no autorizado.<br>Errores de configuración.<br>Errores de registro.<br>Errores de monitorización.<br>Errores de mantenimiento.<br>Fallas en el proceso de calidad.<br>Indisponibilidad del personal.<br>Suplantación de Identidad.<br>Abuso de privilegio de acceso.<br>Inconsistencia de registro de información.<br>Análisis de tráfico.<br>Caída de servicio por agotamiento de recursos. |
| | SW_SICAP | SICAP | Sin acceso a código fuente. |
| | SW_OFI | Ofimática | Software no autorizado. |
| | SW_AV | Antivirus | Difusión de software dañino. |
| | HW_IMP | Impresoras | Fluctuaciones de energía.<br>Manipulación del equipo.<br>Falla de equipo.<br>Errores en programas de mantenimiento preventivo.<br>Carencia de insumos. |
| | HW_PC | Estación de Trabajo | Fluctuaciones de energía.<br>Manipulación del equipo.<br>Falla de equipo.<br>Errores en programas de mantenimiento preventivo. |
| | HW_LBAR | Ticketeras | Fluctuaciones de energía.<br>Manipulación del equipo.<br>Carencia de insumos. |
| | SI_SWEB | Servidor Web | Caídas del servicio de la página web. |
| | SI_SDNS | Servidor DNS | Falta de acceso a algunas páginas. |
| | SI_SISA | Servidor ISA | Pocas políticas de acceso a las páginas web. |
| | SI_MODEM | Modem | La constante intermitencia para el acceso en las páginas web. |
| | SI_SWITCH | Switch | Falla en la transmisión de datos. Los paquetes |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 02 | CÓDIGO IAAC PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de Amenaza por Activos Críticos del Personal | | | | |
| **Objetivo:** Determinar que situaciones pueden amenazar a los activos críticos desde el punto de vista del personal. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 16/11/2017 |

| Proceso | Código | Activo Crítico | Situación de Amenaza |
|---|---|---|---|
| | | | de información lleguen alterados. |
| | SI_SBD | Servidor de Base de Datos | Modificación de la información.<br>Corrupción de la información.<br>Destrucción de información.<br>Intercepción de información.<br>No contar con la información confiable, íntegra y disponible.<br>Fallas eléctricas.<br>Errores de configuración. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 03 | CÓDIGO DRSAPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico del personal | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 20/11/2017 |

Tabla 48- Cuadro de requisito de seguridad por activo crítico del personal

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_PM | El registro de lecturas durante los procesos de toma y crítica deber realizado solo por personal autorizado y supervisado por la jefatura correspondiente. | El registro de lecturas sea por el proceso de toma o crítica debe estar de acorde a la información obtenida en campo y se debe determinar el consumo a facturar respetando la normatividad vigente. | Es importante tener siempre disponible esta información porque permite la resolución de reclamos, y es la base del proceso de facturación. | 15% de la jornada laboral | 35% de la jornada laboral |
| S_PF | Se deben manejar niveles de accesos a esta información desde los diversos procesos comerciales, es importante que solo el personal autorizado acceda a esta. | Generar información de facturación exacta y sin problemas de consistencia, permite evitar reclamos o errores en los procesos subsecuentes. Esta información es declarada ante SUNASS y SUNAT y algún problema de consistencia podría generar multas económicas que afecten a la empresa. | Los importes facturados deben estar disponibles durante todo el ciclo comercial ya que son base de los procesos de cobranzas y atención al cliente. | 1% de la jornada laboral | 10% de la jornada laboral |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 03 | CÓDIGO DRSAPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico del personal | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 20/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_PC | Supervisar y controlar continuamente el acceso a la información de saldos por cobrar y pagos, el acceso no autorizado a este proceso puede generar inconsistencias o tergiversar el resultado de la gestión empresarial. | Evitar errores de digitación y procesamiento de la información debido a que errores de esta índole afectan económicamente a la empresa. | Es importante tener acceso continuo a la información de saldos para poder ejecutar los procesos de cobranza y acciones de cobranza a usuarios morosos. | 10% de la jornada laboral | 25% de la jornada laboral |
| S_PAT | El acceso a la información debe ser controlado y dado solo al personal autorizado o al cliente que lo solicite. Es importante controlar las fugas de información y corroborar el correcto procesamiento de la información. | Es importante supervisar y controlar el correcto registro de información en la operación de este proceso ya de que de este depende cómo nacerá o actualizará los datos de la conexión. | Es necesario que esta información esté disponible para hacer seguimiento desde los diferentes procesos que la requieran para cumplir con los plazos estipulados por la normatividad vigente y de esta forma evitar las diferentes multas que el incumplimiento de esto plazos acarrean. | 25% de la jornada laboral | 50% de la jornada laboral |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 03 | CÓDIGO DRSAPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico del personal | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 20/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| S_CC | La información generada en este proceso es altamente susceptible a ser utilizada con fines ajenos a los objetivos de la empresa y el acceso a ésta debe ser controlado y otorgado solo al personal autorizado. Es importante controlar las fugas de información y corroborar el correcto procesamiento de la información. | La información generada en este proceso es altamente susceptible y el resto de procesos dependen de su correcto procesamiento, por tal motivo es de vital importancia controlar la integridad y coherencia de esta. | La información generada en este proceso es indispensable para los demás procesos del ciclo comercial siendo indispensable que esté disponible constantemente durante todo el proceso. | 25% de la jornada laboral | 50% de la jornada laboral |
| SW_SGC | Acceso no autorizado de los usuarios. | El procesamiento de la información debe ser veraz por que será utilizada para otros procesos. | La información debe estar disponible, porque servirá de apoyo para en los demás procesos de cobranzas, facturación y asegurar la continuidad. | 1% de la jornada laboral<br>70% de equipos instalados | 10% de la jornada laboral<br>50% de equipos instalados |
| SW_SICAP | Acceso no autorizado. | La configuración en el SICAP debe ser correcta, porque puede genera una multa | La disponibilidad de la información del SICAP debe estar disponible, ya que por falta | 25% de la jornada laboral<br>70% de equipos instalados | 50% de la jornada laboral<br>40% de equipos instalados |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 03 | CÓDIGO DRSAPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico del personal | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 20/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| | | a la EPS | de información podría la EPS tener una multa. | | |
| **SW_OFI** | Se controlan la propiedad de los documentos de los usuarios. | Configuración adecuada para asegurar la integridad de la información almacenada | Es necesario la disponibilidad para la gestión informática de documentos, hojas de cálculos | 25% de la jornada laboral<br>70% de equipos instalados | 50% de la jornada laboral<br>40% de equipos instalados |
| **SW_AV** | Personal autorizado en la configuración de antivirus. | Configuración adecuada del antivirus para proteger y asegurar la integridad de la información de los sistemas | La disponibilidad del antivirus es importante para no dañar archivos que son esenciales para los demás áreas. | 90% de equipos instalados | 70% de equipos instalados |
| **HW_IMP** | Ubicación adecuada. | Configuración adecuada para mostrar la información correcta que envió al imprimir | La disponibilidad de este activo es importante para poder imprimir la información de los recibos facturados enviaran a los clientes. | 80% de equipos operativos | 60% de equipos operativos |
| **HW_PC** | La configuración de cada estación de trabajo deben estar bien configurados sus accesos de manera que los usuarios puedan acceder a su información de forma segura y evitar fuga de información. | Asegurar la configuración adecuada en las computadoras, y así no presentar interrupciones que perjudiquen al momento de mostrar información que el usuario requiera. | La disponibilidad de la estación de trabajo es importante para poder generar la información requerida en las áreas. | 95% de equipos operativos | 85% de equipos operativos |
| **HW_LBAR** | Acceso de personal no adecuado. | La impresión debe estar la información enviada. | Tiene que estar disponible en los momentos de impresiones de | 60% de equipos operativos | 40% de equipos operativos |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 03 | CÓDIGO DRSAPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico del personal | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 20/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| | | | refrendos. | | |
| **SI_SWEB** | Solo personal autorizado puede tener acceso al servidor DCHP Ubicación adecuada. | La página web debe mostrarse según como este configurado el servidor web. | Asegurar que la página web de la EPS se encuentre disponible. | 3 horas fuera de línea | 8 horas fuera de línea |
| **SI_SDNS** | Personal no autorizado. | Las estaciones de trabajo funcionaran de acuerdo a la configuración del servidor DNS. | El servidor de dominios debe estar disponible a través de su configuración adecuada. | 1% de la jornada laboral | 10% de la jornada laboral |
| **SI_SISA** | Acceso de personal autorizado. | La seguridad página web debe trabajar según como se ha configurado el servidor ISA. | La configuración del ISA server ayudara tener disponible los servicios. | 1% de la jornada laboral | 10% de la jornada laboral |
| **SI_MODEM** | Ubicación adecuada. | Configuración adecuada para poder comunicarse y mostrar la información correcta. | Configuración adecuada para la disponibilidad de los equipos de procesos core y además asegurar la comunicación con las demás EPS. | 1% de la jornada laboral | 10% de la jornada laboral |
| **SI_SWITCH** | Acceso de personal autorizado. Distribución y configuración de los puntos de red por el personal autorizado. Ubicación adecuada. | Configuración adecuada para poder comunicarse y mostrar la información correcta. | Configuración adecuada para la disponibilidad de los equipos de procesos core. | 1% de la jornada laboral | 10% de la jornada laboral |
| **SI_SBD** | El acceso al servidor de base de datos debe ser por personal | La información que se registra en la base de datos debe estar bien | La disponibilidad del servidor de base de datos, es importante, para | 1% de la jornada laboral | 10% de la jornada laboral |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 03 | CÓDIGO DRSAPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación de requisitos de seguridad por activo crítico del personal | | | | |
| **Objetivo:** Definir los requerimientos de seguridad de los activos críticos en base a los criterios de continuidad, integridad y disponibilidad de la información desde el punto de vista del personal. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 12/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 20/11/2017 |

| Activo Crítico | Confidencialidad | Integridad | Disponibilidad | Apetito | Tolerancia |
|---|---|---|---|---|---|
| | autorizado. | digitada y veraz, para brindar información integra. | poder realizar todos los procesos de la EPS asegurando la continuidad del negocio. | | |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 02 | Proceso: 03 | Actividad: 04 | CÓDIGO IEOA PE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de estrategias de protección y vulnerabilidades organizacionales por activo crítico del personal | | | | |
| **Objetivo:** Identificar cuáles son las estrategias actuales de protección desde el punto del personal. | | | | **TIPO** | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 14/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 21/11/2017 |

Tabla 49- Cuadro de estrategias de protección y vulnerabilidades organizacionales por activo del personal

| Código de Activo | Activo | Estrategias Actuales de protección |
|---|---|---|
| S_PM | Proceso de Medición | Muestreo de padrones de toma de lectura. |
| S_PF | Proceso de Facturación | Muestreo de recibos facturados. |
| S_PC | Proceso de Cobranza | Supervisión de acciones de corte y rehabilitación programadas. |
| S_PAT | Proceso de Atención al Cliente | Ninguna. |
| S_CC | Proceso de Catastro y Conexiones | Ninguna. |
| SW_SGC | Sistema de Gestión Comercial | Tablas de auditoría. |
| SW_SICAP | SICAP | Ninguna. |
| SW_OFI | Ofimática | Ninguna. |
| SW_AV | Antivirus | Actualización automática de bases de firmas de antivirus. |
| HW_IMP | Impresoras | Mantenimiento preventivo. |
| HW_PC | Estación de Trabajo | Mantenimiento preventivo. |
| HW_LBAR | Ticketeras | Ninguna. |
| SI_SWEB | Servidor Web | Ninguna. |
| SI_SDNS | Servidor DNS | Ninguna. |
| SI_SISA | Servidor ISA | Ninguna. |
| SI_MODEM | Modem | Ninguna. |
| SI_SWITCH | Switch | Ninguna. |
| SI_SBD | Servidor de Base de Datos | Copias de seguridad diaria y semanal. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 01 | CÓDIGO POAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ponderación de activos críticos | | | | |
| **Objetivo:** Ponderar y priorizar la gestión de activos más críticos. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 15/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 21/11/2017 |

Tabla 50- Cuadro de ponderación de activos

| | | | Puntuación | | | | |
|---|---|---|---|---|---|---|---|
| Código | Categoría | Activo importante | Dirección | Operativa | Personal | Gestor de Riesgo | Promedio |
| S_PM | Servicios de Información | Proceso de Medición | 5 | 5 | 4 | 4 | 4.5 |
| S_PF | Servicios de Información | Proceso de Facturación | 5 | 5 | 4 | 5 | 4.75 |
| S_PC | Servicios de Información | Proceso de Cobranza | 5 | 5 | 4 | 5 | 4.75 |
| S_PAT | Servicios de Información | Proceso de Atención al Cliente | 3 | 3 | 3 | 4 | 3.25 |
| S_CC | Servicios de Información | Proceso de Catastro y Conexiones | 4 | 4 | 3 | 5 | 4 |
| SW_SGC | Software | Sistema de Gestión Comercial | 5 | 5 | 5 | 5 | 5 |
| SW_SICAP | Software | SICAP | 2 | 3 | 1 | 3 | 2.25 |
| SW_OFI | Software | Ofimática | 1 | 2 | 1 | 2 | 1.5 |
| SW_AV | Software | Antivirus | 2 | 3 | 3 | 3 | 2.75 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 01 | CÓDIGO POAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ponderación de activos críticos | | | | |
| **Objetivo:** Ponderar y priorizar la gestión de activos más críticos. | | | | TIPO | TABLA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 15/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 21/11/2017 |

| | | | Puntuación | | | | |
|---|---|---|---|---|---|---|---|
| Código | Categoría | Activo importante | Dirección | Operativa | Personal | Gestor de Riesgo | Promedio |
| HW_IMP | Hardware | Impresoras | 4 | 5 | 4 | 3 | 4 |
| HW_PC | Hardware | Estación de Trabajo | 5 | 5 | 5 | 5 | 5 |
| HW_LBAR | Hardware | Ticketeras | 1 | 2 | 2 | 3 | 2 |
| SI_SWEB | Soporte de Información | Servidor Web | 3 | 3 | 3 | 2 | 2.75 |
| SI_SDNS | Soporte de Información | Servidor DNS | 2 | 3 | 4 | 2 | 2.75 |
| SI_SISA | Soporte de Información | Servidor ISA | 2 | 3 | 3 | 3 | 2.75 |
| SI_MODEM | Soporte de Información | Modem | 2 | 2 | 3 | 3 | 2.5 |
| SI_SWITCH | Soporte de Información | Switch | 3 | 3 | 5 | 5 | 4 |
| SI_SBD | Soporte de Información | Servidor de Base de Datos | 5 | 5 | 5 | 5 | 5 |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 02 | CÓDIGO LCAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de clasificación de activos críticos | | | | |
| **Objetivo:** Clasificar los activos de acuerdo a las categorías establecidas. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | LMOSCOSO | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 22/11/2017 |

Tabla 51- Cuadro de clasificación de activos

| Ítem | Activos | Código | Categoría | | | |
|---|---|---|---|---|---|---|
| | | | [S] | [SW] | [HW] | [SI] |
| 1 | Proceso de Medición | [S_PM] | X | | | |
| 2 | Proceso de Facturación | [S_PF] | X | | | |
| 3 | Proceso de Cobranza | [S_PC] | X | | | |
| 4 | Proceso de Atención al Cliente | [S_PAT] | X | | | |
| 5 | Proceso de Catastro y Conexiones | [S_CC] | X | | | |
| 6 | Sistema de Gestión Comercial | [SW_SGC] | | X | | |
| 7 | SICAP | [SW_SICAP] | | X | | |
| 8 | Ofimática | [SW_OFIMATICA] | | X | | |
| 9 | Antivirus | [SW_ANTIVIRUS] | | X | | |
| 10 | Impresoras | [HW_IMP] | | | X | |
| 11 | Estación de Trabajo | [HW_PC] | | | X | |
| 12 | Ticketeras / Lectoras de código de barras | [HW_TLCB] | | | X | |
| 13 | Servidor Web | [SI_SWEB] | | | | X |
| 14 | Servidor DNS | [SI_SDNS] | | | | X |
| 15 | Servidor ISA | [SI_ISA] | | | | X |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 02 | CÓDIGO LCAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de clasificación de activos críticos | | | | |
| **Objetivo:** Clasificar los activos de acuerdo a las categorías establecidas. | | | | TIPO | TABLA |
| **Actores** | Gerencia Comercial Equipo de Análisis | **Elaborado Por:** | LMOSCOSO | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 22/11/2017 |

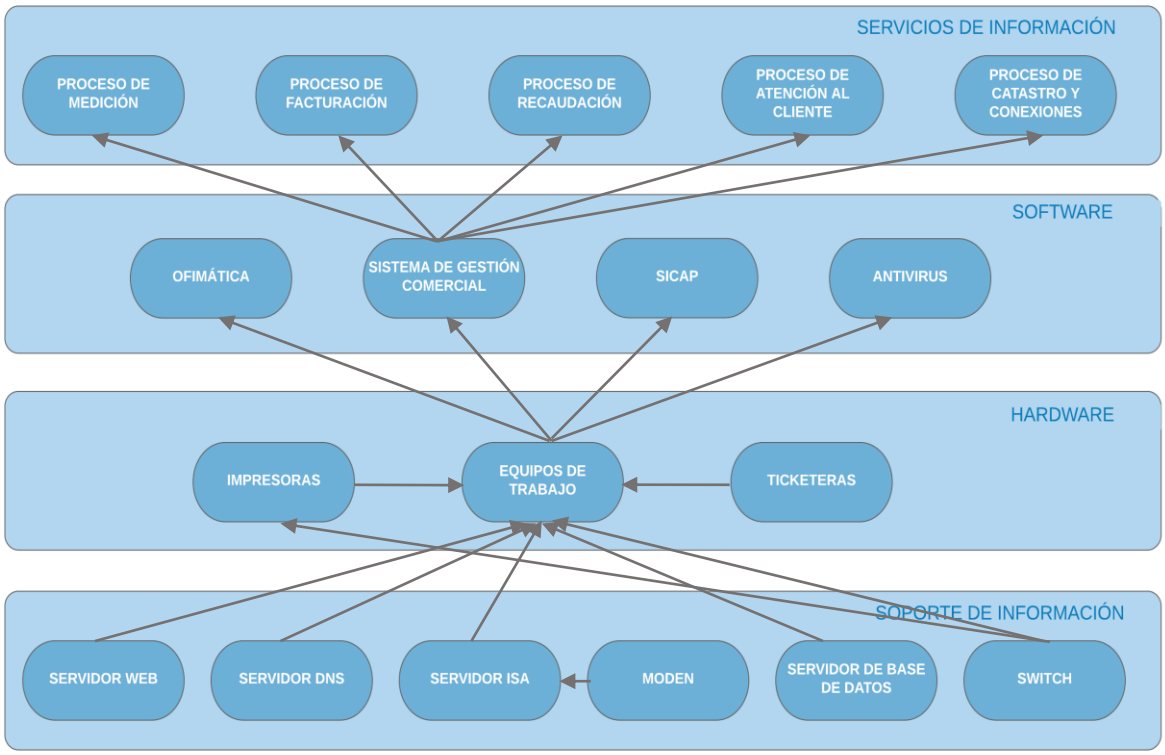
| Ítem | Activos | Código | Categoría | | | |
|---|---|---|---|---|---|---|
| | | | [S] | [SW] | [HW] | [SI] |
| 16 | Modem | [SI_MODEM] | | | | X |
| 17 | Switch | [SI_SWITCH] | | | | X |
| 18 | Servidor de Base de Datos | [SI_SBD] | | | | X |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 02 | CÓDIGO DEAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Dependencia de activos | | | | |
| **Objetivo:** Establecer una relación de dependencia entre los activos críticos identificados. | | | | TIPO | DIAGRAMA |
| Actores | Gerencia Comercial Equipo de Análisis | Elaborado Por: | LMOSCOSO | Fecha Elaboración | 15/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 22/11/2017 |

Diagrama 2-Dependencias de activos de EPSEL S.A.




| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 03 | CÓDIGO VAAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Valoración de activos | | | | |
| **Objetivo:** Valorar los activos críticos identificados en base a los criterios de confidencialidad, integridad y disponibilidad. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 24/11/2017 |

Tabla 52- Cuadro de valoración de activos

| ACTIVO | | | | CRITERIOS | | | | |
|---|---|---|---|---|---|---|---|---|
| N° Ítem | Etiqueta Categoría | Código activo | Descripción del activo | Valoración confidencialidad | Valoración de Integridad | Valoración de Disponibilidad | TOTAL | |
| 1 | [S] | [S_PM] | Proceso de Medición | 5 | 5 | 5 | 15 | MA |
| 2 | [S] | [S_PF] | Proceso de Facturación | 5 | 5 | 5 | 15 | MA |
| 3 | [S] | [S_PC] | Proceso de Cobranza | 5 | 5 | 5 | 15 | MA |
| 4 | [S] | [S_PAT] | Proceso de Atención al Cliente | 5 | 5 | 4 | 14 | MA |
| 5 | [S] | [S_CC] | Proceso de Catastro y Conexiones | 5 | 5 | 5 | 15 | MA |
| 6 | [SW] | [SW_SGC] | Sistema de Gestión Comercial | 5 | 5 | 5 | 15 | MA |
| 7 | [SW] | [SW_SICAP] | SICAP | 1 | 1 | 1 | 3 | B |
| 8 | [SW] | [SW_OFIMATICA] | Ofimática | 1 | 1 | 1 | 3 | B |
| 9 | [SW] | [SW_ANTIVIRUS] | Antivirus | 2 | 1 | 3 | 6 | M |
| 10 | [HW] | [HW_IMP] | Impresoras | 3 | 1 | 4 | 8 | A |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 03 | CÓDIGO VAAC N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Valoración de activos | | | | |
| **Objetivo:** Valorar los activos críticos identificados en base a los criterios de confidencialidad, integridad y disponibilidad. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 24/11/2017 |

| ACTIVO | | | | CRITERIOS | | | | |
|---|---|---|---|---|---|---|---|---|
| N° Ítem | Etiqueta Categoría | Código activo | Descripción del activo | Valoración confidencialidad | Valoración de Integridad | Valoración de Disponibilidad | TOTAL | |
| 11 | [HW] | [HW_PC] | Estación de Trabajo | 4 | 3 | 4 | 11 | MA |
| 12 | [HW] | [HW_TLCB] | Ticketeras / Lectoras de código de barras | 3 | 1 | 3 | 7 | A |
| 13 | [SI] | [SI_SWEB] | Servidor Web | 1 | 1 | 1 | 3 | B |
| 14 | [SI] | [SI_SDNS] | Servidor DNS | 2 | 3 | 3 | 8 | A |
| 15 | [SI] | [SI_ISA] | Servidor ISA | 1 | 1 | 1 | 3 | B |
| 16 | [SI] | [SI_MODEM] | Modem | 2 | 1 | 3 | 6 | M |
| 17 | [SI] | [SI_SWITCH] | Switch | 2 | 1 | 3 | 6 | M |
| 18 | [SI] | [SI_SBD] | Servidor de Base de Datos | 5 | 5 | 5 | 15 | MA |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

Tabla 53- Cuadro de valoración de la amenaza

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| 1 | Fuego | HW_IMP | 3 | 1 | 3 |
| | | HW_PC | 3 | 1 | 3 |
| | | HW_LBAR | 3 | 1 | 3 |
| | | SI_SWEB | 3 | 1 | 3 |
| | | SI_SDNS | 3 | 1 | 3 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_MODEM | 3 | 1 | 3 |
| | | SI_SWITCH | 3 | 1 | 3 |
| | | SI_SBD | 3 | 1 | 3 |
| 2 | Daños por agua | HW_IMP | 3 | 1 | 3 |
| | | HW_PC | 3 | 1 | 3 |
| | | HW_LBAR | 3 | 1 | 3 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | SI_SWEB | 3 | 1 | 3 |
| | | SI_SDNS | 3 | 1 | 3 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_MODEM | 3 | 1 | 3 |
| | | SI_SWITCH | 3 | 1 | 3 |
| | | SI_SBD | 3 | 1 | 3 |
| 3 | Desastres naturales | SW_SGC | 1 | 1 | 1 |
| | | HW_IMP | 1 | 1 | 1 |
| | | HW_PC | 1 | 1 | 1 |
| | | HW_LBAR | 1 | 1 | 1 |
| | | SI_SWEB | 1 | 1 | 1 |
| | | SI_SDNS | 1 | 1 | 1 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | SI_SISA | 1 | 1 | 1 |
| | | SI_MODEM | 1 | 1 | 1 |
| | | SI_SWITCH | 1 | 1 | 1 |
| | | SI_SBD | 1 | 1 | 1 |
| 4 | Corte de suministro eléctrico | SW_SGC | 2 | 2 | 3 |
| | | SW_SICAP | 2 | 2 | 3 |
| | | SW_OFI | 2 | 2 | 3 |
| | | SW_AV | 2 | 2 | 3 |
| | | HW_IMP | 2 | 2 | 3 |
| | | HW_PC | 2 | 2 | 3 |
| | | HW_LBAR | 2 | 2 | 3 |
| | | SI_SWEB | 2 | 2 | 3 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | SI_SDNS | 2 | 2 | 3 |
| | | SI_SISA | 2 | 2 | 3 |
| | | SI_MODEM | 2 | 2 | 3 |
| | | SI_SWITCH | 2 | 2 | 3 |
| | | SI_SBD | 2 | 2 | 3 |
| 5 | Condiciones inadecuadas de temperatura o humedad | HW_IMP | 1 | 1 | 1 |
| | | HW_PC | 1 | 1 | 1 |
| | | HW_LBAR | 1 | 1 | 1 |
| | | SI_SWEB | 1 | 1 | 1 |
| | | SI_SDNS | 1 | 1 | 1 |
| | | SI_SISA | 1 | 1 | 1 |
| | | SI_MODEM | 1 | 1 | 1 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | SI_SWITCH | 1 | 1 | 1 |
| | | SI_SBD | 1 | 1 | 1 |
| 6 | Fallo de servicios de comunicaciones | HW_IMP | 2 | 2 | 3 |
| | | HW_PC | 2 | 2 | 3 |
| | | HW_LBAR | 2 | 2 | 3 |
| | | SI_SWEB | 2 | 2 | 3 |
| | | SI_SDNS | 2 | 2 | 3 |
| | | SI_SISA | 2 | 2 | 3 |
| | | SI_MODEM | 2 | 2 | 3 |
| | | SI_SWITCH | 2 | 2 | 3 |
| | | SI_SGC | 2 | 2 | 3 |
| | | SI_SBD | 2 | 2 | 3 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| 7 | Interrupción de otros servicios y suministros esenciales | HW_IMP | 1 | 2 | 2 |
| | | HW_PC | 1 | 2 | 2 |
| | | HW_LBAR | 1 | 2 | 2 |
| | | SI_SBD | 1 | 2 | 2 |
| 8 | Errores de los usuarios | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 3 | 1 | 3 |
| | | HW_IMP | 1 | 1 | 1 |
| | | HW_PC | 1 | 1 | 1 |
| | | HW_LBAR | 1 | 1 | 1 |
| 9 | Errores de configuración | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 2 | 1 | 2 |
| | | SW_AV | 2 | 2 | 3 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | HW_IMP | 2 | 1 | 2 |
| | | HW_PC | 2 | 1 | 2 |
| | | HW_LBAR | 2 | 1 | 2 |
| | | SI_SWEB | 3 | 2 | 4 |
| | | SI_SDNS | 3 | 2 | 4 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_MODEM | 3 | 1 | 3 |
| | | SI_SWITCH | 3 | 1 | 3 |
| | | SI_SBD | 3 | 3 | 5 |
| 10 | Fuga de información | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 1 | 1 | 1 |
| | | HW_IMP | 2 | 1 | 2 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | HW_PC | 2 | 2 | 3 |
| | | SI_SBD | 3 | 3 | 5 |
| 11 | Introducción de falsa información | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 2 | 1 | 2 |
| | | SI_SBD | 3 | 1 | 3 |
| 12 | Alteración de la información | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 2 | 1 | 2 |
| | | SI_SBD | 3 | 3 | 5 |
| 13 | Corrupción de la información | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 2 | 1 | 2 |
| | | SI_SBD | 3 | 1 | 3 |
| 14 | Destrucción de la información | SW_SGC | 3 | 2 | 4 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | SW_SICAP | 2 | 1 | 2 |
| | | SI_SBD | 3 | 3 | 5 |
| 15 | Degradación de los soportes de almacenamiento de la información | SI_SBD | 3 | 2 | 4 |
| 16 | Difusión de software dañino | HW_PC | 3 | 3 | 5 |
| | | SI_SWEB | 3 | 1 | 3 |
| | | SI_SDNS | 3 | 1 | 3 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_SBD | 3 | 1 | 3 |
| 17 | Errores de mantenimiento / actualización de programas (software) | SW_SGC | 3 | 2 | 4 |
| | | SI_SBD | 3 | 1 | 3 |
| 18 | Errores de mantenimiento / | HW_IMP | 1 | 1 | 1 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | actualización de equipos (hardware) | HW_PC | 2 | 2 | 3 |
| | | HW_LBAR | 1 | 1 | 1 |
| | | SI_SWEB | 3 | 1 | 3 |
| | | SI_SDNS | 3 | 1 | 3 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_SBD | 3 | 1 | 3 |
| 19 | Caída del sistema por sobrecarga | SW_SGC | 3 | 1 | 3 |
| | | SW_SICAP | 2 | 1 | 2 |
| 20 | Pérdida de Equipos | HW_IMP | 1 | 3 | 3 |
| | | HW_PC | 2 | 3 | 4 |
| | | HW_LBAR | 1 | 3 | 3 |
| | | SI_SWEB | 3 | 1 | 3 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| | | SI_SDNS | 3 | 1 | 3 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_MODEM | 3 | 1 | 3 |
| | | SI_SWITCH | 3 | 1 | 3 |
| | | SI_SBD | 3 | 1 | 3 |
| 21 | Indisponibilidad del personal | SW_SGC | 3 | 1 | 3 |
| | | SI_SBD | 3 | 1 | 3 |
| 22 | Abuso de privilegios de acceso | SW_SGC | 3 | 3 | 5 |
| | | SI_SBD | 3 | 3 | 5 |
| 23 | Acceso no autorizado | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 2 | 1 | 2 |
| | | SI_SBD | 3 | 3 | 5 |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVDA N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la amenaza | | | | |
| **Objetivo:** Identificar las amenazas bajo los criterios de capacidad y motivación. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| N° | Amenazas | Activos | Capacidad | Motivación | Valor amenaza |
|---|---|---|---|---|---|
| 24 | Denegación del servicio | HW_IMP | 1 | 2 | 2 |
| | | HW_LBAR | 1 | 2 | 2 |
| | | SI_SWEB | 3 | 1 | 3 |
| | | SI_SDNS | 3 | 1 | 3 |
| | | SI_SISA | 3 | 1 | 3 |
| | | SI_MODEM | 3 | 1 | 3 |
| | | SI_SWITCH | 3 | 1 | 3 |
| 25 | Ingeniería social | SW_SGC | 3 | 3 | 5 |
| | | SW_SICAP | 2 | 1 | 2 |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

Tabla 54- Cuadro de identificación de las vulnerabilidades

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 1 | R1 | HW_IMP | Impresoras | Fuego | Carencia de sistemas de seguridad anti incendios. |
| 2 | R2 | HW_IMP | Impresoras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos. |
| 3 | R3 | HW_IMP | Impresoras | Desastres naturales | Infraestructura inadecuada. |
| 4 | R4 | HW_IMP | Impresoras | Corte de suministro eléctrico | Carencia de grupos electrógenos. |
| 5 | R5 | HW_IMP | Impresoras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada. |
| 6 | R6 | HW_IMP | Impresoras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. |
| 7 | R7 | HW_IMP | Impresoras | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo. |
| 8 | R8 | HW_IMP | Impresoras | Errores de los usuarios | Carencia de un plan de capacitación. |
| 9 | R9 | HW_IMP | Impresoras | Errores de configuración | Ausencia de un plan de configuración de equipos. |
| 10 | R10 | HW_IMP | Impresoras | Fuga de información | Ausencia de un plan de seguridad. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 11 | R11 | HW_IMP | Impresoras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. |
| 12 | R12 | HW_IMP | Impresoras | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 13 | R13 | HW_IMP | Impresoras | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 14 | R14 | HW_PC | Estación de Trabajo | Fuego | Carencia de sistemas de seguridad anti incendios. |
| 15 | R15 | HW_PC | Estación de Trabajo | Daños por agua | Carencia de un plan de concientización del cuidado de equipos. |
| 16 | R16 | HW_PC | Estación de Trabajo | Desastres naturales | Infraestructura inadecuada. |
| 17 | R17 | HW_PC | Estación de Trabajo | Corte de suministro eléctrico | Carencia de grupos electrógenos. |
| 18 | R18 | HW_PC | Estación de Trabajo | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada. |
| 19 | R19 | HW_PC | Estación de Trabajo | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. |
| 20 | R20 | HW_PC | Estación de Trabajo | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 21 | R21 | HW_PC | Estación de Trabajo | Errores de los usuarios | Carencia de un plan de capacitación. |
| 22 | R22 | HW_PC | Estación de Trabajo | Errores de configuración | Ausencia de un plan de configuración de equipos. |
| 23 | R23 | HW_PC | Estación de Trabajo | Fuga de información | Ausencia de un plan de seguridad. |
| 24 | R24 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de un plan de seguridad. |
| 25 | R25 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de Políticas de software mal intencionado. |
| 26 | R26 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Deficiencia en el procedimiento de prevención. |
| 27 | R27 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. |
| 28 | R28 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Deficiencia en la actualización del inventario de equipos. |
| 29 | R29 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 30 | R30 | SI_MODEM | MODEM | Fuego | Deficiencia en infraestructura de la sala de servidores. |
| 31 | R31 | SI_MODEM | MODEM | Daños por agua | Deficiencia en infraestructura de la sala de servidores. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 32 | R32 | SI_MODEM | MODEM | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. |
| 33 | R33 | SI_MODEM | MODEM | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores. |
| 34 | R34 | SI_MODEM | MODEM | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. |
| 35 | R35 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos. |
| 36 | R36 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Deficiencia en las políticas para determinar los acuerdos de niveles de servicio. |
| 37 | R37 | SI_MODEM | MODEM | Errores de configuración | Ausencia de Plan de Gestión de Configuración. |
| 38 | R38 | SI_MODEM | MODEM | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 39 | R39 | SI_MODEM | MODEM | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 40 | R40 | SI_SWITCH | SWITCH | Fuego | Deficiencia en infraestructura de la sala de servidores. |
| 41 | R41 | SI_SWITCH | SWITCH | Daños por agua | Deficiencia en infraestructura de la sala de servidores. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 42 | R42 | SI_SWITCH | SWITCH | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. |
| 43 | R43 | SI_SWITCH | SWITCH | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores. |
| 44 | R44 | SI_SWITCH | SWITCH | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. |
| 45 | R45 | SI_SWITCH | SWITCH | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos. |
| 46 | R46 | SI_SWITCH | SWITCH | Errores de configuración | Ausencia de Plan de Gestión de Configuración. |
| 47 | R47 | SI_SWITCH | SWITCH | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 48 | R48 | SI_SWITCH | SWITCH | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores. |
| 50 | R50 | | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de seguridad. |
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores. |
| 52 | R52 | SI_SBD | Servidor de Base de | Daños por agua | Deficiencia en las políticas de copias de seguridad. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| | | | Datos | | |
| 53 | R53 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. |
| 54 | R54 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en las políticas de copias de seguridad. |
| 55 | R55 | SI_SBD | Servidor de Base de Datos | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores. |
| 56 | R56 | SI_SBD | Servidor de Base de Datos | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. |
| 57 | R57 | SI_SBD | Servidor de Base de Datos | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos. |
| 58 | R58 | SI_SBD | Servidor de Base de Datos | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo. |
| 59 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de plan de gestión de configuración. |
| 60 | R60 | SI_SBD | Servidor de Base de Datos | Fuga de información | Carencia de un plan de seguridad. |
| 61 | R61 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de políticas de revisión por muestreo. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 62 | R62 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de un plan de supervisión. |
| 63 | R63 | SI_SBD | Servidor de Base de Datos | Alteración de la información | Carencia de un plan de supervisión. |
| 64 | R64 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Carencia de un plan de supervisión. |
| 65 | R65 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Deficiencia en las políticas de copias de seguridad. |
| 66 | R66 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Carencia de un plan de supervisión. |
| 67 | R67 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Deficiencia en las políticas de copias de seguridad. |
| 68 | R68 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un plan de supervisión. |
| 69 | R69 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un sistema de información de administración de eventos. |
| 70 | R70 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de un plan de seguridad. |
| 71 | R71 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de políticas de software mal intencionado. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 72 | R72 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de documentación. |
| 73 | R73 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo. |
| 74 | R74 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Ausencia de plan de gestión de configuración. |
| 75 | R75 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de documentación. |
| 76 | R76 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de un plan de mantenimiento preventivo |
| 77 | R77 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de plan de gestión de configuración. |
| 78 | R78 | SI_SBD | Servidor de Base de Datos | Pérdida de Equipos | Carencia de un plan de seguridad. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 79 | R79 | SI_SBD | Servidor de Base de Datos | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de base de datos. |
| 80 | R80 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal. |
| 81 | R81 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. |
| 82 | R82 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un sistema de información de administración de eventos. |
| 83 | R83 | | Servidor de Base de Datos | Acceso no autorizado | Carencia de un plan de auditoría de accesos. |
| 84 | R84 | SW_SGC | Sistema de Gestión Comercial | Corte de suministro eléctrico | Deficiencia en las políticas de copias de seguridad. |
| 85 | R85 | SW_SGC | Sistema de Gestión Comercial | Fallo de servicios de comunicaciones | Carencia de una fuente de conocimiento de incidentes. |
| 86 | R86 | SW_SGC | Sistema de Gestión Comercial | Errores de los usuarios | Carencia de un plan de capacitación. |
| 87 | R87 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de plan de gestión de configuración. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 88 | R88 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. |
| 89 | R89 | SW_SGC | Sistema de Gestión Comercial | Fuga de información | Carencia de un plan de seguridad. |
| 90 | R90 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de políticas de revisión por muestreo. |
| 91 | R91 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de un plan de supervisión. |
| 92 | R92 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de políticas de revisión por muestreo. |
| 93 | R93 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de un plan de supervisión. |
| 94 | R94 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de políticas de revisión por muestreo. |
| 95 | R95 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de un plan de supervisión. |
| 96 | R96 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de políticas de revisión por muestreo. |
| 97 | R97 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de un plan de supervisión. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 98 | R98 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de documentación. |
| 99 | R99 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo. |
| 100 | R100 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Ausencia de Plan de Gestión de Configuración. |
| 101 | R101 | SW_SGC | Sistema de Gestión Comercial | Caída del sistema por sobrecarga | Carencia de un sistema de información de administración de eventos. |
| 102 | R102 | SW_SGC | Sistema de Gestión Comercial | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de base de datos. |
| 103 | R103 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal. |
| 104 | R104 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 105 | R105 | SW_SGC | Sistema de Gestión Comercial | Acceso no autorizado | Carencia de un sistema de información de administración de eventos. |
| 106 | R106 | SW_SGC | Sistema de Gestión Comercial | Ingeniería social | Carencia de capacitación sobre ingeniería social. |
| 107 | R107 | HW_LBAR | Ticketeras | Fuego | Carencia de sistemas de seguridad anti incendios. |
| 108 | R108 | HW_LBAR | Ticketeras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos. |
| 109 | R109 | HW_LBAR | Ticketeras | Desastres naturales | Infraestructura inadecuada. |
| 110 | R110 | HW_LBAR | Ticketeras | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 111 | R111 | HW_LBAR | Ticketeras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada. |
| 112 | R112 | HW_LBAR | Ticketeras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. |
| 113 | R113 | HW_LBAR | Ticketeras | Interrupción de otros servicios y suministros esenciales | Infraestructura inadecuada. |
| 114 | R114 | HW_LBAR | Ticketeras | Errores de los usuarios | Carencia de un plan de capacitación. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 115 | R115 | HW_LBAR | Ticketeras | Errores de configuración | Ausencia de un plan de configuración de equipos. |
| 116 | R116 | HW_LBAR | Ticketeras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. |
| 117 | R117 | HW_LBAR | Ticketeras | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 118 | R118 | HW_LBAR | Ticketeras | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 119 | R119 | SI_SWEB | Servidor Web | Fuego | Carencia de sistemas de seguridad anti incendios. |
| 120 | R120 | SI_SWEB | Servidor Web | Daños por agua | Carencia de un plan de concientización del cuidado de equipos. |
| 121 | R121 | SI_SWEB | Servidor Web | Desastres naturales | Infraestructura inadecuada. |
| 122 | R122 | SI_SWEB | Servidor Web | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 123 | R123 | SI_SWEB | Servidor Web | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada. |
| 124 | R124 | SI_SWEB | Servidor Web | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 125 | R125 | SI_SWEB | Servidor Web | Errores de los usuarios | Carencia de un plan de capacitación. |
| 126 | R126 | SI_SWEB | Servidor Web | Difusión de software dañino | Ausencia de un plan de seguridad. |
| 127 | R127 | SI_SWEB | Servidor Web | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. |
| 128 | R128 | SI_SWEB | Servidor Web | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 129 | R129 | SI_SDNS | Servidor DNS | Fuego | Carencia de sistemas de seguridad anti incendios. |
| 130 | R130 | SI_SDNS | Servidor DNS | Daños por agua | Carencia de un plan de concientización del cuidado de equipos. |
| 131 | R131 | SI_SDNS | Servidor DNS | Desastres naturales | Infraestructura inadecuada. |
| 132 | R132 | SI_SDNS | Servidor DNS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 133 | R133 | SI_SDNS | Servidor DNS | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada. |
| 134 | R134 | SI_SDNS | Servidor DNS | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. |
| 135 | R135 | SI_SDNS | Servidor DNS | Errores de configuración | Carencia de un plan de capacitación. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 136 | R136 | SI_SDNS | Servidor DNS | Difusión de software dañino | Ausencia de un plan de seguridad. |
| 137 | R137 | SI_SDNS | Servidor DNS | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. |
| 138 | R138 | SI_SDNS | Servidor DNS | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 139 | R139 | SI_SDNS | Servidor DNS | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 140 | R140 | SI_SISA | Servidor ISA | Fuego | Carencia de sistemas de seguridad anti incendios. |
| 141 | R141 | SI_SISA | Servidor ISA | Daños por agua | Carencia de un plan de concientización del cuidado de equipos. |
| 142 | R142 | SI_SISA | Servidor ISA | Desastres naturales | Infraestructura inadecuada. |
| 143 | R143 | SI_SISA | Servidor ISA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 144 | R144 | SI_SISA | Servidor ISA | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada. |
| 145 | R145 | SI_SISA | Servidor ISA | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. |
| 146 | R146 | SI_SISA | Servidor ISA | Errores de configuración | Carencia de un plan de capacitación. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 147 | R147 | SI_SISA | Servidor ISA | Difusión de software dañino | Ausencia de un plan de seguridad. |
| 148 | R148 | SI_SISA | Servidor ISA | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. |
| 149 | R149 | SI_SISA | Servidor ISA | Pérdida de Equipos | Carencia de un plan de seguridad. |
| 150 | R150 | SI_SISA | Servidor ISA | Denegación del servicio | Carencia de un sistema de información de administración de eventos. |
| 151 | R151 | SW_SICAP | SICAP | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 152 | R152 | SW_SICAP | SICAP | Errores de los usuarios | Carencia de un plan de capacitación. |
| 153 | R153 | SW_SICAP | SICAP | Errores de configuración | Ausencia de un plan de configuración de equipos. |
| 154 | R154 | SW_SICAP | SICAP | Fuga de información | Ausencia de un plan de seguridad. |
| 155 | R155 | SW_SICAP | SICAP | Introducción de falsa información | Falta de un plan de seguridad. |
| 156 | R156 | SW_SICAP | SICAP | Alteración de la información | Falta de un plan de seguridad. |
| 157 | R157 | SW_SICAP | SICAP | Corrupción de la información | Falta de un plan de seguridad. |
| 158 | R158 | SW_SICAP | SICAP | Destrucción de la información | Falta de un plan de seguridad. |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO IDVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Identificación de las vulnerabilidades | | | | |
| **Objetivo:** Identificar las vulnerabilidadesde cada activo para cada situación de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad |
|---|---|---|---|---|---|
| 159 | R159 | SW_SICAP | SICAP | Caída del sistema por sobrecarga | Falta de un control de accesos a los recursos. |
| 160 | R160 | SW_SICAP | SICAP | Acceso no autorizado | Falta de políticas de control de acceso. |
| 161 | R161 | SW_SICAP | SICAP | Acceso no autorizado | Falta de cuentas de usuarios mal configuradas. |
| 162 | R162 | SW_SICAP | SICAP | Ingeniería social | Falta de políticas de seguridad. |
| 163 | R163 | SW_OFI | OFIMATICA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 164 | R164 | SW_AV | ANTIVIRUS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico. |
| 165 | R165 | SW_AV | ANTIVIRUS | Errores de configuración | Carencia de un plan de capacitación. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

Tabla 55- Cuadro de determinación de la vulnerabilidad

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 1 | R1 | HW_IMP | Impresoras | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 1 | **3** |
| 2 | R2 | HW_IMP | Impresoras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 1 | **3** |
| 3 | R3 | HW_IMP | Impresoras | Desastres naturales | Infraestructura inadecuada | 1 | 1 | **1** |
| 4 | R4 | HW_IMP | Impresoras | Corte de suministro eléctrico | Carencia de grupos electrógenos | 2 | 1 | **2** |
| 5 | R5 | HW_IMP | Impresoras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 2 | 1 | **2** |
| 6 | R6 | HW_IMP | Impresoras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 1 | **3** |
| 7 | R7 | HW_IMP | Impresoras | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo | 2 | 1 | **2** |
| 8 | R8 | HW_IMP | Impresoras | Errores de los usuarios | Carencia de un plan de capacitación | 3 | 2 | **4** |
| 9 | R9 | HW_IMP | Impresoras | Errores de configuración | Ausencia de un plan de configuración de equipos | 3 | 1 | **3** |
| 10 | R10 | HW_IMP | Impresoras | Fuga de información | Ausencia de un plan de seguridad | 3 | 1 | **3** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 11 | R11 | HW_IMP | Impresoras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 2 | 1 | **2** |
| 12 | R12 | HW_IMP | Impresoras | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 1 | **3** |
| 13 | R13 | HW_IMP | Impresoras | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 1 | **3** |
| 14 | R14 | HW_PC | Estación de Trabajo | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 2 | **4** |
| 15 | R15 | HW_PC | Estación de Trabajo | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 2 | **4** |
| 16 | R16 | HW_PC | Estación de Trabajo | Desastres naturales | Infraestructura inadecuada | 1 | 2 | **2** |
| 17 | R17 | HW_PC | Estación de Trabajo | Corte de suministro eléctrico | Carencia de grupos electrógenos | 2 | 2 | **3** |
| 18 | R18 | HW_PC | Estación de Trabajo | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 2 | 2 | **3** |
| 19 | R19 | HW_PC | Estación de Trabajo | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 2 | 2 | **3** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 20 | R20 | HW_PC | Estación de Trabajo | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo | 2 | 2 | **3** |
| 21 | R21 | HW_PC | Estación de Trabajo | Errores de los usuarios | Carencia de un plan de capacitación | 3 | 2 | **4** |
| 22 | R22 | HW_PC | Estación de Trabajo | Errores de configuración | Ausencia de un plan de configuración de equipos | 3 | 2 | **4** |
| 23 | R23 | HW_PC | Estación de Trabajo | Fuga de información | Ausencia de un plan de seguridad | 3 | 2 | **4** |
| 24 | R24 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 2 | **4** |
| 25 | R25 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de políticas de software mal intencionado | 3 | 2 | **4** |
| 26 | R26 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Deficiencia en el procedimiento de prevención | 3 | 2 | **4** |
| 27 | R27 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 3 | 2 | **4** |
| 28 | R28 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Deficiencia en la actualización del inventario de equipos | 3 | 2 | **4** |
| 29 | R29 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 2 | **4** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 30 | R30 | SI_MODEM | MODEM | Fuego | Deficiencia en infraestructura de la sala de servidores | 3 | 2 | **4** |
| 31 | R31 | SI_MODEM | MODEM | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 2 | **4** |
| 32 | R32 | SI_MODEM | MODEM | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. | 1 | 2 | **2** |
| 33 | R33 | SI_MODEM | MODEM | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores | 2 | 2 | **3** |
| 34 | R34 | SI_MODEM | MODEM | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. | 2 | 2 | **3** |
| 35 | R35 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos | 2 | 2 | **3** |
| 36 | R36 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Deficiencia en las políticas para determinar los acuerdos de niveles de servicio | 2 | 2 | **3** |
| 37 | R37 | SI_MODEM | MODEM | Errores de configuración | Ausencia de plan de gestión de configuración | 3 | 2 | **4** |
| 38 | R38 | SI_MODEM | MODEM | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 2 | **4** |
| 39 | R39 | SI_MODEM | MODEM | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 2 | 2 | **3** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 40 | R40 | SI_SWITCH | SWITCH | Fuego | Deficiencia en infraestructura de la sala de servidores | 3 | 3 | **5** |
| 41 | R41 | SI_SWITCH | SWITCH | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 3 | **5** |
| 42 | R42 | SI_SWITCH | SWITCH | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. | 1 | 3 | **3** |
| 43 | R43 | SI_SWITCH | SWITCH | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores | 2 | 3 | **4** |
| 44 | R44 | SI_SWITCH | SWITCH | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores | 2 | 3 | **4** |
| 45 | R45 | SI_SWITCH | SWITCH | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos | 2 | 3 | **4** |
| 46 | R46 | SI_SWITCH | SWITCH | Errores de configuración | Ausencia de plan de gestión de configuración | 3 | 3 | **5** |
| 47 | R47 | SI_SWITCH | SWITCH | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 3 | **5** |
| 48 | R48 | SI_SWITCH | SWITCH | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 3 | **5** |
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores | 2 | 3 | **4** |
| 50 | R50 | | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de | 2 | 3 | **4** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| | | | | | seguridad | | | |
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 3 | **5** |
| 52 | R52 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en las políticas de copias de seguridad | 3 | 3 | **5** |
| 53 | R53 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en infraestructura de la sala de servidores | 1 | 3 | **3** |
| 54 | R54 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en las políticas de copias de seguridad | 1 | 3 | **3** |
| 55 | R55 | SI_SBD | Servidor de Base de Datos | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores | 2 | 3 | **4** |
| 56 | R56 | SI_SBD | Servidor de Base de Datos | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores | 2 | 3 | **4** |
| 57 | R57 | SI_SBD | Servidor de Base de Datos | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos | 2 | 3 | **4** |
| 58 | R58 | SI_SBD | Servidor de Base de Datos | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo | 1 | 3 | **3** |
| 59 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de plan de gestión de configuración | 2 | 3 | **4** |
| 60 | R60 | SI_SBD | Servidor de Base de Datos | Fuga de información | Carencia de un plan de seguridad | 2 | 3 | **4** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 61 | R61 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 2 | 3 | **4** |
| 62 | R62 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de un plan de supervisión | 2 | 3 | **4** |
| 63 | R63 | SI_SBD | Servidor de Base de Datos | Alteración de la información | Carencia de un plan de supervisión | 3 | 3 | **5** |
| 64 | R64 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Carencia de un plan de supervisión | 3 | 3 | **5** |
| 65 | R65 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Deficiencia en las políticas de copias de seguridad | 3 | 3 | **5** |
| 66 | R66 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Carencia de un plan de supervisión | 2 | 3 | **4** |
| 67 | R67 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Deficiencia en las políticas de copias de seguridad | 2 | 3 | **4** |
| 68 | R68 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un plan de supervisión | 3 | 3 | **5** |
| 69 | R69 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un sistema de información de administración de eventos | 3 | 3 | **5** |
| 70 | R70 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 3 | **5** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 71 | R71 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de políticas de software mal intencionado | 3 | 3 | **5** |
| 72 | R72 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de documentación | 3 | 3 | **5** |
| 73 | R73 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo | 3 | 3 | **5** |
| 74 | R74 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Ausencia de plan de gestión de configuración | 3 | 3 | **5** |
| 75 | R75 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de documentación | 3 | 3 | **5** |
| 76 | R76 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de un plan de mantenimiento preventivo | 3 | 3 | **5** |
| 77 | R77 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de plan de gestión de configuración | 3 | 3 | **5** |
| 78 | R78 | SI_SBD | Servidor de Base de Datos | Pérdida de Equipos | Carencia de un plan de seguridad | 1 | 3 | **3** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 79 | R79 | SI_SBD | Servidor de Base de Datos | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de Base de Datos | 2 | 3 | **4** |
| 80 | R80 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal | 3 | 3 | **5** |
| 81 | R81 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 3 | 3 | **5** |
| 82 | R82 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un sistema de información de administración de eventos | 3 | 3 | **5** |
| 83 | R83 | | Servidor de Base de Datos | Acceso no autorizado | Carencia de un plan de auditoría de accesos | 3 | 3 | **5** |
| 84 | R84 | SW_SGC | Sistema de Gestión Comercial | Corte de suministro eléctrico | Deficiencia en las políticas de copias de seguridad | 2 | 3 | **4** |
| 85 | R85 | SW_SGC | Sistema de Gestión Comercial | Fallo de servicios de comunicaciones | Carencia de una fuente de conocimiento de incidentes | 2 | 3 | **4** |
| 86 | R86 | SW_SGC | Sistema de Gestión Comercial | Errores de los usuarios | Carencia de un plan de capacitación. | 3 | 3 | **5** |
| 87 | R87 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de plan de gestión de configuración | 3 | 3 | **5** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 88 | R88 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 3 | 3 | **5** |
| 89 | R89 | SW_SGC | Sistema de Gestión Comercial | Fuga de información | Carencia de un plan de seguridad | 3 | 3 | **5** |
| 90 | R90 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 3 | 3 | **5** |
| 91 | R91 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de un plan de supervisión | 3 | 3 | **5** |
| 92 | R92 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de políticas de revisión por muestreo | 3 | 3 | **5** |
| 93 | R93 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de un plan de supervisión | 3 | 3 | **5** |
| 94 | R94 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de políticas de revisión por muestreo | 1 | 3 | **3** |
| 95 | R95 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de un plan de supervisión | 1 | 3 | **3** |
| 96 | R96 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de políticas de revisión por muestreo | 1 | 3 | **3** |
| 97 | R97 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de un plan de supervisión | 1 | 3 | **3** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 98 | R98 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de Documentación | 3 | 3 | **5** |
| 99 | R99 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo | 3 | 3 | **5** |
| 100 | R100 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Ausencia de plan de gestión de configuración | 3 | 3 | **5** |
| 101 | R101 | SW_SGC | Sistema de Gestión Comercial | Caída del sistema por sobrecarga | Carencia de un sistema de información de administración de eventos. | 2 | 3 | **4** |
| 102 | R102 | SW_SGC | Sistema de Gestión Comercial | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de Base de Datos | 2 | 3 | **4** |
| 103 | R103 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal | 3 | 3 | **5** |
| 104 | R104 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados | 3 | 3 | **5** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 105 | R105 | SW_SGC | Sistema de Gestión Comercial | Acceso no autorizado | Carencia de un sistema de información de administración de eventos | 3 | 3 | **5** |
| 106 | R106 | SW_SGC | Sistema de Gestión Comercial | Ingeniería social | Carencia de Capacitación sobre Ingeniería Social | 3 | 3 | **5** |
| 107 | R107 | HW_LBAR | Ticketeras | Fuego | Carencia de sistemas de seguridad anti incendios | 1 | 1 | **1** |
| 108 | R108 | HW_LBAR | Ticketeras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 1 | 1 | **1** |
| 109 | R109 | HW_LBAR | Ticketeras | Desastres naturales | Infraestructura inadecuada | 1 | 1 | **1** |
| 110 | R110 | HW_LBAR | Ticketeras | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 1 | 1 | **1** |
| 111 | R111 | HW_LBAR | Ticketeras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 1 | **1** |
| 112 | R112 | HW_LBAR | Ticketeras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 1 | 1 | **1** |
| 113 | R113 | HW_LBAR | Ticketeras | Interrupción de otros servicios y suministros esenciales | Infraestructura inadecuada | 1 | 1 | **1** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 114 | R114 | HW_LBAR | Ticketeras | Errores de los usuarios | Carencia de un plan de capacitación | 2 | 2 | **3** |
| 115 | R115 | HW_LBAR | Ticketeras | Errores de configuración | Ausencia de un plan de configuración de equipos | 1 | 2 | **2** |
| 116 | R116 | HW_LBAR | Ticketeras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 2 | 2 | **3** |
| 117 | R117 | HW_LBAR | Ticketeras | Pérdida de Equipos | Carencia de un plan de seguridad | 2 | 2 | **3** |
| 118 | R118 | HW_LBAR | Ticketeras | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 2 | 2 | **3** |
| 119 | R119 | SI_SWEB | Servidor Web | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 3 | **5** |
| 120 | R120 | SI_SWEB | Servidor Web | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 3 | **5** |
| 121 | R121 | SI_SWEB | Servidor Web | Desastres naturales | Infraestructura inadecuada | 3 | 3 | **5** |
| 122 | R122 | SI_SWEB | Servidor Web | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 1 | 1 | **1** |
| 123 | R123 | SI_SWEB | Servidor Web | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 2 | 1 | **2** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 124 | R124 | SI_SWEB | Servidor Web | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 2 | 2 | **3** |
| 125 | R125 | SI_SWEB | Servidor Web | Errores de los usuarios | Carencia de un plan de capacitación | 2 | 2 | **3** |
| 126 | R126 | SI_SWEB | Servidor Web | Difusión de software dañino | Ausencia de un plan de seguridad | 2 | 2 | **3** |
| 127 | R127 | SI_SWEB | Servidor Web | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 3 | 3 | **5** |
| 128 | R128 | SI_SWEB | Servidor Web | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 3 | **5** |
| 129 | R129 | SI_SDNS | Servidor DNS | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 3 | **5** |
| 130 | R130 | SI_SDNS | Servidor DNS | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 3 | **5** |
| 131 | R131 | SI_SDNS | Servidor DNS | Desastres naturales | Infraestructura inadecuada | 3 | 3 | **5** |
| 132 | R132 | SI_SDNS | Servidor DNS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 1 | 1 | **1** |
| 133 | R133 | SI_SDNS | Servidor DNS | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 2 | 2 | **3** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 134 | R134 | SI_SDNS | Servidor DNS | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 3 | **5** |
| 135 | R135 | SI_SDNS | Servidor DNS | Errores de configuración | Carencia de un plan de capacitación | 2 | 2 | **3** |
| 136 | R136 | SI_SDNS | Servidor DNS | Difusión de software dañino | Ausencia de un plan de seguridad | 2 | 2 | **3** |
| 137 | R137 | SI_SDNS | Servidor DNS | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 2 | 2 | **3** |
| 138 | R138 | SI_SDNS | Servidor DNS | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 3 | **5** |
| 139 | R139 | SI_SDNS | Servidor DNS | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 2 | 3 | **4** |
| 140 | R140 | SI_SISA | Servidor ISA | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 3 | **5** |
| 141 | R141 | SI_SISA | Servidor ISA | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 3 | **5** |
| 142 | R142 | SI_SISA | Servidor ISA | Desastres naturales | Infraestructura inadecuada | 3 | 3 | **5** |
| 143 | R143 | SI_SISA | Servidor ISA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 1 | 1 | **1** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 144 | R144 | SI_SISA | Servidor ISA | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 2 | 2 | **3** |
| 145 | R145 | SI_SISA | Servidor ISA | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 3 | **5** |
| 146 | R146 | SI_SISA | Servidor ISA | Errores de configuración | Carencia de un plan de capacitación | 3 | 2 | **4** |
| 147 | R147 | SI_SISA | Servidor ISA | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 2 | **4** |
| 148 | R148 | SI_SISA | Servidor ISA | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 2 | 2 | **3** |
| 149 | R149 | SI_SISA | Servidor ISA | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 3 | **5** |
| 150 | R150 | SI_SISA | Servidor ISA | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 3 | **5** |
| 151 | R151 | SW_SICAP | SICAP | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 2 | 1 | **2** |
| 152 | R152 | SW_SICAP | SICAP | Errores de los usuarios | Carencia de un plan de capacitación | 3 | 3 | **5** |
| 153 | R153 | SW_SICAP | SICAP | Errores de configuración | Ausencia de un plan de configuración de equipos | 3 | 2 | **4** |
| 154 | R154 | SW_SICAP | SICAP | Fuga de información | Ausencia de un plan de seguridad | 3 | 3 | **5** |

| LOGO | Fase: 03 | Proceso: 01 | Actividad: 04 | CÓDIGO DVVU N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Determinación del valor de la vulnerabilidad | | | | |
| **Objetivo:** Determinar las vulnerabilidades bajos los criterios de severidad y exposición | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 15/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 27/11/2017 |

| Ítem | Código Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Severidad | Exposición | Valor Vulnerabilidad |
|---|---|---|---|---|---|---|---|---|
| 155 | R155 | SW_SICAP | SICAP | Introducción de falsa información | Falta de un plan de seguridad | 3 | 3 | **5** |
| 156 | R156 | SW_SICAP | SICAP | Alteración de la información | Falta de un plan de seguridad | 3 | 3 | **5** |
| 157 | R157 | SW_SICAP | SICAP | Corrupción de la información | Falta de un plan de seguridad | 3 | 3 | **5** |
| 158 | R158 | SW_SICAP | SICAP | Destrucción de la información | Falta de un plan de seguridad | 3 | 3 | **5** |
| 159 | R159 | SW_SICAP | SICAP | Caída del sistema por sobrecarga | Falta de un control de accesos a los recursos | 3 | 3 | **5** |
| 160 | R160 | SW_SICAP | SICAP | Acceso no autorizado | Falta de políticas de control de acceso | 3 | 3 | **5** |
| 161 | R161 | SW_SICAP | SICAP | Acceso no autorizado | Falta de cuentas de usuarios mal configuradas | 3 | 3 | **5** |
| 162 | R162 | SW_SICAP | SICAP | Ingeniería social | Falta de políticas de seguridad | 3 | 3 | **5** |
| 163 | R163 | SW_OFI | OFIMATICA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 1 | 1 | **1** |
| 164 | R164 | SW_AV | ANTIVIRUS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 2 | 1 | **2** |
| 165 | R165 | SW_AV | ANTIVIRUS | Errores de configuración | Carencia de un plan de capacitación | 2 | 2 | **3** |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

Tabla 56- Cuadro de matriz del nivel de riesgo

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | R1 | HW_IMP | Impresoras | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 3 | 2 | 2 | 4 | 36 |
| 2 | R2 | HW_IMP | Impresoras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 3 | 2 | 2 | 4 | 36 |
| 3 | R3 | HW_IMP | Impresoras | Desastres naturales | Infraestructura inadecuada | 1 | 1 | 1 | 2 | 2 | 2 |
| 4 | R4 | HW_IMP | Impresoras | Corte de suministro eléctrico | Carencia de grupos electrógenos. | 3 | 2 | 1 | 2 | 2 | 12 |
| 5 | R5 | HW_IMP | Impresoras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 2 | 1 | 1 | 1 | 2 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | R6 | HW_IMP | Impresoras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 3 | 2 | 2 | 4 | 36 |
| 7 | R7 | HW_IMP | Impresoras | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo | 2 | 2 | 2 | 2 | 4 | 16 |
| 8 | R8 | HW_IMP | Impresoras | Errores de los usuarios | Carencia de un plan de capacitación. | 1 | 4 | 3 | 2 | 6 | 24 |
| 9 | R9 | HW_IMP | Impresoras | Errores de configuración | Ausencia de un plan de configuración de equipos | 2 | 3 | 3 | 2 | 6 | 36 |
| 10 | R10 | HW_IMP | Impresoras | Fuga de información | Ausencia de un plan de seguridad | 2 | 3 | 1 | 1 | 1 | 6 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | R11 | HW_IMP | Impresoras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. | 1 | 2 | 1 | 1 | 1 | 2 |
| 12 | R12 | HW_IMP | Impresoras | Pérdida de Equipos | Carencia de un plan de seguridad. | 3 | 3 | 3 | 3 | 9 | 81 |
| 13 | R13 | HW_IMP | Impresoras | Denegación del servicio | Carencia de un sistema de información de administración de eventos. | 2 | 3 | 1 | 2 | 2 | 12 |
| 14 | R14 | HW_PC | Estación de Trabajo | Fuego | Carencia de sistemas de seguridad anti incendios. | 3 | 4 | 2 | 4 | 8 | 96 |
| 15 | R15 | HW_PC | Estación de Trabajo | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 4 | 2 | 4 | 8 | 96 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | R16 | HW_PC | Estación de Trabajo | Desastres naturales | Infraestructura inadecuada | 1 | 2 | 1 | 4 | 4 | 8 |
| 17 | R17 | HW_PC | Estación de Trabajo | Corte de suministro eléctrico | Carencia de grupos electrógenos. | 3 | 3 | 2 | 3 | 6 | 54 |
| 18 | R18 | HW_PC | Estación de Trabajo | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 3 | 1 | 3 | 3 | 9 |
| 19 | R19 | HW_PC | Estación de Trabajo | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. | 3 | 3 | 3 | 4 | 12 | 108 |
| 20 | R20 | HW_PC | Estación de Trabajo | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo. | 2 | 3 | 3 | 4 | 12 | 72 |
| 21 | R21 | HW_PC | Estación de Trabajo | Errores de los usuarios | Carencia de un plan de capacitación. | 1 | 4 | 3 | 5 | 15 | 60 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 22 | R22 | HW_PC | Estación de Trabajo | Errores de configuración | Ausencia de un plan de configuración de equipos. | 2 | 4 | 3 | 4 | 12 | 96 |
| 23 | R23 | HW_PC | Estación de Trabajo | Fuga de información | Ausencia de un plan de seguridad | 3 | 4 | 3 | 5 | 15 | 180 |
| 24 | R24 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de un plan de seguridad | 5 | 4 | 2 | 4 | 8 | 160 |
| 25 | R25 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de políticas de software mal intencionado | 5 | 4 | 2 | 4 | 8 | 160 |
| 26 | R26 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Deficiencia en el procedimiento de prevención | 3 | 4 | 2 | 3 | 6 | 72 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 27 | R27 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 3 | 4 | 2 | 3 | 6 | 72 |
| 28 | R28 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Deficiencia en la actualización del inventario de equipos | 4 | 4 | 2 | 4 | 8 | 128 |
| 29 | R29 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Carencia de un plan de seguridad | 4 | 4 | 2 | 4 | 8 | 128 |
| 30 | R30 | SI_MODEM | MODEM | Fuego | Deficiencia en infraestructura de la sala de servidores | 3 | 4 | 2 | 5 | 10 | 120 |
| 31 | R31 | SI_MODEM | MODEM | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 4 | 1 | 4 | 4 | 48 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 32 | R32 | SI_MODEM | MODEM | Desastres naturales | Deficiencia en infraestructura de la sala de servidores | 1 | 2 | 2 | 4 | 8 | 16 |
| 33 | R33 | SI_MODEM | MODEM | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores | 3 | 3 | 1 | 3 | 3 | 27 |
| 34 | R34 | SI_MODEM | MODEM | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores | 1 | 3 | 1 | 3 | 3 | 9 |
| 35 | R35 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos | 3 | 3 | 2 | 3 | 6 | 54 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 36 | R36 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Deficiencia en las políticas para determinar los acuerdos de niveles de servicio | 3 | 3 | 2 | 3 | 6 | 54 |
| 37 | R37 | SI_MODEM | MODEM | Errores de configuración | Ausencia de plan de gestión de configuración | 3 | 4 | 1 | 3 | 3 | 36 |
| 38 | R38 | SI_MODEM | MODEM | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 4 | 1 | 3 | 3 | 36 |
| 39 | R39 | SI_MODEM | MODEM | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 3 | 1 | 3 | 3 | 27 |
| 40 | R40 | SI_SWITCH | SWITCH | Fuego | Deficiencia en infraestructura de la sala de servidores | 3 | 5 | 2 | 5 | 10 | 150 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 41 | R41 | SI_SWITCH | SWITCH | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 5 | 1 | 5 | 5 | 75 |
| 42 | R42 | SI_SWITCH | SWITCH | Desastres naturales | Deficiencia en infraestructura de la sala de servidores | 1 | 3 | 2 | 4 | 8 | 24 |
| 43 | R43 | SI_SWITCH | SWITCH | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores | 3 | 4 | 1 | 4 | 4 | 48 |
| 44 | R44 | SI_SWITCH | SWITCH | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores | 1 | 4 | 2 | 5 | 10 | 40 |
| 45 | R45 | SI_SWITCH | SWITCH | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos | 3 | 4 | 2 | 4 | 8 | 96 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 46 | R46 | SI_SWITCH | SWITCH | Errores de configuración | Ausencia de plan de gestión de configuración | 3 | 5 | 1 | 5 | 5 | 75 |
| 47 | R47 | SI_SWITCH | SWITCH | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 5 | 1 | 3 | 3 | 45 |
| 48 | R48 | SI_SWITCH | SWITCH | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 5 | 1 | 5 | 5 | 75 |
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores | 3 | 4 | 2 | 5 | 10 | 120 |
| 50 | R50 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de seguridad | 3 | 4 | 2 | 5 | 10 | 120 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores | 3 | 5 | 2 | 5 | 10 | 150 |
| 52 | R52 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en las políticas de copias de seguridad | 3 | 5 | 2 | 5 | 10 | 150 |
| 53 | R53 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en infraestructura de la sala de servidores | 1 | 3 | 1 | 5 | 5 | 15 |
| 54 | R54 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Políticas de copias de seguridad deficiente | 1 | 3 | 1 | 5 | 5 | 15 |
| 55 | R55 | SI_SBD | Servidor de Base de Datos | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores | 3 | 4 | 2 | 5 | 10 | 120 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 56 | R56 | SI_SBD | Servidor de Base de Datos | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores | 1 | 4 | 1 | 5 | 5 | 20 |
| 57 | R57 | SI_SBD | Servidor de Base de Datos | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos | 3 | 4 | 2 | 5 | 10 | 120 |
| 58 | R58 | SI_SBD | Servidor de Base de Datos | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo | 2 | 3 | 2 | 5 | 10 | 60 |
| 59 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de plan de gestión de configuración | 5 | 4 | 4 | 5 | 20 | 400 |
| 60 | R60 | SI_SBD | Servidor de Base de Datos | Fuga de información | Carencia de un plan de seguridad | 5 | 4 | 4 | 5 | 20 | 400 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 61 | R61 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 3 | 4 | 3 | 5 | 15 | 180 |
| 62 | R62 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de un plan de supervisión | 3 | 4 | 3 | 5 | 15 | 180 |
| 63 | R63 | SI_SBD | Servidor de Base de Datos | Alteración de la información | Carencia de un plan de supervisión | 5 | 5 | 5 | 5 | 25 | 625 |
| 64 | R64 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Carencia de un plan de supervisión | 3 | 5 | 3 | 5 | 15 | 225 |
| 65 | R65 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Deficiencia en las políticas de copias de seguridad | 3 | 5 | 3 | 5 | 15 | 225 |
| 66 | R66 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Carencia de un plan de supervisión | 5 | 4 | 5 | 5 | 25 | 500 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 67 | R67 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Deficiencia en las políticas de copias de seguridad | 5 | 4 | 5 | 5 | 25 | 500 |
| 68 | R68 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un plan de supervisión | 4 | 5 | 3 | 5 | 15 | 300 |
| 69 | R69 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un sistema de información de administración de eventos | 4 | 5 | 3 | 5 | 15 | 300 |
| 70 | R70 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 5 | 3 | 5 | 15 | 225 |
| 71 | R71 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de políticas de software mal intencionado | 3 | 5 | 3 | 5 | 15 | 225 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 72 | R72 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de documentación | 3 | 5 | 2 | 5 | 10 | 150 |
| 73 | R73 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo | 3 | 5 | 2 | 5 | 10 | 150 |
| 74 | R74 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Ausencia de plan de gestión de configuración | 3 | 5 | 2 | 5 | 10 | 150 |
| 75 | R75 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de documentación | 3 | 5 | 2 | 5 | 10 | 150 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 76 | R76 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de un plan de mantenimiento preventivo | 3 | 5 | 3 | 5 | 15 | 225 |
| 77 | R77 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de plan de gestión de configuración | 3 | 5 | 3 | 5 | 15 | 225 |
| 78 | R78 | SI_SBD | Servidor de Base de Datos | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 3 | 3 | 3 | 9 | 81 |
| 79 | R79 | SI_SBD | Servidor de Base de Datos | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de base de datos | 3 | 4 | 3 | 4 | 12 | 144 |
| 80 | R80 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal | 5 | 5 | 5 | 5 | 25 | 625 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 81 | R81 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados | 5 | 5 | 5 | 5 | 25 | 625 |
| 82 | R82 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un sistema de información de administración de eventos | 5 | 5 | 3 | 5 | 15 | 375 |
| 83 | R83 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un plan de auditoría de accesos | 5 | 5 | 3 | 5 | 15 | 375 |
| 84 | R84 | SW_SGC | Sistema de Gestión Comercial | Corte de suministro eléctrico | Deficiencia en las políticas de copias de seguridad | 3 | 4 | 2 | 4 | 8 | 96 |
| 85 | R85 | SW_SGC | Sistema de Gestión Comercial | Fallo de servicios de comunicaciones | Carencia de una fuente de conocimiento de incidentes | 3 | 4 | 3 | 4 | 12 | 144 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 86 | R86 | SW_SGC | Sistema de Gestión Comercial | Errores de los usuarios | Carencia de un plan de capacitación | 5 | 5 | 5 | 5 | 25 | 625 |
| 87 | R87 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de plan de gestión de configuración | 5 | 5 | 5 | 5 | 25 | 625 |
| 88 | R88 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados | 5 | 5 | 4 | 5 | 20 | 500 |
| 89 | R89 | SW_SGC | Sistema de Gestión Comercial | Fuga de información | Carencia de un plan de seguridad | 5 | 5 | 4 | 5 | 20 | 500 |
| 90 | R90 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 5 | 5 | 4 | 5 | 20 | 500 |
| 91 | R91 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de un plan de supervisión | 5 | 5 | 4 | 5 | 20 | 500 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 92 | R92 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de políticas de revisión por muestreo | 5 | 5 | 4 | 5 | 20 | 500 |
| 93 | R93 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de un plan de supervisión | 5 | 5 | 4 | 5 | 20 | 500 |
| 94 | R94 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de políticas de revisión por muestreo | 5 | 3 | 4 | 5 | 20 | 300 |
| 95 | R95 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de un plan de supervisión | 5 | 3 | 4 | 5 | 20 | 300 |
| 96 | R96 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de políticas de revisión por muestreo | 4 | 3 | 4 | 5 | 20 | 240 |
| 97 | R97 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de un plan de supervisión | 4 | 3 | 4 | 5 | 20 | 240 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 98 | R98 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de documentación | 4 | 5 | 2 | 5 | 10 | 200 |
| 99 | R99 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo | 4 | 5 | 2 | 5 | 10 | 200 |
| 100 | R100 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Ausencia de plan de gestión de configuración | 4 | 5 | 3 | 5 | 15 | 300 |
| 101 | R101 | SW_SGC | Sistema de Gestión Comercial | Caída del sistema por sobrecarga | Carencia de un sistema de información de administración de eventos | 3 | 4 | 2 | 4 | 8 | 96 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 102 | R102 | SW_SGC | Sistema de Gestión Comercial | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de base de datos | 3 | 4 | 3 | 4 | 12 | 144 |
| 103 | R103 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal | 5 | 5 | 5 | 5 | 25 | 625 |
| 104 | R104 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados | 5 | 5 | 4 | 5 | 20 | 500 |
| 105 | R105 | SW_SGC | Sistema de Gestión Comercial | Acceso no autorizado | Carencia de un sistema de información de administración de eventos | 5 | 5 | 4 | 5 | 20 | 500 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 106 | R106 | SW_SGC | Sistema de Gestión Comercial | Ingeniería social | Carencia de Capacitación sobre ingeniería social | 5 | 5 | 5 | 5 | 25 | 625 |
| 107 | R107 | HW_LBAR | Ticketeras | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 1 | 2 | 1 | 2 | 6 |
| 108 | R108 | HW_LBAR | Ticketeras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 1 | 2 | 1 | 2 | 6 |
| 109 | R109 | HW_LBAR | Ticketeras | Desastres naturales | Infraestructura inadecuada | 1 | 1 | 1 | 1 | 1 | 1 |
| 110 | R110 | HW_LBAR | Ticketeras | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 1 | 1 | 1 | 1 | 3 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 111 | R111 | HW_LBAR | Ticketeras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 1 | 1 | 1 | 1 | 1 |
| 112 | R112 | HW_LBAR | Ticketeras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 1 | 2 | 2 | 4 | 12 |
| 113 | R113 | HW_LBAR | Ticketeras | Interrupción de otros servicios y suministros esenciales | Infraestructura inadecuada | 2 | 1 | 1 | 2 | 2 | 4 |
| 114 | R114 | HW_LBAR | Ticketeras | Errores de los usuarios | Carencia de un plan de capacitación | 1 | 3 | 3 | 2 | 6 | 18 |
| 115 | R115 | HW_LBAR | Ticketeras | Errores de configuración | Ausencia de un plan de configuración de equipos | 2 | 2 | 3 | 2 | 6 | 24 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 116 | R116 | HW_LBAR | Ticketeras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 1 | 3 | 1 | 1 | 1 | 3 |
| 117 | R117 | HW_LBAR | Ticketeras | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 3 | 3 | 3 | 9 | 81 |
| 118 | R118 | HW_LBAR | Ticketeras | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 2 | 3 | 1 | 2 | 2 | 12 |
| 119 | R119 | SI_SWEB | Servidor Web | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 5 | 2 | 5 | 10 | 150 |
| 120 | R120 | SI_SWEB | Servidor Web | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 5 | 2 | 5 | 10 | 150 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 121 | R121 | SI_SWEB | Servidor Web | Desastres naturales | Infraestructura inadecuada | 1 | 5 | 1 | 5 | 5 | 25 |
| 122 | R122 | SI_SWEB | Servidor Web | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 1 | 2 | 5 | 10 | 30 |
| 123 | R123 | SI_SWEB | Servidor Web | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 2 | 2 | 5 | 10 | 20 |
| 124 | R124 | SI_SWEB | Servidor Web | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 3 | 3 | 4 | 12 | 108 |
| 125 | R125 | SI_SWEB | Servidor Web | Errores de los usuarios | Carencia de un plan de capacitación | 4 | 3 | 3 | 5 | 15 | 180 |
| 126 | R126 | SI_SWEB | Servidor Web | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 3 | 1 | 5 | 5 | 45 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 127 | R127 | SI_SWEB | Servidor Web | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 3 | 5 | 3 | 5 | 15 | 225 |
| 128 | R128 | SI_SWEB | Servidor Web | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 5 | 1 | 5 | 5 | 75 |
| 129 | R129 | SI_SDNS | Servidor DNS | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 5 | 2 | 5 | 10 | 150 |
| 130 | R130 | SI_SDNS | Servidor DNS | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 5 | 2 | 5 | 10 | 150 |
| 131 | R131 | SI_SDNS | Servidor DNS | Desastres naturales | Infraestructura inadecuada | 1 | 5 | 1 | 5 | 5 | 25 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 132 | R132 | SI_SDNS | Servidor DNS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 1 | 2 | 5 | 10 | 30 |
| 133 | R133 | SI_SDNS | Servidor DNS | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 3 | 2 | 5 | 10 | 30 |
| 134 | R134 | SI_SDNS | Servidor DNS | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 5 | 3 | 4 | 12 | 180 |
| 135 | R135 | SI_SDNS | Servidor DNS | Errores de configuración | Carencia de un plan de capacitación | 4 | 3 | 1 | 5 | 5 | 60 |
| 136 | R136 | SI_SDNS | Servidor DNS | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 3 | 1 | 5 | 5 | 45 |
| 137 | R137 | SI_SDNS | Servidor DNS | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 3 | 3 | 3 | 5 | 15 | 135 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 138 | R138 | SI_SDNS | Servidor DNS | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 5 | 3 | 3 | 9 | 135 |
| 139 | R139 | SI_SDNS | Servidor DNS | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 4 | 1 | 5 | 5 | 60 |
| 140 | R140 | SI_SISA | Servidor ISA | Fuego | Carencia de sistemas de seguridad anti incendios | 3 | 5 | 2 | 5 | 10 | 150 |
| 141 | R141 | SI_SISA | Servidor ISA | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 3 | 5 | 2 | 5 | 10 | 150 |
| 142 | R142 | SI_SISA | Servidor ISA | Desastres naturales | Infraestructura inadecuada | 1 | 5 | 1 | 5 | 5 | 25 |
| 143 | R143 | SI_SISA | Servidor ISA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 1 | 2 | 5 | 10 | 30 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 144 | R144 | SI_SISA | Servidor ISA | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | 3 | 2 | 5 | 10 | 30 |
| 145 | R145 | SI_SISA | Servidor ISA | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 3 | 5 | 3 | 4 | 12 | 180 |
| 146 | R146 | SI_SISA | Servidor ISA | Errores de configuración | Carencia de un plan de capacitación | 3 | 4 | 1 | 5 | 5 | 60 |
| 147 | R147 | SI_SISA | Servidor ISA | Difusión de software dañino | Ausencia de un plan de seguridad | 3 | 4 | 1 | 5 | 5 | 60 |
| 148 | R148 | SI_SISA | Servidor ISA | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 3 | 3 | 3 | 5 | 15 | 135 |
| 149 | R149 | SI_SISA | Servidor ISA | Pérdida de Equipos | Carencia de un plan de seguridad | 3 | 5 | 3 | 5 | 15 | 225 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 150 | R150 | SI_SISA | Servidor ISA | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 3 | 5 | 1 | 5 | 5 | 75 |
| 151 | R151 | SW_SICAP | SICAP | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 2 | 2 | 4 | 8 | 48 |
| 152 | R152 | SW_SICAP | SICAP | Errores de los usuarios | Carencia de un plan de capacitación | 3 | 5 | 3 | 5 | 15 | 225 |
| 153 | R153 | SW_SICAP | SICAP | Errores de configuración | Ausencia de un plan de configuración de equipos | 2 | 4 | 1 | 5 | 5 | 40 |
| 154 | R154 | SW_SICAP | SICAP | Fuga de información | Ausencia de un plan de seguridad | 1 | 5 | 4 | 5 | 20 | 100 |
| 155 | R155 | SW_SICAP | SICAP | Introducción de falsa información | Falta de un plan de seguridad | 2 | 5 | 4 | 5 | 20 | 200 |
| 156 | R156 | SW_SICAP | SICAP | Alteración de la información | Falta de un plan de seguridad | 2 | 5 | 4 | 5 | 20 | 200 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 157 | R157 | SW_SICAP | SICAP | Corrupción de la información | Falta de un plan de seguridad | 2 | 5 | 4 | 5 | 20 | 200 |
| 158 | R158 | SW_SICAP | SICAP | Destrucción de la información | Falta de un plan de seguridad | 2 | 5 | 4 | 5 | 20 | 200 |
| 159 | R159 | SW_SICAP | SICAP | Caída del sistema por sobrecarga | Falta de un control de accesos a los recursos | 2 | 5 | 2 | 4 | 8 | 80 |
| 160 | R160 | SW_SICAP | SICAP | Acceso no autorizado | Falta de políticas de control de acceso | 2 | 5 | 4 | 5 | 20 | 200 |
| 161 | R161 | SW_SICAP | SICAP | Acceso no autorizado | Falta de cuentas de usuarios mal configuradas | 2 | 5 | 4 | 5 | 20 | 200 |
| 162 | R162 | SW_SICAP | SICAP | Ingeniería social | Falta de políticas de seguridad | 2 | 5 | 5 | 5 | 25 | 250 |
| 163 | R163 | SW_OFI | OFIMATICA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 1 | 2 | 3 | 6 | 18 |
| 164 | R164 | SW_AV | ANTIVIRUS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 3 | 2 | 2 | 5 | 10 | 60 |

| LOGO | Fase: 04 | Proceso: 01 | Actividad: -- | | CÓDIGO MDNR N°___ | Pág. __/____ |
|---|---|---|---|---|---|---|
| | Matriz del nivel de riesgo | | | | | |
| **Objetivo:** Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | | **Elaborado Por:** | EPEÑA - MSOTO | **Fecha Elaboración** | 16/10/2017 |
| **Revisado Por:** | JSEGURA | | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 28/11/2017 |

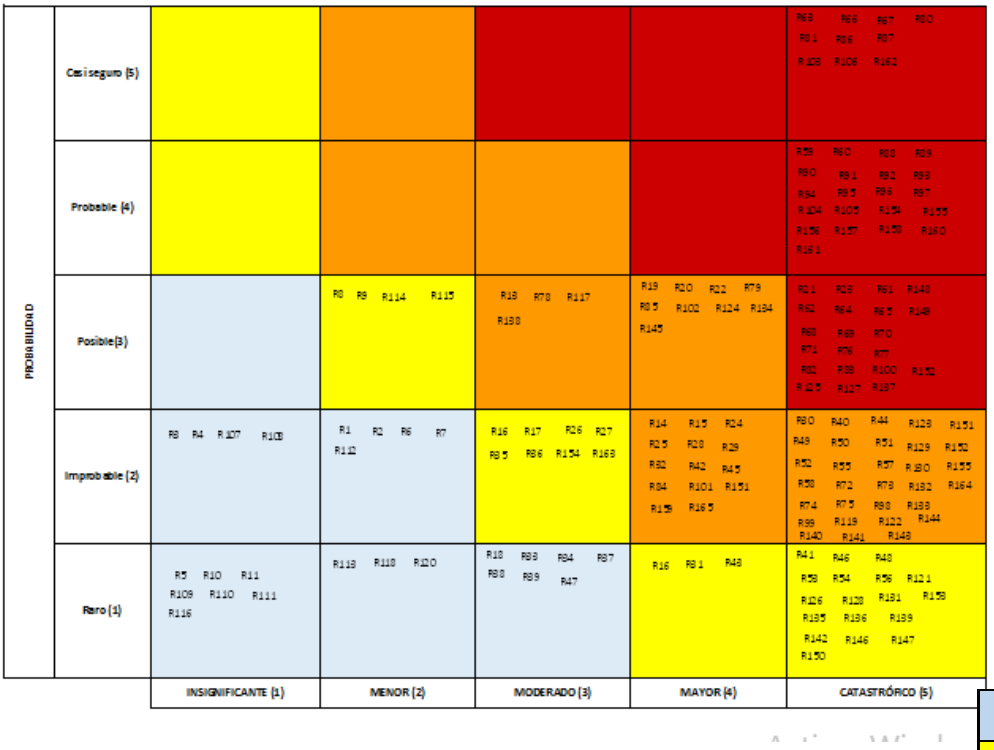
| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Valor Amenaza (1) | Valor Vulnerabilidad (2) | Posibilidad (3) | Impacto (4) | Riesgo (3)x(4) (5) | Riesgo Total (1)x(2)x(5) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 165 | R165 | SW_AV | ANTIVIRUS | Errores de configuración | Carencia de un plan de capacitación | 3 | 3 | 2 | 4 | 8 | 72 |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO MDCR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de clasificación de riesgos | | | | |
| **Objetivo:** Elaborar la matriz de clasificación del riesgo de acuerdo a la valor obtenido para la posibilidad y el impacto. | | | | **TIPO** | MATRIZ DE COLOR |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 17/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 30/11/2017 |

Tabla 57- Cuadro de matriz de clasificación de riesgos




Leyenda de prioridad

| | | |
|---|---|---|
| | Prioridad 4 | 1 - 3 |
| | Prioridad 3 | 4 - 6 |
| | Prioridad 2 | 8 - 12 |
| | Prioridad 1 | 15 - 25 |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 17/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 30/11/2017 |

Tabla 58- Cuadro de priorización del riesgo

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 1 | R1 | 2 | 2 | 4 | Moderada |
| 2 | R2 | 2 | 2 | 4 | Moderada |
| 3 | R3 | 1 | 2 | 2 | Baja |
| 4 | R4 | 1 | 2 | 2 | Baja |
| 5 | R5 | 1 | 1 | 1 | Baja |
| 6 | R6 | 2 | 2 | 4 | Moderada |
| 7 | R7 | 2 | 2 | 4 | Moderada |
| 8 | R8 | 3 | 2 | 6 | Moderada |
| 9 | R9 | 3 | 2 | 6 | Moderada |
| 10 | R10 | 1 | 1 | 1 | Baja |
| 11 | R11 | 1 | 1 | 1 | Baja |
| 12 | R12 | 3 | 3 | 9 | Alta |
| 13 | R13 | 1 | 2 | 2 | Baja |
| 14 | R14 | 2 | 4 | 8 | Alta |
| 15 | R15 | 2 | 4 | 8 | Alta |
| 16 | R16 | 1 | 4 | 4 | Moderada |
| 17 | R17 | 2 | 3 | 6 | Moderada |
| 18 | R18 | 1 | 3 | 3 | Baja |
| 19 | R19 | 3 | 4 | 12 | Alta |
| 20 | R20 | 3 | 4 | 12 | Alta |
| 21 | R21 | 3 | 5 | 15 | Extrema |
| 22 | R22 | 3 | 4 | 12 | Alta |
| 23 | R23 | 3 | 5 | 15 | Extrema |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 17/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 30/11/2017 |

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 24 | R24 | 2 | 4 | 8 | Alta |
| 25 | R25 | 2 | 4 | 8 | Alta |
| 26 | R26 | 2 | 3 | 6 | Moderada |
| 27 | R27 | 2 | 3 | 6 | Moderada |
| 28 | R28 | 2 | 4 | 8 | Alta |
| 29 | R29 | 2 | 4 | 8 | Alta |
| 30 | R30 | 2 | 5 | 10 | Alta |
| 31 | R31 | 1 | 4 | 4 | Moderada |
| 32 | R32 | 2 | 4 | 8 | Alta |
| 33 | R33 | 1 | 3 | 3 | Baja |
| 34 | R34 | 1 | 3 | 3 | Baja |
| 35 | R35 | 2 | 3 | 6 | Moderada |
| 36 | R36 | 2 | 3 | 6 | Moderada |
| 37 | R37 | 1 | 3 | 3 | Baja |
| 38 | R38 | 1 | 3 | 3 | Baja |
| 39 | R39 | 1 | 3 | 3 | Baja |
| 40 | R40 | 2 | 5 | 10 | Alta |
| 41 | R41 | 1 | 5 | 5 | Moderada |
| 42 | R42 | 2 | 4 | 8 | Alta |
| 43 | R43 | 1 | 4 | 4 | Moderada |
| 44 | R44 | 2 | 5 | 10 | Alta |
| 45 | R45 | 2 | 4 | 8 | Alta |
| 46 | R46 | 1 | 5 | 5 | Moderada |
| 47 | R47 | 1 | 3 | 3 | Baja |
| 48 | R48 | 1 | 5 | 5 | Moderada |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 17/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 30/11/2017 |

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 49 | R49 | 2 | 5 | 10 | Alta |
| 50 | R50 | 2 | 5 | 10 | Alta |
| 51 | R51 | 2 | 5 | 10 | Alta |
| 52 | R52 | 2 | 5 | 10 | Alta |
| 53 | R53 | 1 | 5 | 5 | Moderada |
| 54 | R54 | 1 | 5 | 5 | Moderada |
| 55 | R55 | 2 | 5 | 10 | Alta |
| 56 | R56 | 1 | 5 | 5 | Moderada |
| 57 | R57 | 2 | 5 | 10 | Alta |
| 58 | R58 | 2 | 5 | 10 | Alta |
| 59 | R59 | 4 | 5 | 20 | Extrema |
| 60 | R60 | 4 | 5 | 20 | Extrema |
| 61 | R61 | 3 | 5 | 15 | Extrema |
| 62 | R62 | 3 | 5 | 15 | Extrema |
| 63 | R63 | 5 | 5 | 25 | Extrema |
| 64 | R64 | 3 | 5 | 15 | Extrema |
| 65 | R65 | 3 | 5 | 15 | Extrema |
| 66 | R66 | 5 | 5 | 25 | Extrema |
| 67 | R67 | 5 | 5 | 25 | Extrema |
| 68 | R68 | 3 | 5 | 15 | Extrema |
| 69 | R69 | 3 | 5 | 15 | Extrema |
| 70 | R70 | 3 | 5 | 15 | Extrema |
| 71 | R71 | 3 | 5 | 15 | Extrema |
| 72 | R72 | 2 | 5 | 10 | Alta |
| 73 | R73 | 2 | 5 | 10 | Alta |
| 74 | R74 | 2 | 5 | 10 | Alta |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 17/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 30/11/2017 |

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 75 | R75 | 2 | 5 | 10 | Alta |
| 76 | R76 | 3 | 5 | 15 | Extrema |
| 77 | R77 | 3 | 5 | 15 | Extrema |
| 78 | R78 | 3 | 3 | 9 | Alta |
| 79 | R79 | 3 | 4 | 12 | Alta |
| 80 | R80 | 5 | 5 | 25 | Extrema |
| 81 | R81 | 5 | 5 | 25 | Extrema |
| 82 | R82 | 3 | 5 | 15 | Extrema |
| 83 | R83 | 3 | 5 | 15 | Extrema |
| 84 | R84 | 2 | 4 | 8 | Alta |
| 85 | R85 | 3 | 4 | 12 | Alta |
| 86 | R86 | 5 | 5 | 25 | Extrema |
| 87 | R87 | 5 | 5 | 25 | Extrema |
| 88 | R88 | 4 | 5 | 20 | Extrema |
| 89 | R89 | 4 | 5 | 20 | Extrema |
| 90 | R90 | 4 | 5 | 20 | Extrema |
| 91 | R91 | 4 | 5 | 20 | Extrema |
| 92 | R92 | 4 | 5 | 20 | Extrema |
| 93 | R93 | 4 | 5 | 20 | Extrema |
| 94 | R94 | 4 | 5 | 20 | Extrema |
| 95 | R95 | 4 | 5 | 20 | Extrema |
| 96 | R96 | 4 | 5 | 20 | Extrema |
| 97 | R97 | 4 | 5 | 20 | Extrema |
| 98 | R98 | 2 | 5 | 10 | Alta |
| 99 | R99 | 2 | 5 | 10 | Alta |
| 100 | R100 | 3 | 5 | 15 | Extrema |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 17/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 30/11/2017 |

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 101 | R101 | 2 | 4 | 8 | Alta |
| 102 | R102 | 3 | 4 | 12 | Alta |
| 103 | R103 | 5 | 5 | 25 | Extrema |
| 104 | R104 | 4 | 5 | 20 | Extrema |
| 105 | R105 | 4 | 5 | 20 | Extrema |
| 106 | R106 | 5 | 5 | 25 | Extrema |
| 107 | R107 | 2 | 1 | 2 | Baja |
| 108 | R108 | 2 | 1 | 2 | Baja |
| 109 | R109 | 1 | 1 | 1 | Baja |
| 110 | R110 | 1 | 1 | 1 | Baja |
| 111 | R111 | 1 | 1 | 1 | Baja |
| 112 | R112 | 2 | 2 | 4 | Moderada |
| 113 | R113 | 1 | 2 | 2 | Baja |
| 114 | R114 | 3 | 2 | 6 | Moderada |
| 115 | R115 | 3 | 2 | 6 | Moderada |
| 116 | R116 | 1 | 1 | 1 | Baja |
| 117 | R117 | 3 | 3 | 9 | Alta |
| 118 | R118 | 1 | 2 | 2 | Baja |
| 119 | R119 | 2 | 5 | 10 | Alta |
| 120 | R120 | 2 | 5 | 10 | Alta |
| 121 | R121 | 1 | 5 | 5 | Moderada |
| 122 | R122 | 2 | 5 | 10 | Alta |
| 123 | R123 | 2 | 5 | 10 | Alta |
| 124 | R124 | 3 | 4 | 12 | Alta |
| 125 | R125 | 3 | 5 | 15 | Extrema |
| 126 | R126 | 1 | 5 | 5 | Moderada |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 17/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 30/11/2017 |

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 127 | R127 | 3 | 5 | 15 | Extrema |
| 128 | R128 | 1 | 5 | 5 | Moderada |
| 129 | R129 | 2 | 5 | 10 | Alta |
| 130 | R130 | 2 | 5 | 10 | Alta |
| 131 | R131 | 1 | 5 | 5 | Moderada |
| 132 | R132 | 2 | 5 | 10 | Alta |
| 133 | R133 | 2 | 5 | 10 | Alta |
| 134 | R134 | 3 | 4 | 12 | Alta |
| 135 | R135 | 1 | 5 | 5 | Moderada |
| 136 | R136 | 1 | 5 | 5 | Moderada |
| 137 | R137 | 3 | 5 | 15 | Extrema |
| 138 | R138 | 3 | 3 | 9 | Alta |
| 139 | R139 | 1 | 5 | 5 | Moderada |
| 140 | R140 | 2 | 5 | 10 | Alta |
| 141 | R141 | 2 | 5 | 10 | Alta |
| 142 | R142 | 1 | 5 | 5 | Moderada |
| 143 | R143 | 2 | 5 | 10 | Alta |
| 144 | R144 | 2 | 5 | 10 | Alta |
| 145 | R145 | 3 | 4 | 12 | Alta |
| 146 | R146 | 1 | 5 | 5 | Moderada |
| 147 | R147 | 1 | 5 | 5 | Moderada |
| 148 | R148 | 3 | 5 | 15 | Extrema |
| 149 | R149 | 3 | 5 | 15 | Extrema |
| 150 | R150 | 1 | 5 | 5 | Moderada |
| 151 | R151 | 2 | 4 | 8 | Alta |
| 152 | R152 | 3 | 5 | 15 | Extrema |

| LOGO | Fase: 05 | Proceso: 01 | Actividad: -- | CÓDIGO PRDR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Priorización del riesgo | | | | |
| **Objetivo:** Priorizar los riesgosde acuerdo al valor de riesgo obtenido del producto de la posibilidad y el impacto. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 17/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 30/11/2017 |

| N° | CÓDIGO DE RIESGO | Posibilidad [P] | Impacto [I] | ([P]x[I]) | Prioridad |
|---|---|---|---|---|---|
| 153 | R153 | 1 | 5 | 5 | Moderada |
| 154 | R154 | 4 | 5 | 20 | Extrema |
| 155 | R155 | 4 | 5 | 20 | Extrema |
| 156 | R156 | 4 | 5 | 20 | Extrema |
| 157 | R157 | 4 | 5 | 20 | Extrema |
| 158 | R158 | 4 | 5 | 20 | Extrema |
| 159 | R159 | 2 | 4 | 8 | Alta |
| 160 | R160 | 4 | 5 | 20 | Extrema |
| 161 | R161 | 4 | 5 | 20 | Extrema |
| 162 | R162 | 5 | 5 | 25 | Extrema |
| 163 | R163 | 2 | 3 | 6 | Moderada |
| 164 | R164 | 2 | 5 | 10 | Alta |
| 165 | R165 | 2 | 4 | 8 | Alta |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

Tabla 59- Cuadro de matriz de valoración de riesgos

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | R1 | HW_IMP | Impresoras | Fuego | Carencia de sistemas de seguridad anti incendios. | 4 | Moderada | 5 | 10 | Aceptable |
| 2 | R2 | HW_IMP | Impresoras | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 4 | Moderada | 5 | 10 | Aceptable |
| 3 | R3 | HW_IMP | Impresoras | Desastres naturales | Infraestructura inadecuada | 2 | Baja | 5 | 10 | Aceptable |
| 4 | R4 | HW_IMP | Impresoras | Corte de suministro eléctrico | Carencia de grupos electrógenos. | 2 | Baja | 5 | 10 | Aceptable |
| 5 | R5 | HW_IMP | Impresoras | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | Baja | 5 | 10 | Aceptable |
| 6 | R6 | HW_IMP | Impresoras | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 4 | Moderada | 5 | 10 | Aceptable |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 7 | R7 | HW_IMP | Impresoras | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo | 4 | Moderada | 5 | 10 | Aceptable |
| 8 | R8 | HW_IMP | Impresoras | Errores de los usuarios | Carencia de un plan de capacitación. | 6 | Moderada | 5 | 10 | Debe ser tratado |
| 9 | R9 | HW_IMP | Impresoras | Errores de configuración | Ausencia de un plan de configuración de equipos. | 6 | Moderada | 5 | 10 | Debe ser tratado |
| 10 | R10 | HW_IMP | Impresoras | Fuga de información | Ausencia de un plan de seguridad. | 1 | Baja | 5 | 10 | Aceptable |
| 11 | R11 | HW_IMP | Impresoras | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. | 1 | Baja | 5 | 10 | Aceptable |
| 12 | R12 | HW_IMP | Impresoras | Pérdida de Equipos | Carencia de un plan de seguridad. | 9 | Alta | 5 | 10 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 13 | R13 | HW_IMP | Impresoras | Denegación del servicio | Carencia de un sistema de información de administración de eventos. | 2 | Baja | 5 | 10 | Aceptable |
| 14 | R14 | HW_PC | Estación de Trabajo | Fuego | Carencia de sistemas de seguridad anti incendios. | 8 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 15 | R15 | HW_PC | Estación de Trabajo | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 8 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 16 | R16 | HW_PC | Estación de Trabajo | Desastres naturales | Infraestructura inadecuada | 4 | Moderada | 1.25 | 3.75 | Debe ser tratado |
| 17 | R17 | HW_PC | Estación de Trabajo | Corte de suministro eléctrico | Carencia de grupos electrógenos. | 6 | Moderada | 1.25 | 3.75 | Debe ser tratado |
| 18 | R18 | HW_PC | Estación de Trabajo | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 3 | Baja | 1.25 | 3.75 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 19 | R19 | HW_PC | Estación de Trabajo | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo. | 12 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 20 | R20 | HW_PC | Estación de Trabajo | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo. | 12 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 21 | R21 | HW_PC | Estación de Trabajo | Errores de los usuarios | Carencia de un plan de capacitación. | 15 | Extrema | 1.25 | 3.75 | Debe ser tratado |
| 22 | R22 | HW_PC | Estación de Trabajo | Errores de configuración | Ausencia de un plan de configuración de equipos. | 12 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 23 | R23 | HW_PC | Estación de Trabajo | Fuga de información | Ausencia de un plan de seguridad. | 15 | Extrema | 1.25 | 3.75 | Debe ser tratado |
| 24 | R24 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de un plan de seguridad. | 8 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 25 | R25 | HW_PC | Estación de Trabajo | Difusión de software dañino | Ausencia de Políticas de software mal intencionado | 8 | Alta | 1.25 | 3.75 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 26 | R26 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Deficiencia en el procedimiento de prevención. | 6 | Moderada | 1.25 | 3.75 | Debe ser tratado |
| 27 | R27 | HW_PC | Estación de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. | 6 | Moderada | 1.25 | 3.75 | Debe ser tratado |
| 28 | R28 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Deficiencia en la actualización del inventario de equipos. | 8 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 29 | R29 | HW_PC | Estación de Trabajo | Pérdida de Equipos | Carencia de un plan de seguridad. | 8 | Alta | 1.25 | 3.75 | Debe ser tratado |
| 30 | R30 | SI_MODEM | MODEM | Fuego | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 31 | R31 | SI_MODEM | MODEM | Daños por agua | Deficiencia en infraestructura de la sala de servidores. | 4 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 32 | R32 | SI_MODEM | MODEM | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 33 | R33 | SI_MODEM | MODEM | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores. | 3 | Baja | 0.25 | 2.5 | Debe ser tratado |
| 34 | R34 | SI_MODEM | MODEM | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. | 3 | Baja | 0.25 | 2.5 | Debe ser tratado |
| 35 | R35 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos. | 6 | Moderada | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 36 | R36 | SI_MODEM | MODEM | Fallo de servicios de comunicaciones | Deficiencia en las políticas para determinar los acuerdos de niveles de servicio. | 6 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 37 | R37 | SI_MODEM | MODEM | Errores de configuración | Ausencia de Plan de Gestión de Configuración | 3 | Baja | 0.25 | 2.5 | Debe ser tratado |
| 38 | R38 | SI_MODEM | MODEM | Pérdida de Equipos | Carencia de un plan de seguridad. | 3 | Baja | 0.25 | 2.5 | Debe ser tratado |
| 39 | R39 | SI_MODEM | MODEM | Denegación del servicio | Carencia de un sistema de información de administración de eventos. | 3 | Baja | 0.25 | 2.5 | Debe ser tratado |
| 40 | R40 | SI_SWITCH | SWITCH | Fuego | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 41 | R41 | SI_SWITCH | SWITCH | Daños por agua | Deficiencia en infraestructura de la sala de servidores. | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 42 | R42 | SI_SWITCH | SWITCH | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 43 | R43 | SI_SWITCH | SWITCH | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores. | 4 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 44 | R44 | SI_SWITCH | SWITCH | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 45 | R45 | SI_SWITCH | SWITCH | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos. | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 46 | R46 | SI_SWITCH | SWITCH | Errores de configuración | Ausencia de Plan de Gestión de Configuración | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 47 | R47 | SI_SWITCH | SWITCH | Pérdida de Equipos | Carencia de un plan de seguridad. | 3 | Baja | 0.25 | 2.5 | Debe ser tratado |
| 48 | R48 | SI_SWITCH | SWITCH | Denegación del servicio | Carencia de un sistema de información de administración de eventos. | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 49 | R49 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 50 | R50 | SI_SBD | Servidor de Base de Datos | Fuego | Deficiencia en las políticas de copias de seguridad | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 51 | R51 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 52 | R52 | SI_SBD | Servidor de Base de Datos | Daños por agua | Deficiencia en las políticas de copias de seguridad | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 53 | R53 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Deficiencia en infraestructura de la sala de servidores. | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 54 | R54 | SI_SBD | Servidor de Base de Datos | Desastres naturales | Políticas de copias de seguridad deficiente | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 55 | R55 | SI_SBD | Servidor de Base de Datos | Corte de suministro eléctrico | Deficiencia en infraestructura de la sala de servidores. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 56 | R56 | SI_SBD | Servidor de Base de Datos | Condiciones inadecuadas de temperatura o humedad | Deficiencia en infraestructura de la sala de servidores. | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 57 | R57 | SI_SBD | Servidor de Base de Datos | Fallo de servicios de comunicaciones | Carencia de un sistema de información de administración de eventos. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 58 | R58 | SI_SBD | Servidor de Base de Datos | Interrupción de otros servicios y suministros esenciales | Carencia de políticas de mantenimiento preventivo. | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 59 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de Plan de Gestión de Configuración | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 60 | R60 | SI_SBD | Servidor de Base de Datos | Fuga de información | Carencia de un plan de seguridad. | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 61 | R61 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 62 | R62 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de un plan de supervisión | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 63 | R63 | SI_SBD | Servidor de Base de Datos | Alteración de la información | Carencia de un plan de supervisión | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 64 | R64 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Carencia de un plan de supervisión | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 65 | R65 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Deficiencia en las políticas de copias de seguridad | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 66 | R66 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Carencia de un plan de supervisión | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 67 | R67 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Deficiencia en las políticas de copias de seguridad | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 68 | R68 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un plan de supervisión | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 69 | R69 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un sistema de información de administración de eventos. | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 70 | R70 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de un plan de seguridad. | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 71 | R71 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de Políticas de software mal intencionado | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 72 | R72 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de Documentación | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 73 | R73 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 74 | R74 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de programas (software) | Ausencia de Plan de Gestión de Configuración | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 75 | R75 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de Documentación | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 76 | R76 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de un plan de mantenimiento preventivo | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 77 | R77 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de Plan de Gestión de Configuración | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 78 | R78 | SI_SBD | Servidor de Base de Datos | Pérdida de Equipos | Carencia de un plan de seguridad. | 9 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 79 | R79 | SI_SBD | Servidor de Base de Datos | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de Base de Datos | 12 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 80 | R80 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal. | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 81 | R81 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 82 | R82 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un sistema de información de administración de eventos. | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 83 | R83 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un plan de auditoría de accesos | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 84 | R84 | SW_SGC | Sistema de Gestión Comercial | Corte de suministro eléctrico | Deficiencia en las políticas de copias de seguridad | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 85 | R85 | SW_SGC | Sistema de Gestión Comercial | Fallo de servicios de comunicaciones | Carencia de una fuente de conocimiento de incidentes | 12 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 86 | R86 | SW_SGC | Sistema de Gestión Comercial | Errores de los usuarios | Carencia de un plan de capacitación. | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 87 | R87 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de Plan de Gestión de Configuración | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 88 | R88 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 89 | R89 | SW_SGC | Sistema de Gestión Comercial | Fuga de información | Carencia de un plan de seguridad. | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 90 | R90 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de políticas de revisión por muestreo | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 91 | R91 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de un plan de supervisión | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 92 | R92 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de políticas de revisión por muestreo | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 93 | R93 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de un plan de supervisión | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 94 | R94 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de políticas de revisión por muestreo | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 95 | R95 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de un plan de supervisión | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 96 | R96 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de políticas de revisión por muestreo | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 97 | R97 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de un plan de supervisión | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 98 | R98 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de Documentación | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 99 | R99 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Carencia de un plan de mantenimiento preventivo | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 100 | R100 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Ausencia de Plan de Gestión de Configuración | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 101 | R101 | SW_SGC | Sistema de Gestión Comercial | Caída del sistema por sobrecarga | Carencia de un sistema de información de administración de eventos. | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 102 | R102 | SW_SGC | Sistema de Gestión Comercial | Indisponibilidad del personal | Dependencia excesiva de personal de la gestión de Base de Datos | 12 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 103 | R103 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Deficiencia en la política de rotación de personal. | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 104 | R104 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 105 | R105 | SW_SGC | Sistema de Gestión Comercial | Acceso no autorizado | Carencia de un sistema de información de administración de eventos. | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 106 | R106 | SW_SGC | Sistema de Gestión Comercial | Ingeniería social | Carencia de Capacitación sobre Ingeniería Social. | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 107 | R107 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Fuego | Carencia de sistemas de seguridad anti incendios | 2 | Baja | 10 | 15 | Aceptable |
| 108 | R108 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 2 | Baja | 10 | 15 | Aceptable |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | **TIPO** | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 109 | R109 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Desastres naturales | Infraestructura inadecuada | 1 | Baja | 10 | 15 | Aceptable |
| 110 | R110 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 1 | Baja | 10 | 15 | Aceptable |
| 111 | R111 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 1 | Baja | 10 | 15 | Aceptable |
| 112 | R112 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 4 | Moderada | 10 | 15 | Aceptable |
| 113 | R113 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Interrupción de otros servicios y suministros esenciales | Infraestructura inadecuada | 2 | Baja | 10 | 15 | Aceptable |
| 114 | R114 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Errores de los usuarios | Carencia de un plan de capacitación | 6 | Moderada | 10 | 15 | Aceptable |
| 115 | R115 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Errores de configuración | Ausencia de un plan de configuración de equipos | 6 | Moderada | 10 | 15 | Aceptable |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 116 | R116 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 1 | Baja | 10 | 15 | Aceptable |
| 117 | R117 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Pérdida de Equipos | Carencia de un plan de seguridad | 9 | Alta | 10 | 15 | Aceptable |
| 118 | R118 | HW_LBAR | Ticketeras/Lectoras de Trabajo | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 2 | Baja | 10 | 15 | Aceptable |
| 119 | R119 | SI_SWEB | Servidor Web | Fuego | Carencia de sistemas de seguridad anti incendios | 10 | Alta | 3.25 | 8.25 | Debe ser tratado |
| 120 | R120 | SI_SWEB | Servidor Web | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 10 | Alta | 3.25 | 8.25 | Debe ser tratado |
| 121 | R121 | SI_SWEB | Servidor Web | Desastres naturales | Infraestructura inadecuada | 5 | Moderada | 3.25 | 8.25 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 122 | R122 | SI_SWEB | Servidor Web | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 10 | Alta | 3.25 | 8.25 | Debe ser tratado |
| 123 | R123 | SI_SWEB | Servidor Web | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 10 | Alta | 3.25 | 8.25 | Debe ser tratado |
| 124 | R124 | SI_SWEB | Servidor Web | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 12 | Alta | 3.25 | 8.25 | Debe ser tratado |
| 125 | R125 | SI_SWEB | Servidor Web | Errores de los usuarios | Carencia de un plan de capacitación | 15 | Extrema | 3.25 | 8.25 | Debe ser tratado |
| 126 | R126 | SI_SWEB | Servidor Web | Difusión de software dañino | Ausencia de un plan de seguridad | 5 | Moderada | 3.25 | 8.25 | Debe ser tratado |
| 127 | R127 | SI_SWEB | Servidor Web | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 15 | Extrema | 3.25 | 8.25 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 128 | R128 | SI_SWEB | Servidor Web | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 5 | Moderada | 3.25 | 8.25 | Debe ser tratado |
| 129 | R129 | SI_SDNS | Servidor DNS | Fuego | Carencia de sistemas de seguridad anti incendios | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 130 | R130 | SI_SDNS | Servidor DNS | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 131 | R131 | SI_SDNS | Servidor DNS | Desastres naturales | Infraestructura inadecuada | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 132 | R132 | SI_SDNS | Servidor DNS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 133 | R133 | SI_SDNS | Servidor DNS | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 134 | R134 | SI_SDNS | Servidor DNS | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 12 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 135 | R135 | SI_SDNS | Servidor DNS | Errores de configuración | Carencia de un plan de capacitación | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 136 | R136 | SI_SDNS | Servidor DNS | Difusión de software dañino | Ausencia de un plan de seguridad | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 137 | R137 | SI_SDNS | Servidor DNS | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 138 | R138 | SI_SDNS | Servidor DNS | Pérdida de Equipos | Carencia de un plan de seguridad | 9 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 139 | R139 | SI_SDNS | Servidor DNS | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 140 | R140 | SI_SISA | Servidor ISA | Fuego | Carencia de sistemas de seguridad anti incendios | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 141 | R141 | SI_SISA | Servidor ISA | Daños por agua | Carencia de un plan de concientización del cuidado de equipos | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 142 | R142 | SI_SISA | Servidor ISA | Desastres naturales | Infraestructura inadecuada | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 143 | R143 | SI_SISA | Servidor ISA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 144 | R144 | SI_SISA | Servidor ISA | Condiciones inadecuadas de temperatura o humedad | Carencia de infraestructura adecuada | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 145 | R145 | SI_SISA | Servidor ISA | Fallo de servicios de comunicaciones | Carencia de políticas de mantenimiento preventivo | 12 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 146 | R146 | SI_SISA | Servidor ISA | Errores de configuración | Carencia de un plan de capacitación | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 147 | R147 | SI_SISA | Servidor ISA | Difusión de software dañino | Ausencia de un plan de seguridad | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| **Actores** | Equipo de Análisis | **Elaborado Por:** | MSOTO | **Fecha Elaboración** | 21/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 148 | R148 | SI_SISA | Servidor ISA | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 149 | R149 | SI_SISA | Servidor ISA | Pérdida de Equipos | Carencia de un plan de seguridad | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 150 | R150 | SI_SISA | Servidor ISA | Denegación del servicio | Carencia de un sistema de información de administración de eventos | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 151 | R151 | SI_SISA | SICAP | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 152 | R152 | SI_SISA | SICAP | Errores de los usuarios | Carencia de un plan de capacitación | 15 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 153 | R153 | SI_SISA | SICAP | Errores de configuración | Ausencia de un plan de configuración de equipos | 5 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 154 | R154 | SI_SISA | SICAP | Fuga de información | Ausencia de un plan de seguridad | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 155 | R155 | SI_SISA | SICAP | Introducción de falsa información | Falta de un plan de seguridad | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 156 | R156 | SI_SISA | SICAP | Alteración de la información | Falta de un plan de seguridad | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 157 | R157 | SI_SISA | SICAP | Corrupción de la información | Falta de un plan de seguridad | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 158 | R158 | SI_SISA | SICAP | Destrucción de la información | Falta de un plan de seguridad | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 159 | R159 | SI_SISA | SICAP | Caída del sistema por sobrecarga | Falta de un control de accesos a los recursos | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 160 | R160 | SI_SISA | SICAP | Acceso no autorizado | Falta de políticas de control de acceso | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 161 | R161 | SI_SISA | SICAP | Acceso no autorizado | Falta de cuentas de usuarios mal configuradas | 20 | Extrema | 0.25 | 2.5 | Debe ser tratado |
| 162 | R162 | SI_SISA | SICAP | Ingeniería social | Falta de políticas de seguridad | 25 | Extrema | 0.25 | 2.5 | Debe ser tratado |

| LOGO | Fase: 05 | Proceso: 02 | Actividad: -- | CÓDIGO MDVR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Matriz de valorización de riesgos | | | | |
| **Objetivo:** Determinar la capacidad en base a los límites de tolerancia y apetito de riesgo. | | | | TIPO | TABLA |
| Actores | Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 21/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 04/12/2017 |

| Ítem | Código del Riesgo | Código de Activo | Activo | Amenaza | Vulnerabilidad | Riesgo | Prioridad | Apetito | Tolerancia | Nivel |
|---|---|---|---|---|---|---|---|---|---|---|
| 163 | R163 | SI_SISA | OFIMATICA | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 6 | Moderada | 0.25 | 2.5 | Debe ser tratado |
| 164 | R164 | SI_SISA | ANTIVIRUS | Corte de suministro eléctrico | Falta de equipos de respaldo eléctrico | 10 | Alta | 0.25 | 2.5 | Debe ser tratado |
| 165 | R165 | SI_SISA | ANTIVIRUS | Errores de configuración | Carencia de un plan de capacitación | 8 | Alta | 0.25 | 2.5 | Debe ser tratado |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

Tabla 60- Cuadro de inventario de proyectos

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | R21 | HW_PC | Estación de Trabajo | Errores de los usuarios | Carencia de un plan de capacitación. | **60** | Extrema | Reducir | Capacitación de uso de equipos | S/.2,660.00 |
| 2 | R152 | SW_SICAP | SICAP | Errores de los usuarios | Carencia de un plan de capacitación. | **225** | Extrema | Reducir | | |
| 3 | R125 | SI_SWEB | Servidor Web | Errores de los usuarios | Carencia de un plan de capacitación. | **180** | Extrema | Transferir | Capacitación de uso y configuración de servidores | S/.1,050.00 |
| 4 | R106 | SW_SGC | Sistema de Gestión Comercial | Ingeniería social | Carencia de Capacitación sobre Ingeniería Social. | **625** | Extrema | Transferir | Capacitación en ingeniería social | S/.1,000.00 |
| 5 | R65 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Deficiencia en las políticas de copias de seguridad. | **225** | Extrema | Reducir | Definir e implementar política de copias de seguridad | $ 0,0224 por GB |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | R67 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Deficiencia en las políticas de copias de seguridad. | 500 | Extrema | Reducir | | |
| 7 | R61 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de políticas de revisión por muestreo. | 180 | Extrema | Reducir | Definir e implementar política de supervisión por muestreo para los diferentes procesos comerciales | S/.8,082.00 |
| 8 | R90 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de políticas de revisión por muestreo. | 500 | Extrema | Reducir | | |
| 9 | R92 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de políticas de revisión por muestreo. | 500 | Extrema | Reducir | | |
| 10 | R94 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de políticas de revisión por muestreo. | 300 | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 | R96 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de políticas de revisión por muestreo. | **240** | Extrema | Reducir | | |
| 12 | R71 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de Políticas de software mal intencionado. | **225** | Extrema | Reducir | Definir políticas de software malintencionado | S/.271.20 |
| 13 | R86 | SW_SGC | Sistema de Gestión Comercial | Errores de los usuarios | Carencia de un plan de capacitación. | **625** | Extrema | Reducir | Implementar directiva de capacitación del sistema de gestión Comercial | S/.1,000.00 |
| 14 | R81 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | **625** | Extrema | Reducir | Documentar los perfiles de acceso a los diferentes sistemas o equipos e implementar una directiva que describa el procedimiento de asignación del perfil | S/.1,000.00 |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 15 | R88 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 500 | Extrema | Reducir | Implementar plan de gestión de configuración de todos los equipos. | S/.2,660.00 |
| 16 | R104 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | 500 | Extrema | Reducir | | |
| 17 | R59 | SI_SBD | Servidor de Base de Datos | Errores de configuración | Ausencia de Plan de Gestión de Configuración. | 400 | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 18 | R77 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de Plan de Gestión de Configuración. | **225** | Extrema | Reducir | | |
| 19 | R87 | SW_SGC | Sistema de Gestión Comercial | Errores de configuración | Ausencia de Plan de Gestión de Configuración. | **625** | Extrema | Reducir | | |
| 20 | R100 | SW_SGC | Sistema de Gestión Comercial | Errores de mantenimiento / actualización de programas (software) | Ausencia de Plan de Gestión de Configuración. | **300** | Extrema | Reducir | | |
| 21 | R127 | SI_SWEB | Servidor Web | Errores de mantenimiento / actualización de equipos | Ausencia de un plan de mantenimiento de equipos. | **225** | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | (hardware) | | | | | | |
| 22 | R137 | SI_SDNS | Servidor DNS | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. | **135** | Extrema | Reducir | | |
| 23 | R148 | SI_SISA | Servidor ISA | Errores de mantenimiento / actualización de equipos (hardware) | Ausencia de un plan de mantenimiento de equipos. | **135** | Extrema | Reducir | | |
| 24 | R76 | SI_SBD | Servidor de Base de Datos | Errores de mantenimiento / actualización de equipos (hardware) | Carencia de un plan de mantenimiento preventivo. | **225** | Extrema | Reducir | Implementar plan de mantenimiento preventivo | S/.295,909.00 |
| 25 | R23 | HW_PC | Estación de Trabajo | Fuga de información | Ausencia de un plan de seguridad. | **180** | Extrema | Reducir | Implementar plan de seguridad | S/.126,496.00 |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 26 | R60 | SI_SBD | Servidor de Base de Datos | Fuga de información | Ausencia de un plan de seguridad. | 400 | Extrema | Reducir | | |
| 27 | R70 | SI_SBD | Servidor de Base de Datos | Difusión de software dañino | Ausencia de un plan de seguridad. | 225 | Extrema | Reducir | | |
| 28 | R89 | SW_SGC | Sistema de Gestión Comercial | Fuga de información | Ausencia de un plan de seguridad. | 500 | Extrema | Reducir | | |
| 29 | R154 | SW_SICAP | SICAP | Fuga de información | Ausencia de un plan de seguridad. | 100 | Extrema | Reducir | | |
| 30 | R155 | SW_SICAP | SICAP | Introducción de falsa información | Falta de un plan de seguridad | 200 | Extrema | Reducir | | |
| 31 | R156 | SW_SICAP | SICAP | Alteración de la información | Falta de un plan de seguridad | 200 | Extrema | Reducir | | |
| 32 | R157 | SW_SICAP | SICAP | Corrupción de la información | Falta de un plan de seguridad | 200 | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 33 | R158 | SW_SICAP | SICAP | Destrucción de la información | Falta de un plan de seguridad | **200** | Extrema | Reducir | | |
| 34 | R162 | SW_SICAP | SICAP | Ingeniería social | Falta de políticas de seguridad | **250** | Extrema | Reducir | | |
| 35 | R149 | SI_SISA | Servidor ISA | Pérdida de Equipos | Ausencia de un plan de seguridad. | **225** | Extrema | Reducir | Implementar plan de seguridad | S/.126,496.00 |
| 36 | R83 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un plan de auditoría de accesos. | **375** | Extrema | Reducir | Implementar proceso de auditoría de base de datos | S/.3,580.00 |
| 37 | R160 | SW_SICAP | SICAP | Acceso no autorizado | Falta de políticas de control de acceso | **200** | Extrema | Reducir | | |
| 38 | R62 | SI_SBD | Servidor de Base de Datos | Introducción de falsa información | Carencia de un plan de supervisión. | **180** | Extrema | Reducir | Implementar un plan de supervisión. | S/.8,082.00 |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 39 | R63 | SI_SBD | Servidor de Base de Datos | Alteración de la información | Carencia de un plan de supervisión. | **625** | Extrema | Reducir | | |
| 40 | R64 | SI_SBD | Servidor de Base de Datos | Corrupción de la información | Carencia de un plan de supervisión. | **225** | Extrema | Reducir | | |
| 41 | R66 | SI_SBD | Servidor de Base de Datos | Destrucción de la información | Carencia de un plan de supervisión. | **500** | Extrema | Reducir | | |
| 42 | R68 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un plan de supervisión. | **300** | Extrema | Reducir | | |
| 43 | R91 | SW_SGC | Sistema de Gestión Comercial | Introducción de falsa información | Carencia de un plan de supervisión. | **500** | Extrema | Reducir | | |
| 44 | R93 | SW_SGC | Sistema de Gestión Comercial | Alteración de la información | Carencia de un plan de supervisión. | **500** | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 45 | R95 | SW_SGC | Sistema de Gestión Comercial | Corrupción de la información | Carencia de un plan de supervisión. | **300** | Extrema | Reducir | | |
| 46 | R97 | SW_SGC | Sistema de Gestión Comercial | Destrucción de la información | Carencia de un plan de supervisión. | **240** | Extrema | Reducir | | |
| 47 | R170 | SW_SICAP | SICAP | Acceso no autorizado | Ausencia de una fuente de información de perfiles de acceso descritos y autorizados. | **200** | Extrema | Reducir | Documentar los perfiles de acceso a los diferentes sistemas o equipos e implementar una directiva que describa el procedimiento de asignación del perfil | S/.1,000.00 |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 48 | R69 | SI_SBD | Servidor de Base de Datos | Degradación de los soportes de almacenamiento de la información | Carencia de un sistema de información de administración de eventos. | **300** | Extrema | Reducir | Implementar un sistema de administración de eventos. | S/.8,082.00 |
| 49 | R80 | SI_SBD | Servidor de Base de Datos | Abuso de privilegios de acceso | Carencia de un sistema de información de administración de eventos. | **625** | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 50 | R82 | SI_SBD | Servidor de Base de Datos | Acceso no autorizado | Carencia de un sistema de información de administración de eventos. | **375** | Extrema | Reducir | | |
| 51 | R103 | SW_SGC | Sistema de Gestión Comercial | Abuso de privilegios de acceso | Carencia de un sistema de información de administración de eventos. | **625** | Extrema | Reducir | | |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 01 | CÓDIGO INDP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Inventario de Proyectos | | | | |
| **Objetivo:** Identificar proyectos de seguridad que sirvan de tratamiento a los riesgos identificados de acuerdo a la prioridad establecida. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 22/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 06/12/2017 |

| Ítem | Código Riesgo | Código activo | Activo | Amenaza | Vulnerabilidad | Valor Riesgo | Nivel | Acciones | Proyecto | Costo |
|---|---|---|---|---|---|---|---|---|---|---|
| 52 | R105 | SW_SGC | Sistema de Gestión Comercial | Acceso no autorizado | Carencia de un sistema de información de administración de eventos. | 500 | Extrema | Reducir | | |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 61- Ficha de proyecto de capacitación de uso de equipos

| **Proyecto N° 01: "Capacitación de uso de equipos"** | |
|---|---|
| **Alcance** | El presente plan de capacitación brindada por un tercero es de aplicación para el personal cuya labor está relacionada a los procesos de gestión comercial en la empresa EPSEL S.A. |
| **Objetivo** | Reducir el índice de errores de usuario en el ingreso de datos en los sistemas de sistema de gestión comercial y el SICAP. |
| **Riesgo/Clasificación** | R21 |
| **Estimación de Tiempos** | 20 horas. |
| **Requerimientos** | 1. Identificar las partes que componen una computadora.<br>2. Ensamblar una computadora.<br>3. Instalar y configurar software utilitario.<br>4. Brindar un mantenimiento preventivo a los equipos de cómputo.<br>5. Especificar mejoras a equipos computacionales. |
| **PROYECTO** | |

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Mantenimiento y uso de computadoras | 100% | S/ 2,660.00 | Ver anexo 07 |

| | |
|---|---|
| **Unidad Responsable** | Oficina de informática. |
| **Activos afectados** | - Estación de trabajo. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 62- Ficha de proyecto implementar plan de seguridad

| **Proyecto N° 02: "Implementar plan de seguridad"** | |
|---|---|
| **Alcance** | El proyecto de implementación de un plan de seguridad contribuye a mejorar la seguridad en los activos de las EPS. |
| **Objetivo** | - Disminuir la difusión de software dañino.<br>- Reducir fuga de información.<br>- Prevenir la perdida de equipos.<br>- Reducir la manipulación de los datos que impacte negativamente en la gestión del proceso comercial. |
| **Riesgo/Clasificación** | R23/R60/R70/R89/R154/R155/R156/R157/R158/R162/R149 |
| **Estimación de Tiempos** | 6 meses. |
| **Requerimientos** | 1. Formar un comité de gestión de seguridad.<br>2. Obtener el compromiso de alta dirección.<br>3. Identificar la lista de activos de la entidad.<br>4. Evaluar los riesgos que podría tener cada activo de la entidad.<br>5. Definir la priorización de los riesgos de los activos.<br>6. Establecer medidas de protección de los activos en base a los riesgos identificados. |

| **PROYECTO** | | | |
|---|---|---|---|
| **Cotización** | **Cumplimiento (%)** | **Presupuesto (S/)** | **Propuesta** |
| Organismo Supervisor de las Contrataciones del Estado - OSCE | 100% | S/ 126,496.00 | Ver anexo 07 |

| | |
|---|---|
| **Unidad Responsable** | Oficina de Informática. |
| **Activos afectados** | - Impresoras. - Estación de Trabajo. - Servidor de base de datos. - Servidor DHCP. - SICAP. |

Fuente: Propia

| | | |
|---|---|---|
| **Ejecutor** | **Revisor** | **V°B°** |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 63- Ficha de proyecto implementar plan de gestión de configuración de todos los equipos

| **Proyecto N° 03: "Implementar plan de gestión de configuración de todos los equipos"** | |
|---|---|
| **Alcance** | La presente implementación del plan de gestión de configuración de todos los equipos es de aplicación para el servidor de base de datos y el SICDESA relacionados a los procesos de gestión comercial de la empresa EPSEL S.A. |
| **Objetivo** | Identificar y definir claramente el propósito del proyecto de implementación del plan de gestión de configuración para el servidor de base de datos y el SICDESA, los documentos que se redactarán, los plazos y las funciones y responsabilidades del proyecto. |
| **Riesgo/Clasificación** | R59/R77/R87/R100/R127/R137/R148 |
| **Estimación de Tiempos** | 1 mes |
| **Requerimientos** | 1. Elaborar cronograma de verificación de equipos.<br>2. Actualizar inventario de equipos.<br>3. Elaborar lista de cada PC y servidor con sus respectivos sistemas informáticos y utilitarios instalados.<br>4. Monitorear revisión de los equipos. |
| **PROYECTO** | |

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Plan de gestión de configuración de equipos | 100 % | S/ 1000 | Área de informática. |

| | |
|---|---|
| **Unidad Responsable** | Oficina de informática. |
| **Activos afectados** | - Servidor de base de datos.<br>- Sistema de gestión comercial. |

Fuente: Propia

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

Tabla 64- Ficha de proyecto definir e implementar política de supervisión por muestreo para los diferentes procesos comerciales

| Proyecto N° 04: "Definir e implementar política de supervisión por muestreo para los diferentes procesos comerciales" | |
|---|---|
| Alcance | Este proyecto esta aplicada para el personal que está vinculado con el SICDESA y El Servidor de Base de Datos en las EPS. |
| Objetivo | - Reducir la introducción de falsa información.<br>- Evitar la alteración de la información. |
| Riesgo/Clasificación | R61/R90/R92/R94/R96 |
| Estimación de Tiempos | 1 mes. |
| Requerimientos | 1. Recolección de Logs de Eventos y Monitoreo.<br>2. Monitoreo de Logs de Eventos para Cumplimiento Regulatorio.<br>3. Forense de Logs y Búsqueda de logs Crudos en la Información de Logs de Eventos.<br>4. Reportes de los Servidores Windows y las estaciones de trabajo.<br>5. Configura Alertas en Tiempo Real en servidores Windows y Estaciones de Trabajo.<br>6. Compatibilidad en: Windows 2003 Server, Windows 2008, Windows NT, Windows 7.<br>7. Todos los demás sistemas operativos de Windows. |

| PROYECTO | | | |
|---|---|---|---|
| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
| Software de monitoreo de eventos de Windows (Event Log Analyzer) | 100% | S/.8,082 | Ver anexo 07 |

| | |
|---|---|
| Unidad Responsable | Oficina de informática. |
| Activos afectados | - Servidor de base de datos.<br>- Sistema de Gestión Comercial. |

Fuente: Propia

| | | |
|---|---|---|
| | | |
| Ejecutor | Revisor | V°B° |

Tabla 65- Ficha de proyecto implementar un plan de supervisión

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

| Proyecto N° 05: "Implementar un plan de supervisión" | |
|---|---|
| Alcance | La presente implementación del plan de supervisión es de aplicación para el personal relacionados a los procesos de gestión comercial de la empresa EPSEL S.A. |
| Objetivo | Implementar controles de validación en las entradas de datos del sistema. |
| Riesgo/Clasificación | R62/R63/R64/R66/R68/R91/R93/R95/R97 |
| Estimación de Tiempos | 2 meses |
| Requerimientos | Supervisar los equipos con el sistema de gestión comercial:<br>1. Elaborar cronograma de verificación de equipos.<br>2. Elaborar lista de cada PC y servidor con sus respectivos sistemas informáticos y utilitarios instalados.<br>3. Monitorear revisión de los equipos<br>Registro de Log:<br>1. Recolección y supervisión de eventos.<br>2. Monitoreo de eventos para cumplimiento regulatorio.<br>3. Forense y búsqueda de eventos crudos en la información.<br>4. Reportes de los servidores Windows y las estaciones de trabajo<br>5. Configurar alertas en tiempo real en servidores Windows y Estaciones de Trabajo.<br>6. Compatibilidad en: Windows 2012 Server, Windows Vista, Windows 7, Windows 10. |

PROYECTO

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Plan de gestión de configuración de equipos | 30 % | S/ 0 | Área de Informática. |
| Software de monitoreo de eventos Windows (Event Log Analyzer) | 70% | S/.8,082 | Ver Anexo 07 |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

| | |
|---|---|
| Unidad Responsable | Oficina de informática. |
| Activos afectados | - Servidor de base de datos.<br>- Sistema de gestión comercial. |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 66- Ficha de proyecto definir e implementar política de copias de seguridad

| **Proyecto N° 06: "Definir e implementar política de copias de seguridad automatizada"** | | | |
|---|---|---|---|
| **Alcance** | Este proyecto involucra al personal encargado de la gestión del servidor de Base de Datos. | | |
| **Objetivo** | Mantener la seguridad de la información de la base de datos. | | |
| **Riesgo/Clasificación** | R65 / R67 | | |
| **Estimación de Tiempos** | 1 mes | | |
| **Requerimientos** | 1. Reducción de costos innecesarios.<br>2. Implementación sencilla y de interfaz intuitiva.<br>3. Protección contra ransomware.<br>4. Resguardo de información segura. | | |
| **PROYECTO** | | | |
| **Cotización** | **Cumplimiento (%)** | **Presupuesto (S/)** | **Propuesta** |
| Copia de seguridad sencilla y fiable integrada en la nube | 100% | Primer 1 TB (TB)/mes - $0,024 por GB. | Ver anexo 07 |
| **Unidad Responsable** | Oficina de informática. | | |
| **Activos afectados** | - Servidor de base de datos. | | |

Fuente: Propia

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

Tabla 67- Ficha de proyecto implementar un sistema de administración de eventos

| Proyecto N° 07: "Implementar un sistema de administración de eventos" | |
|---|---|
| Alcance | El presente proyecto de implementación de un sistema de administración de eventos relacionados a los procesos de gestión comercial de la empresa EPSEL S.A. |
| Objetivo | Registrar los eventos bajo las políticas del SICDESA y servidor de base de datos. |
| Riesgo/Clasificación | R69 / R80/R82 / R103/R105. |
| Estimación de Tiempos | 1 mes |
| Requerimientos | Supervisar los equipos con el sistema de gestión comercial:<br>1. Elaborar cronograma de verificación de equipos.<br>2. Elaborar lista de cada PC y servidor con sus respectivos sistemas informáticos y utilitarios instalados.<br>3. Monitorear revisión de los equipos<br>Registro de Log:<br>7. Recolección y supervisión de eventos.<br>8. Monitoreo de eventos para cumplimiento regulatorio.<br>9. Forense y búsqueda de eventos crudos en la información.<br>10. Reportes de los servidores Windows y las estaciones de trabajo<br>1. Configurar alertas en tiempo real en servidores Windows y Estaciones de Trabajo.<br>2. Compatibilidad en: Windows 2012 Server, Windows Vista, Windows 7, Windows 10 |

**PROYECTO**

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Software de monitoreo de eventos Windows (Event Log Analyzer) | 100% | S/.8,082 | Ver anexo 07 |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

| | |
|---|---|
| Unidad Responsable | Oficina de informática. |
| Activos afectados | - Servidor de base de datos.<br>- Sistema de gestión comercial. |

Fuente: Propia

Tabla 68- Ficha de proyecto definir políticas de software mal intencionado

| Proyecto N° 08: "Definir políticas de software mal intencionado" | | | |
|---|---|---|---|
| Alcance | Este proyecto involucra al personal encargado de la gestión del servidor de Base de Datos con el fin de evitar el uso de software malintencionado. | | |
| Objetivo | Mantener la seguridad de la información de la base de datos. | | |
| Riesgo/Clasificación | R71 | | |
| Estimación de Tiempos | 1 Mes | | |
| Requerimientos | 1. Gestionar perfiles de seguridad.<br>2. Proteger equipos y servidores de archivos.<br>3. Controlar aplicaciones. | | |
| PROYECTOS | | | |
| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
| Software Kaspersky | 100% | S/ 39595.2 | Ver Anexo07 |
| Unidad Responsable | Oficina de informática. | | |
| Activos afectados | - Servidor de base de datos. | | |

Fuente: Propia

| | | |
|---|---|---|
| | | |
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

Tabla 69- Ficha de proyecto implementar plan de mantenimiento preventivo

| Proyecto N° 09: "Implementar plan de mantenimiento preventivo" | |
|---|---|
| Alcance | El presente proyecto de mantenimiento preventivo es de aplicación para la base de datos del proceso de gestión comercial en la empresa EPSEL S.A. |
| Objetivo | Realizar un procedimiento para el mantenimiento de hardware. |
| Riesgo/Clasificación | R76. |
| Estimación de Tiempos | 12 meses |
| Requerimientos | 1. Supervisar las actividades relacionadas a la operación de la arquitectura de los equipos.<br>2. Elaborar programas aplicativos según requerimientos de los equipos.<br>3. Realizar, programar y supervisar el soporte técnico informático.<br>4. Mantener actualizada la información de los sistemas informáticos. |
| PROYECTOS | |

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Plan de mantenimiento preventivo | 100% | S/. 295 909 | Ver Anexo 07 |

| | |
|---|---|
| Unidad Responsable | Oficina de informática. |
| Activos afectados | - Servidor de base de datos. |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 70- Ficha de proyecto documentar los perfiles de acceso a los diferentes sistemas o equipos e implementar una directiva que describa el procedimiento de asignación del perfil

| **Proyecto N° 11: "Documentar los perfiles de acceso a los diferentes sistemas o equipos e implementar una directiva que describa el procedimiento de asignación del perfil"** | |
|---|---|
| **Alcance** | El presente proyecto es de documentar los perfiles de acceso a los diferentes sistemas o equipos e implementar una directiva que describa el procedimiento de asignación del perfil que involucra los proceso de gestión comercial en la empresa EPSEL S.A. |
| **Objetivo** | Realizar un procedimiento de los perfiles de acceso para los sistemas o equipos e implementar de una directiva. |
| **Riesgo/Clasificación** | R170 |
| **Estimación de Tiempos** | 1 mes |
| **Requerimiento** | 1. Gestionar lista de trabajadores.<br>2. Gestionar Perfiles de trabajadores.<br>3. Documentar privilegios de por perfil. |
| **PROYECTO** | |

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Gestionar perfiles de acceso. (Área de Informática) | 100 % | S/ 1000 | Área de Informática. |

| | |
|---|---|
| **Unidad Responsable** | Oficina de informática. |
| **Activos afectados** | Servidor de base de datos.<br>Sistema de gestión comercial.<br>SICAP. |

Fuente: Propia

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 71- Ficha de proyecto implementar proceso de auditoría de base de datos

| **Proyecto N° 12: "Implementar proceso de auditoría de base de datos"** | |
|---|---|
| **Alcance** | Este proyecto está dirigida al personal encargado de la gestión de base datos. |
| **Objetivo** | Establecer un proceso de monitoreo sobre la información de la base de datos. |
| **Riesgo/Clasificación** | R83/R160 |
| **Estimación de Tiempos** | 1 Mes |
| **Requerimiento** | Servidor de Pruebas:<br>1. Motherboard GIGABYTE GA-B250M-DS3H, LGA1151.<br>2. Procesador Intel Core i7-7700, 3.60 GHz, 8 MB Caché L3, LGA1151.<br>3. Memoria Corsair CMV8GX4M1A2133C15, 8 GB, DDR4, 2133 MHz.<br>4. Unidad de estado sólido Western Digital Blue, 500GB, SATA 6Gb/s, M.2.<br>5. DVD SuperMulti LG GH24NSD1, 24X, interno, SATA.<br>6. Case Thermaltake Versa H23, Mid Tower, 500W, Negro.<br>7. Kit Teclado y Mouse GeniusSlimStar C130, USB, Negro.<br>8. Monitor Advance A-195MS, 19.5" LED, 1600 x 900.<br>9. UPS Elise AUR-650, interactivo, 650VA, 360W, 162~290 VAC, 6 tomas NEMA. |

| **PROYECTO** | | | |
|---|---|---|---|
| **Cotización** | **Cumplimiento (%)** | **Presupuesto (S/)** | **Propuesta** |
| Servidor de pruebas | 70% | S/ 3580.00 | Ver anexo 7 |

| | |
|---|---|
| **Unidad Responsable** | Oficina de informática. |
| **Activos afectados** | Servidor de base de datos. |

Fuente: Propia

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 72- Ficha de proyecto implementar directiva de capacitación del sistema de gestión comercial

| **Proyecto N° 13: "Implementar directiva de capacitación del sistema de gestión Comercial"** | |
|---|---|
| **Alcance** | El presente proyecto es de implementar por el área de informática la directiva de capacitación del sistema de gestión comercial en la empresa EPSEL S.A. |
| **Objetivo** | Redactar e implementar por el área de informática la directiva de capacitación del sistema de gestión comercial. |
| **Riesgo/Clasificación** | R86 |
| **Estimación de Tiempos** | 1 mes |
| **Requerimiento** | 1. Analizar el proceso de gestión comercial.<br>2. Analizar subprocesos de gestión comercial.<br>3. Relacionar el proceso de la gestión comercial con los demás procesos.<br>4. Diseñar un flujograma del sistema de gestión comercial. |
| **PROYECTO** | |

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Implementar directivas de capacitación del Sistema de Gestión Comercial. | 100% | S/ 1000 | Ver anexo 7 |

| | |
|---|---|
| **Unidad Responsable** | Oficina de informática. |
| **Activos afectados** | Sistema de gestión comercial. |

Fuente: Propia

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

Tabla 73- Ficha de proyecto capacitación en ingeniería social

| Proyecto N° 14: "Capacitación en ingeniería social" | | | |
|---|---|---|---|
| Alcance | Este proyecto está dirigido al personal de todas las oficinas de las EPS, con la finalidad de concientizar la confidencialidad de la información. | | |
| Objetivo | Establecer una conducta confidencial del personal sobre la información. | | |
| Riesgo/Clasificación | R106. | | |
| Estimación de Tiempos | 2 Semanas. | | |
| Requerimiento | 1. Definir términos de ingeniería social<br>2. Implementar escenarios basados en ingeniería social.<br>3. Concientizar al personal sobre los posibles ataques que se pueden producir mediante la ingeniería social.<br>4. Realizar talleres hasta cumplir el objetivo de concientización. | | |
| PROYECTO | | | |
| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
| Capacitación en ingeniería social | 100% | S/. 1000 | Área de Informática |
| Unidad Responsable | Oficina de informática. | | |
| Activos afectados | Sistema de gestión comercial. | | |

Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __/____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | **TIPO** | TABLA |
| **Actores** | Oficina de Informática Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 12/12/2017 |

Tabla 74- Ficha de proyecto capacitación de uso y configuración de servidores

| **Proyecto N° 15: "Capacitación de uso y configuración de servidores"** | |
|---|---|
| **Alcance** | El presente proyecto de capacitación de uso y configuración del servidor web a través de un proveedor externo para el área de informática de la empresa EPSEL S.A. |
| **Objetivo** | Contratar el servicio de un tercero para brindar la capacitación de uso y configuración de servidor web. |
| **Riesgo/Clasificación** | R125 |
| **Estimación de Tiempos** | 2 meses |
| **Requerimiento** | 1. Implementación y administración de Windows Server 2012.<br>2. Implementación de la virtualización de servidores con Hyper-V.<br>3. Implementación de Active Directory Domain Services.<br>4. Administración de los Objetos de Dominio de Active Directory.<br>5. Implementación de IPv4 Sesión.<br>6. Implementación de DHCP.<br>7. Implementación de DNS, WINS.<br>8. Implementación de directivas de grupo GPOs.<br>9. Gestión de Virtualización – Hyper-V.<br>10. Gestión de GPOs.<br>11. Implementación Acceso Remoto.<br>12. Implementación IIS, WEB, FTP. |
| **PROYECTO** | |

| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
|---|---|---|---|
| Diplomado Windows Server 2012 | 100 % | S/ 1050.00 | Ver Anexo 7 |

| | |
|---|---|
| **Unidad Responsable** | Oficina de informática. |
| **Activos afectados** | Servidor web. |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 02 | CÓDIGO FIPR N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Ficha de proyecto | | | | |
| **Objetivo:** Realizar el llenado de la ficha del proyecto con los datos generales del proyecto a ejecutar. | | | | TIPO | TABLA |
| Actores | Oficina de Informática Equipo de Análisis | Elaborado Por: | EPEÑA | Fecha Elaboración | 23/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 12/12/2017 |

Tabla 75- Ficha de proyecto implementar plan de mantenimiento de equipos

| Proyecto N° 16: "Implementar plan de Mantenimiento de equipos" | | | |
|---|---|---|---|
| Alcance | Este proyecto está dirigido al personal de la oficina de informática de la EPS, con el fin de tener las capacidades y habilidades de realizar el mantenimiento de los equipos. | | |
| Objetivo | Implementar un plan de mantenimiento de equipos. | | |
| Riesgo/Clasificación | R59/R77/R87/R100/R127 / R137 / R148 | | |
| Estimación de Tiempos | 1 Semana | | |
| Requerimiento | 1. Identificar las partes que componen una computadora.<br>2. Ensamblar una computadora.<br>3. Instalar y configurar software utilitario.<br>4. Brindar un mantenimiento preventivo a los equipos de cómputo.<br>5. Especificar mejoras a equipos computacionales. | | |
| PROYECTO | | | |
| Cotización | Cumplimiento (%) | Presupuesto (S/) | Propuesta |
| Mantenimiento y uso de computadoras | 100% | S/ 2,660.00 | Ver anexo 07 |
| Unidad Responsable | Oficina de informática. | | |
| Activos afectados | Sistema de gestión comercial. | | |

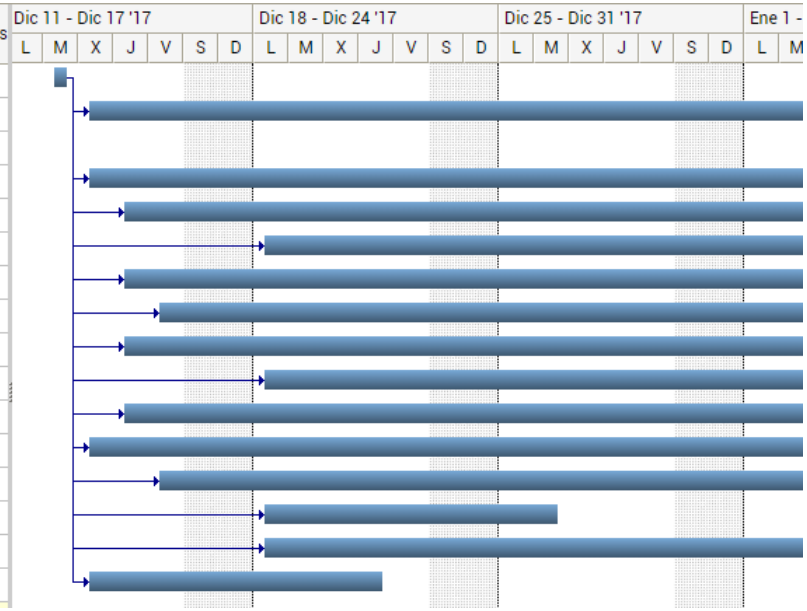
Fuente: Propia

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

| LOGO | Fase: 06 | Proceso: 01 | Actividad: 03 | CÓDIGO CDPE N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Cronograma del plan de ejecución | | | | |
| **Objetivo:** Establecer el cronograma de ejecución de los proyectos identificados. | | | | **TIPO** | DIAGRAMA DE GANTT |
| **Actores** | Oficina de Informática<br>Equipo de Análisis | **Elaborado Por:** | EPEÑA | **Fecha Elaboración** | 23/10/2017 |
| **Revisado Por:** | JSEGURA | **Aprobado Por:** | JSEGURA | **Fecha Aplicación** | 18/12/2017 |

Tabla 76- Cuadro de cronograma de ejecución del plan

| | Nombre | Duración | Inicio | Fin | Predecesoras |
|---|---|---|---|---|---|
| 1 | Capacitación de uso de equipos | 1día? | 12/12/2017 | 12/12/2017 | |
| 2 | Implementar Plan de Seguridad | 131días? | 13/12/2017 | 13/06/2018 | 1 |
| 3 | Implementar plan de gestión de configuración de todos l | 22días? | 14/06/2018 | 13/07/2018 | 2 |
| 4 | Definir e implementar política de supervisión por muestre | 24días? | 13/12/2017 | 15/01/2018 | 1 |
| 5 | Implementar un plan de supervisión | 23días? | 14/12/2017 | 15/01/2018 | 1 |
| 6 | Definir e implementar política de copias de seguridad | 25días? | 18/12/2017 | 19/01/2018 | 1 |
| 7 | Implementar un sistema de administración de eventos | 84días? | 14/12/2017 | 10/04/2018 | 1 |
| 8 | Definir políticas de software malintencionado | 45días? | 15/12/2017 | 15/02/2018 | 1 |
| 9 | Implementar plan de mantenimiento preventivo | 29días? | 14/12/2017 | 23/01/2018 | 1 |
| 10 | Revisar y mejorar la política de rotación de personal | 45días? | 18/12/2017 | 16/02/2018 | 1 |
| 11 | Documentar los perfiles de acceso a los diferentes siste | 29días? | 14/12/2017 | 23/01/2018 | 1 |
| 12 | Implementar proceso de auditoría de base de datos | 29días? | 13/12/2017 | 22/01/2018 | 1 |
| 13 | Implementar directiva de capacitación del Sistema de ge | 29días? | 15/12/2017 | 24/01/2018 | 1 |
| 14 | Capacitación en Ingeniería Social | 7días? | 18/12/2017 | 26/12/2017 | 1 |
| 15 | Capacitación de uso y configuración de servidores | 29días? | 18/12/2017 | 25/01/2018 | 1 |
| 16 | Implementar plan de Mantenimiento de equipos | 7días? | 13/12/2017 | 21/12/2017 | 1 |




Fuente: Propia

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

Tabla 77 - Listado de Indicadores a evaluar por proyecto

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| Capacitación de uso de equipos | R21 | ✓ Número de incidentes en falla de equipos por error humano | Mensual | | | | | |
| Capacitación de uso y configuración de servidores | R125 | ✓ Cantidad de Incidentes por falla de configuración de servidores<br>✓ Tiempo Promedio de Servicio Web fuera de línea | Mensual | | | | | |
| Capacitación en ingeniería social | R106 | ✓ Cantidad de incidentes de acceso no autorizado<br>✓ Cantidad de ataques externos detectados | Mensual | | | | | |
| Definir e implementar política de copias de seguridad | R65 - R67 | ✓ Porcentaje de la muestra con errores de consistencia<br>✓ Porcentaje de la muestra con alteración de registros<br>✓ Cantidad de registros eliminados sin sustento<br>✓ Porcentaje de tareas ejecutadas correctamente.<br>✓ Porcentaje de copias de seguridad | Mensual | | | | | |

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| | | que han sido probadas y son operables<br>✓ Número de caídas de la base de datos y tiempo promedio de recuperación | | | | | | |
| Definir e implementar política de supervisión por muestreo para los diferentes procesos comerciales | R61 - R90 - R92 - R94 - R96 | ✓ Cantidad de supervisiones programas por proceso<br>✓ Cantidad de supervisiones ejecutadas por proceso<br>✓ Porcentaje de la muestra con errores de consistencia por proceso<br>✓ Porcentaje de la muestra con alteración de registros por proceso | Mensual | | | | | |
| Definir políticas de software malintencionado | R71 | ✓ Índice de rendimiento (cantidad de consultas atendidas)<br>✓ Tiempo promedio de respuesta<br>✓ Índice de accesos no autorizados | Mensual | | | | | |

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ✓ Porcentaje de la muestra con errores de consistencia de información<br>✓ Porcentaje de la muestra con evidencias de alteración información<br>✓ Tiempo promedio de operatividad | | | | | | |
| Documentar los perfiles de acceso a los diferentes sistemas o equipos e implementar una directiva que describa el procedimiento de asignación del perfil | R81 - R88 - R104 - R160 - R161 | ✓ Cantidad de accesos no autorizados<br>✓ Índice de variación de asignación de perfiles de accesos<br>✓ Porcentaje de la muestra con errores de perfil de acceso<br>✓ Porcentaje de la muestra problemas de configuración del perfil de acceso.<br>✓ Índice de perfiles activos versus personal en actividad<br>✓ Cantidad de accesos por rangos | Mensual | | | | | |

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| | | horarios | | | | | | |
| Implementar directiva de capacitación del sistema de gestión comercial | R86 | ✓ Cantidad de incidentes atendidos por errores de usuario.<br>✓ Tiempo promedio de atención ante un incidente. | Mensual | | | | | |
| Implementar plan de gestión de configuración de todos los equipos | R59 - R77 - R87 - R100 | ✓ Cantidad de equipos sin actualización vigente.<br>✓ Cantidad de incidentes por errores de configuración. | Bimestral | | | | | |
| Implementar plan de mantenimiento de equipos | R127 - R137 - R148 | ✓ Porcentaje de cumplimiento del plan de mantenimiento.<br>✓ Cantidad de incidentes por falta de mantenimiento. | Semestral | | | | | |
| Implementar plan de mantenimiento preventivo | R76 | ✓ Porcentaje de cumplimiento del plan de mantenimiento.<br>✓ Cantidad de incidentes por falta de mantenimiento. | Trimestral | | | | | |

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| Implementar plan de seguridad | R23 - R60 - R70 - R89 - R149 - R152 - R154 - R155 - R156 - R157 - R158 - R162 | ✓ Cantidad de caídas del servidor<br>✓ Cantidad de quejas de usuarios por incidentes de seguridad<br>✓ Porcentaje de equipos con software no licenciado<br>✓ Indicie de nivel de servicio<br>✓ Cantidad de accesos no autorizados<br>✓ Cantidades denegaciones de servicio. | Trimestral | | | | | |
| Implementar proceso de auditoría de base de datos | R83 | ✓ Cantidad de accesos no autorizados<br>✓ Porcentaje de la muestra problemas de configuración del perfil de acceso.<br>✓ Índice de perfiles activos versus personal en actividad<br>✓ Cantidad de accesos por rangos | Mensual | | | | | |

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| | | horarios | | | | | | |
| Implementar un plan de supervisión | R62 - R63 - R64 - R66 - R68 - R91 - R93 - R95 - R97 | ✓ Porcentaje de la muestra con errores de consistencia<br>Porcentaje de la muestra con alteración de registros<br>Cantidad de registros eliminados sin sustento<br>✓ Índice de crecimiento de los archivos físicos de la base de datos | Mensual | | | | | |
| Implementar un sistema de administración de eventos | R69 - R82 - R105 | ✓ Índice de crecimiento de los archivos físicos de la base de datos<br>✓ Cantidad de accesos no autorizados<br>✓ Porcentaje de la muestra problemas de configuración del perfil de acceso. | Mensual | | | | | |
| Revisar y mejorar la | R80 - | ✓ Cantidad de accesos no | Mensual | | | | | |

| LOGO | Fase: 07 | Proceso: 01 | Actividad: -- | CÓDIGO LIEP N°___ | Pág. __ /____ |
|---|---|---|---|---|---|
| | Lista de control de indicadores a evaluar por proyecto | | | | |
| **Objetivo:** Determinar el listado de indicadores a evaluar por proyecto | | | | TIPO | TABLA |
| Actores | Oficina de Informática<br>Equipo de Análisis | Elaborado Por: | MSOTO | Fecha Elaboración | 24/10/2017 |
| Revisado Por: | JSEGURA | Aprobado Por: | JSEGURA | Fecha Aplicación | 19/12/2017 |

| Proyecto | Riesgos Tratados | Indicadores a Evaluar | Periodicidad de Evaluación | Fecha de Control / Número Ficha Monitoreo/Responsable | | | | |
|---|---|---|---|---|---|---|---|---|
| política de rotación de personal | R103 | autorizados<br>✓ Porcentaje de la muestra problemas de configuración del perfil de acceso. | | | | | | |

Fuente: Propia

Nota: El cuadro no contiene información del seguimiento de los proyectos propuestos debido, a la fecha de la presentación de la presente, la empresa que se tomó como caso de estudio no ha implementado ninguno, ya que no han sido incluidos en el presupuesto anual.

| | | |
|---|---|---|
| Ejecutor | Revisor | V°B° |

# CAPÍTULO V: CONCLUSIONES

1. En la presente tesis se propuso el modelo de gestión de riesgos de TI que contribuya a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú, que se validó por 03 profesionales expertos, quienes aceptaron el modelo validando las características de flexibilidad y simplificación de procesos que promuevan la gestión de riesgos de TI en este tipo de empresa, como se muestra en el análisis de resultados. (Anexo N° 04 y Anexo N°5), De la aplicación del Método Alfa de Cronbach para estimar la fiabilidad del modelo propuesto se ha obtenido un coeficiente de confianza de 0.909, que de acuerdo a la escala de George y Mallery (2003, p. 231) manejada para este modelo, corresponde a un modelo "excelente". Mientras que, de la aplicación del coeficiente de Kendall se ha obtenido 0.994 que indica que la hipótesis es aceptada debido a que existe una fuerte asociación entre las clasificaciones y los valores estándar asignados por los profesionales expertos que evaluaron el modelo.Finalmente, concluir que, de la combinación de los resultados de los dos métodos aplicados para la evaluación, se puede indicar existe una alto nivel de concordancia entre los 03 evaluadores expertos y por el valor obtenido con la aplicación del método de Alfa de Cronbanch, el modelo alcanza un nivel de excelente.

2. El modelo propuesto, en la presente tesis, se aplicó en la empresa prestadora de servicios de saneamiento de Lambayeque como caso de estudio, verificando que es posible contribuir como la operación de los procesos de gestión comercial, debido a que fue posible identificar 165 riesgos cuya materialización podría afectar la operación de los procesos de gestión comercial de esta empresa. Estos riesgos, se colocaron en una matriz semaforizada (Tabla N°55) en base a la cual se pudo obtener el cuadro de priorización de riesgos de TI (Tabla N°56), y de esta manera 52 riesgos categorizados como de alta prioridad, permitiendo de esta forma apoyar a la efectiva toma de decisiones.

3. Así también, con la aplicación del modelo de gestión de riesgos de TI desarrollado en la presente tesis, en el caso de estudio, se logró formular 16 proyectos que permiten dar tratamiento a los 52 riesgos calificados como de alta prioridad, promoviendo de esta manera una toma de decisiones de carácter proactivo y evitando el comportamiento reactivo que acarrea consigo los costos de corregir los efectos de un riesgo de TI materializado.

4. Finalmente, con la aplicación del modelo de gestión de riesgos de TI propuesto, se demuestra que con características de procesos simplificados es posible mapear los 165 riesgos identificados, en un esquema de priorización, con una lectura semaforizada que permite al encargado de la gestión de las tecnologías de información, proponer proyectos para el tratamiento de los mismos de manera proactiva, definiendo los recursos requeridos y las actividades de mejora continua.

# REFERENCIAS BIBLIOGRÁFICAS

[1]Ponemon Institute. 2017. Cost Data Breach Study. https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

[2]El comercio. 2018. Whatsapp sufre una caída mundial basada en un profundo cambio. http://www.elcomercio.es/tecnologia/201705/04/whatsapp-caida-mundial-basada-20170504043123.html

[3]Deloitte. 2018. Lecciones tras la caída de Whatsapp https://www2.deloitte.com/do/es/pages/risk/articles/lecciones-tras-la-caida-de-whatsapp.html

[4]La prensa gráfica. 2018. "Esto es un error de estudiante de primer año de informática": 5 datos claves para entender el "error humano" de Smartmatic en la elecciones 2018. https://www.laprensagrafica.com/techlife/Esto-es-un-error-de-estudiante-de-primer-ano-de-informatica-5-datos-claves-para-entender-el-error-humano-de-Smartmatic-en-las-Elecciones-2018-20180306-0049.html

[5]RPP Noticias. 2014. Caída del sistema genera aglomeración de pasajeros en el Jorge Chávez. http://rpp.pe/lima/actualidad/caida-de-sistema-genera-aglomeracion-de-pasajeros-en-el-jorge-chavez-noticia-694161

[6]Oficina de asuntos del consumidor de la casa blanca. Capítulo 15. Influencia del consumidor y difusión de las innovaciones. 515. https://books.google.com.pe/books?id=Wqj9hlxqW-

IC&pg=PA515&dq=oficina+de+Asuntos+del+Consumidor+de+la+casa+blanca&hl=es-419&sa=X&ved=0ahUKEwi0nsGU--fZAhUN7lMKHXpMBtEQ6AEILTAB#v=onepage&q=oficina%20de%20Asuntos%20del%20Consumidor%20de%20la%20casa%20blanca&f=false

[7]EY. 2017. El camino hacia la resiliencia cibernética. http://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resiliencia-cibernetica/$FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf

[8] NATO Alliance Ground Surveillance Management Agency (NAGSMA). 2013. Bélgica. Implementando un estándar de gestión de riesgos.

[9] Vanegas G, 2014, "Hacia un modelo para la gestión de riesgos de TI en MiPyMES: MOGRIT"

[10]Celi E., 2014, Lambayeque. "Un modelo para la gestión de TI en las empresas microfinancieras: caso Lambayeque, Perú"

[11] Molina, M. 2015. Madrid. Propuesta de un plan de gestión de riesgos de tecnología superior politécnica. http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

[12] Murillo Ch. y S. Rivas, 2015, Colombia. Propuesta metodológica para la gestión del riesgo en microempresas comercializadoras de electrodomésticos basada en los modelos ISO 31000:2011 y OHSAS 18001:2007. https://repositorio.escuelaing.edu.co/bitstream/001/226/1/EC-Especializaci%C3%B3n%20en%20Gestion%20Integrada%20QHSE-1072493699.pdf

[13]Arangurí, M., R. Iman y G. León, 2016, Chiclayo. Modelo de gestión de riesgos de TI basados en estándares adaptados a las TI que soportan los procesos para contribuir a la generación de valor en las universidades privadas de la región Lambayeque.

[14]Chillogallo, E., V. Zambrano, 2016, Quito. Elaboración de un modelo de gestión de riesgos de tecnologías de información para la fiscalía general del estado.

[15]Coronel, K., 2017, Ecuador. Modelo de gobierno y gestión de TI para industrias farmacéuticas ecuatorianas, tomando como referencia las mejores prácticas de manufactura y gobierno de TI. Caso de estudio: Laboratorios industriales farmacéuticos ecuatorianos (LIFE)

[16]Instituto de Auditores Internos. 2013. España. Definición e implantación de apetito de riesgo. 15-16. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

[17]Instituto de Auditores Internos. 2013. España. Definición e implantación de apetito de riesgo. 16. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

[18]Instituto de Auditores Internos. 2013. España. Definición e implantación de apetito de riesgo. 16. https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

[19] Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México-

Edición Única. 23-25.

https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

[20] Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México- Edición Única. 28-29. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

[21] Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México- Edición Única. 29-30. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

[22] Guerra M., Tecnológico de Monterrey, 2006. Resumen de la tesis: evaluación del riesgo informático ponderado y su implantación en el campus estado México- Edición Única. 32-36. https://repositorio.itesm.mx/ortec/bitstream/11285/567630/1/DocsTec_4892.pdf

[23]Sunass: «El Plan Maestro Optimizado permite tomar decisiones acertadas de tarifas», 2016, http://www.otass.gob.pe/noticia.php?idnoticia=46

# ANEXOS

## Anexo N° 01: Encuesta para determinar la importancia de los activos que contribuyen a la continuidad de la operación de los procesos comerciales

| Encuesta para determinar la importancia de los activos que contribuyen a la continuidad de la operación de los Procesos Comerciales | | | Pág. ____ /_____ |
|---|---|---|---|
| **Objetivo:** | **Identificar que activos contribuyen a la continuidad en la operación de los procesos comerciales.** | | |
| **Entidad:** | **Área** | **Puesto** | **Fecha** |

| N° | Paso 1: identifique los activos[1] importantes para la operación de los procesos comerciales | Paso 2: Determine el grado de importancia de los activos mencionados en el paso 1. (1 = Muy Alta, 2 = Alta, 3 = Regular, 4= Baja, 5=Muy Baja) | Paso 3: Describa brevemente las situaciones en las que estos activos se ven amenazados[2]. | Paso 4. Para cada uno de los siguientes criterios, determine los requerimientos de seguridad cada activo | | | Paso 5: Indique que estrategias se utilizan actualmente para la protección del activo citado y defina aceptables y tolerables ante la presencia de un incidente. |
|---|---|---|---|---|---|---|---|
| | | | | Confidencialidad[3] | Integridad[4] | Disponibilidad[5] | |
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |

**1** Un activo es algo que la Organización tiene o usa y que, si es perdido o dañado, causaría un daño a la Organización.
2 Cualquier cosa que puede suceder y cuando ocurre tiene consecuencias negativas sobre el valor del activo.
3 Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
4 Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
5 Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

## Anexo N° 02: Encuesta de gestión de riesgos de tecnologías de información en la empresa

**Objetivo:** Identificar el nivel de riesgos de tecnologías de información aplicado en la institución.

**Instrucciones:** A continuación se le presentará una serie de afirmaciones relacionadas a la Gestión de Riesgos de Tecnologías de la información. De acuerdo a su experiencia, marque una (X) en la columna que corresponda a la escala de calificación que otorgaría a su empresa. En caso requiera hacer alguna aclaración puntual sobre el tema, sírvase usar la columna "Observaciones".

| N | Preguntas | Nunca | A veces | Con Frecuencia | Siempre |
|---|---|---|---|---|---|
| Evaluar la gestión de riesgos | | | | | |
| 1 | ¿Determina la empresa el nivel de riesgos relacionados con las TI que está dispuesta a asumir para cumplir con sus objetivos? | | | | |
| 2 | ¿Frente a los niveles de riesgo y oportunidad aceptables, la empresa evalúa y aprueba propuestas de umbrales de tolerancia al riesgo de TI? | | | | |
| 3 | ¿Determina la empresa el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales? | | | | |
| 4 | ¿Con que frecuencia se evalúa los factores de riesgo de TI con anterioridad a las decisiones estratégicas de la empresa pendientes y se asegura que las decisiones de la empresa se toman conscientes de los riesgos? | | | | |
| 5 | ¿Con que frecuencia determina si el uso de TI está sujeto a una valoración y evaluación de | | | | |

| N | Preguntas | Nunca | A veces | Con Frecuencia | Siempre |
|---|---|---|---|---|---|
| | riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes? | | | | |
| 6 | ¿Con que frecuencia la empresa evalúa las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos? | | | | |
| Orientar la gestión de riesgos. | | | | | |
| 7 | ¿Promueve una cultura consciente de los riesgos TI e impulsa a la identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio? | | | | |
| 8 | ¿Orienta la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas? | | | | |
| 9 | ¿Con que frecuencia se orienta a la elaboración de planes de comunicación de riesgos, así como los planes de acción de riesgo? | | | | |
| 10 | ¿Con que periodicidad se orienta la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y se notifica a los niveles adecuados de | | | | |

| N | Preguntas | Nunca | A veces | Con Frecuencia | Siempre |
|---|---|---|---|---|---|
| | gestión? | | | | |
| Supervisar la gestión de riesgos | | | | | |
| 11 | ¿Con que regularidad, se supervisa hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo? | | | | |
| 12 | ¿Con que regularidad se supervisan las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos? | | | | |
| 13 | ¿Se facilita la revisión por las partes interesadas del progreso de la empresa hacia los objetivos identificados? | | | | |
| 14 | ¿Se Informa cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección? | | | | |

# Anexo N° 03: Matrices de juicio de expertos

**MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS**

**Objetivo:** la matriz de consistencia, tiene como objetivo, contrastar la validez del modelo de gestión de riesgos de TI que apoya en la operación de los procesos de gestión comercial de las empresas de saneamiento del norte del Perú. El modelo propuesto se enfoca en brindar al usuario, a partir de la investigación de las distintas metodologías y estándares de gestión de riesgos de TI, un modelo simple y flexible que promueva su aplicación, con la intención de que se desarrolle una cultura organizacional de acción preventiva en la gestión de riesgos de tecnologías de información en las empresas de saneamiento.

Escala: (1) En total desacuerdo (2) En desacuerdo (3)Ni de acuerdo ni de desacuerdo (4) De acuerdo (5)Totalmente de acuerdo

Procedimiento: Marcar con X la opción elegida

| Procesos | Objetivo | Descripción del Indicador | Escala | | | | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | |
| **Fase 1: Definir el Contexto** | | | | | | | | |
| Definir Contexto Interno | Definir parámetros básicos internos para alcanzar los objetivos estratégicos de la organización. | Nivel de elementos por factor (cultural, normativo,partes internas involucradas, recursos, estructura, metas y objetivos , valores). | | | | X | | |
| Definir Contexto Externo | Definir parámetros básicos externos para alcanzar los objetivos estratégicos de la organización. | Nivel de elementos por factor (Ambiente de negocio, normativo y político, finaciero). | | | | X | | |
| **Fase 2: Crear Perfil de Activos** | | | | | | | | |
| Identificar los conocimientos de dirección | Captar el conocimiento desde el punto de vista de la alta dirección para identificar los activos importantes, las áreas que estan involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales. | Cantidad de activos identificados. | | | | | X | |
| | | Nivel de identificación de requimientos de seguridad. | | | | | X | |
| Identificar los conocimientos en el área de gestión operativa | Captar el conocimiento desde el punto de vista de los gerentes y jefaturas, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales. | Cantidad de activos identificados. | | | | | X | |
| | | Nivel de identificación de requimientos de seguridad. | | | | | X | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Identificar los conocimientos de personal | Captar el conocimiento desde el punto de vista del personal operativo, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales. | Cantidad de activos identificados.<br>Nivel de identificación de requimientos de seguridad. | | | | | X | |
| Identificar activos a gestionar | Determinar los activos de mayor importancia, de acuerdo al puntaje obtenido desde los distintos puntos organizacionales: dirección, gestión operativa y personal. | Porcentaje de activos que superan la media de la valorización. | | | | | X | |
| **Fase 3: Identificar los Riesgos** | | | | | | | | |
| Clasificación de Activos | Clasificar los activos críticos, identificados en la fase 2, en las categorías establecidas por el método MAGERIT. | Cantidad de activos clasificados por categoría. | | | | | X | |
| Dependencia de Activos | Identificarlos activos y establecer la relación de dependencia. | Numero de relaciones de dependencia identificada entre activos. | | | | X | | |
| Valoración de Activos | Valorar el grado de importancia de cada activos teniendo en cuenta criterios de disponibilidad, integridad y confidencialidad. | Número de criteros determinados. | | | | | X | |
| | | Número de escalas suficientes para calcular criticidad de activos. | | | | | X | |
| | | Nivel de simplicidad para determinar la valorización de los activos identificados. | | | | | X | |
| Identificación de las Amenazas y Vulnerabilidades | Identificar las vulnerabilidades y amenazas de los activos valorizados en la actividad anterior. | Nivel de simplicidad para determinar las vulnerabilidades y amenazas para cada activo. | | | | | X | |
| **Fase 4: Analisis de Riesgos** | | | | | | | | |
| Determinación de Probabilidad | Determinar el valor de la probabilidad de que una amenaza se materialice a causa de una determinada vulnerabilidad. | Número de valores suficientes para determinar la probalidad o frecuenta de ocurrencia. | | | | | X | |
| Analisis de Impacto | Medir los efectos adversos resultantes de la materialización de una amenaza para cada uno de los riesgos identificados para cada activo crítico. | Número de valores suficientes para determinar el nivel de impacto. | | | | | X | |
| Determinación del riesgo | Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza. | Nivel de simplicidad para determinar el valor total del riesgo. | | | | | X | |
| **Fase 5: Evaluación del riesgo** | | | | | | | | |
| Elaboración de la matriz de clasificación del riesgo | Clasificar a los riesgos según su prioridad de tratamiento. | Número de categorías de riesgo suficiente para la valorización. | | | | | X | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Valorización del riesgo | Evaluar mediante la medición de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible, y la probabilidad que dicha pérdida o daño llegue a ocurrir. | Nivel de simplicidad para determinar la valorización del riesgo frente a los niveles de apetito y tolerancia determinados. | | | | | X | |
| **Fase 6: Políticas y administración de Riesgos** | | | | | | | | |
| Plan de seguridad | Identificación de proyectos de seguridad. | Nivel de suficiencia con respecto a las denominaciones de evitar, mitigar, transferir y aceptar para las estrategias de tratamiento. | | | | X | | |
| | Plan de Ejecución. | Número de criterios suficientes para la formulación de proyectos. | | | | X | | |
| **Fase 7: Monitorización y Revisión** | | | | | | | | |
| Monitoreo | Ejecutar para obtener datos para el procesamiento de los indicadores. | Nivel de simplicidad para identificar acciones para el procesamiento de indicadores. | | | | X | | |
| | Identificar las características del objetivo del proyecto para determinar el indicador de medición. | Nivel de simplicidad para identificar las variables a controlar. | | | | X | | |
| | Identificar la medida de lo logrado en la aplicación del procesamiento. | Nivel de simplicidad para identificar los indicadores. | | | | X | | |
| Revisión | Identificar medidas correctivas para mejorar los resultados obtenidos. | Nivel de simplicidad para identificar las medidas correctivas. | | | | X | | |

| | |
|---|---|
| **DISCONFORMIDAD** | |
| **OBSERVADO** | |
| **ACEPTACIÓN** | X |

**MGRT. ERNESTO KARLO CELI ARÉVALO**
**Profesional Experto**

## MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

**Objetivo:** la matriz de consistencia, tiene como objetivo, contrastar la validez del modelo de gestión de riesgos de TI que apoya en la operación de los procesos de gestión comercial de las empresas de saneamiento del norte del Perú. El modelo propuesto se enfoca en brindar al usuario, a partir de la investigación de las distintas metodologías y estándares de gestión de riesgos de TI, un modelo simple y flexible que promueva su aplicación, con la intención de que se desarrolle una cultura organizacional de acción preventiva en la gestión de riesgos de tecnologías de información en las empresas de saneamiento.

Escala: (1) En total desacuerdo (2) En desacuerdo (3)Ni de acuerdo ni de desacuerdo (4) De acuerdo (5)Totalmente de acuerdo

Procedimiento: Marcar con X la opción elegida

| Proceso | Objetivo | Descripción del Indicador | Escala | | | | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | |
| **Fase 1: Definir el Contexto** | | | | | | | | |
| Definir Contexto Interno | Definir parámetros básicos internos para alcanzar los objetivos estratégicos de la organización | Nivel de elementos por factor (cultural, normativo,partes internas involucradas, recursos, estructura, metas y objetivos , valores) | | | | | X | |
| Definir Contexto Externo | Definir parámetros básicos externos para alcanzar los objetivos estratégicos de la organización | Nivel de elementos por factor (Ambiente de negocio, normativo y politico, finaciero) | | | | | X | |
| **Fase 2: Crear Perfil de Activos** | | | | | | | | |
| Identificar los conocimientos de dirección | Captar el conocimiento desde el punto de vista de la alta dirección para identificar los activos importantes, las áreas que están involucradas, | Cantidad de activos identificados. | | | | | X | |
| | | Nivel de identificación de requimientos de seguridad. | | | | | X | |
| Identificar los conocimientos en el área de gestión operativa | Captar el conocimiento desde el punto de vista de los gerentes y jefaturas, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales | Cantidad de activos identificados.<br>Nivel de identificación de requimientos de seguridad. | | | | | X | |
| Identificar los conocimientos de personal | Captar el conocimiento desde el punto de vista del personal operativo, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales | Cantidad de activos identificados.<br>Nivel de identificación de requimientos de seguridad. | | | | | X | |

| Proceso | Objetivo | Descripción del Indicador | Escala | | | | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | |
| Identificar activos a gestionar | Determinar los activos de mayor importancia, de acuerdo al puntaje obtenido desde los distintos puntos organizacionales: dirección, gestión operativa y personal | Porcentaje de activos que superan la media de la valorización. | | | | | X | |
| **Fase 3: Identificar los Riesgos** | | | | | | | | |
| Clasificación de Activos | Clasificar los activos críticos, identificados en la fase 2, en las categorías establecidas por el método MAGERIT | Cantidad de activos clasificados por categoría. | | | | | X | |
| Dependencia de Activos | Identificarlos activos y establecer la relación de dependencia | Numero de relaciones de dependencia identificada entre activos | | | | | X | |
| Valoración de Activos | Valorar el grado de importancia de cada activos teniendo en cuenta criterios de disponibilidad, integridad y confidencialidad. | Número de criteros determinados. | | | | | X | |
| | | Número de escalas suficientes para calcular criticidad de activos. | | | | | X | |
| | | Nivel de simplicidad para determinar la valorización de los activos identificados | | | | | X | |
| Identificación de las Amenazas y Vulnerabilidades | Identificar las vulnerabilidades y amenazas de los activos valorizados en la actividad anterior. | Nivel de simplicidad para determinar las vulnerabilidades y amenazas para cada activo | | | | | X | |
| **Fase 4: Analisis de Riesgos** | | | | | | | | |
| Determinación de Probabilidad | Determinar el valor de la probabilidad de que una amenaza se materialice a causa de una determinada vulnerabilidad. | Número de valores suficientes para determinar la probalidad o frecuenta de ocurrencia | | | | | X | |
| Analisis de Impacto | Medir los efectos adversos resultantes de la materialización de una amenaza para cada uno de los riesgos identificados para cada activo crítico. | Número de valores suficientes para determinar el nivel de impacto | | | | X | | |
| Determinación del riesgo | Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza | Nivel de simplicidad para determinar el valor total del riesgo | | | | | X | |
| **Fase 5: Evaluación del riesgo** | | | | | | | | |
| Elaboración de la matriz de clasificación del riesgo | Clasificar a los riesgos según su prioridad de tratamiento | Número de categorías de riesgo suficiente para la valorización | | | | X | | |
| Valorización del riesgo | Evaluar mediante la medición de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible, y la probabilidad que dicha pérdida o daño llegue a ocurrir. | Nivel de simplicidad para determinar la valorización del riesgo frente a los niveles de apetito y tolerancia determinados | | | | X | | |

| Proceso | Objetivo | Descripción del Indicador | Escala 1 | 2 | 3 | 4 | 5 | Observaciones |
|---|---|---|---|---|---|---|---|---|
| **Fase 6: Políticas y administración de Riesgos** | | | | | | | | |
| Plan de seguridad | Identificación de proyectos de seguridad | Nivel de suficiencia con respecto a las denominaciones de evitar, mitigar, transferir y aceptar para las estrategias de tratamiento | | | | X | | |
| | Plan de Ejecución | Número de criterios suficientes para la formulación de proyectos | | | | X | | |
| **Fase 7: Monitorización y Revisión** | | | | | | | | |
| Monitoreo | Ejecutar para obtener datos para el procesamiento de los indicadores | Nivel de simplicidad para identificar acciones para el procesamiento de indicadores | | | | X | | |
| | Identificar las características del objetivo del proyecto para determinar el indicador de medición | Nivel de simplicidad para identificar las variables a controlar | | | | X | | |
| | Identificar la medida de lo logrado en la aplicación del procesamiento | Nivel de simplicidad para identificar los indicadores | | | | X | | |
| Revisión | Identificar medidas correctivas para mejorar los resultados obtenidos | Nivel de simplicidad para identificar las medidas correctivas | | | | X | | |

| | |
|---|---|
| DISCONFORMIDAD | |
| OBSERVADO | |
| ACEPTACIÓN | X |

MGRT. GREGORIO LEÓN TENORIO
Profesional Experto

| Proceso | Objetivo | Descripción del Indicador | Escala | | | | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | |
| **Fase 1: Definir el Contexto** | | | | | | | | |
| Definir Contexto Interno | Definir parámetros básicos internos para alcanzar los objetivos estratégicos de la organización | Nivel de elementos por factor (cultural, normativo,partes internas involucradas, recursos, estructura, metas y objetivos , valores) | | | X | | | redefinir stakeholders internos |
| Definir Contexto Externo | Definir parámetros básicos externos para alcanzar los objetivos estratégicos de la organización | Nivel de elementos por factor (Ambiente de negocio, normativo y político, financiero) | | | | X | | |
| **Fase 2: Crear Perfil de Activos** | | | | | | | | |
| Identificar los conocimientos de dirección | Captar el conocimiento desde el punto de vista de la alta dirección para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las | Cantidad de activos identificados. | | | | X | | |
| | | Nivel de identificación de requerimientos de seguridad. | | | | ✓ | | |
| Identificar los conocimientos en el área de gestión operativa | Captar el conocimiento desde el punto de vista de los gerentes y jefaturas, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales | Cantidad de activos identificados. Nivel de identificación de requerimientos de seguridad. | | | | X | | |
| Identificar los conocimientos de personal | Captar el conocimiento desde el punto de vista del personal operativo, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales | Cantidad de activos identificados. Nivel de identificación de requerimientos de seguridad. | | | | X | | |
| Identificar activos a gestionar | Determinar los activos de mayor importancia, de acuerdo al puntaje obtenido desde los distintos puntos organizacionales: dirección, gestión operativa y personal | Porcentaje de activos que superan la media de la valorización. | | | | X | | |
| **Fase 3: Identificar los Riesgos** | | | | | | | | |
| Clasificación de Activos | Clasificar los activos críticos, identificados en la fase 2, en las categorías establecidas por el método MAGERIT | Cantidad de activos clasificados por categoría | | | | X | | |
| Dependencia de Activos | Identificarlos activos y establecer la relación de dependencia | Numero de relaciones de dependencia identificada entre activos | | | X | | | Revisar activos y dep. |
| Valoración de Activos | Valorar el grado de importancia de cada activos teniendo en cuenta criterios de disponibilidad, | Número de criterios determinados. | | | | Y | | |
| | | Número de escalas suficientes para calcular criticidad de | | | | X | | |

| Proceso | Objetivo | Descripción del indicador | Escala | | | | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | |
| **Fase 1: Definir el Contexto** | | | | | | | | |
| | integridad y confidencialidad. | Nivel de simplicidad para determinar la valorización de los activos identificados | | | | X | | |
| Identificación de las Amenazas y Vulnerabilidades | Identificar las vulnerabilidades y amenazas de los activos valorizados en la actividad anterior. | | | | X | | | definición de vulnerabili. |
| **Fase 4: Analisis de Riesgos** | | | | | | | | |
| Determinación de Probabilidad | Determinar el valor de la probabilidad de que una amenaza se materialice a causa de una determinada vulnerabilidad. | Número de valores suficientes para determinar la probabilidad o frecuenta de ocurrencia | | | X | | | Unificar criterio. |
| Análisis de Impacto | Medir los efectos adversos resultantes de la materialización de una amenaza para cada uno de los riesgos identificados para cada activo | Número de valores suficientes para determinar el nivel de impacto | | | | X | | |
| Determinación del riesgo | Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza | Nivel de simplicidad para determinar el valor total del riesgo | | | X | | | |
| **Fase 5: Evaluación del riesgo** | | | | | | | | |
| Elaboración de la matriz de clasificación del riesgo | Clasificar a los riesgos según su prioridad de tratamiento | Número de categorías de riesgo suficiente para la valorización | | | | | X | |
| Valorización del riesgo | Evaluar mediante la medición de los dos parámetros que la determinan, la magnitud de la pérdida o daño posible, y la probabilidad que dicha pérdida o daño llegue a ocurrir. | Nivel de simplicidad para determinar la valorización del riesgo frente a los niveles de apetito y tolerancia determinados | | | X | | | Completar |
| **Fase 6: Políticas y administración de Riesgos** | | | | | | | | |
| Plan de seguridad | Identificación de proyectos de seguridad | Nivel de suficiencia con respecto a las denominaciones de evitar, mitigar, transferir y aceptar para las estrategias de | | | | X | | |
| | Plan de Ejecución | Número de criterios suficientes para la formulación de | | | | X | | |
| **Fase 7: Monitorización y Revisión** | | | | | | | | |
| Monitoreo | Ejecutar para obtener datos para el procesamiento de los indicadores | Nivel de simplicidad para identificar acciones para el procesamiento de indicadores | | X | | | | Completar |
| | Identificar las características del objetivo del proyecto para determinar el indicador de medición | Nivel de simplicidad para identificar las variables a controlar | | X | | | | Completar |

| Proceso | Objetivo | Descripción del Indicador | Escala | | | | | Observaciones |
|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | |
| **Fase 1: Definir el Contexto** | | | | | | | | |
| | Identificar la medida de lo logrado en la aplicación del procesamiento | Nivel de simplicidad para identificar los indicadores | | X | | | | Completar |
| Revisión | Identificar medidas correctivas para mejorar los resultados obtenidos | Nivel de simplicidad para identificar las medidas correctivas | | X | | | | Completar |

Justo José L. R.
DNI 08421705

## Anexo N° 04: Aplicación del Método Alfa de Cronbach para estimar la fiabilidad del modelo propuesto

Tabla 78 Análisis comparativo del juicio de expertos

| Proceso | Objetivo | EXPERTO 1 | EXPERTO 2 | EXPERTO 3 |
|---|---|---|---|---|
| **Fase 1: Definir el Contexto** | | | | |
| Definir Contexto Interno | Definir parámetros básicos internos para alcanzar los objetivos estratégicos de la organización | 3.5 | 5 | 4 |
| Definir Contexto Externo | Definir parámetros básicos externos para alcanzar los objetivos estratégicos de la organización | | | |
| **Fase 2: Crear Perfil de Activos** | | | | |
| Identificar los conocimientos de dirección | Captar el conocimiento desde el punto de vista de la alta dirección para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales | 4 | 5 | 5 |
| Identificar los conocimientos en el área de gestión operativa | Captar el conocimiento desde el punto de vista de los gerentes y jefaturas, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de | | | |

| Proceso | Objetivo | EXPERTO 1 | EXPERTO 2 | EXPERTO 3 |
|---|---|---|---|---|
| | protección y vulnerabilidades organizacionales | | | |
| Identificar los conocimientos de personal | Captar el conocimiento desde el punto de vista del personal operativo, para identificar los activos importantes, las áreas que están involucradas, los requerimientos de seguridad y las estrategias actuales de protección y vulnerabilidades organizacionales | | | |
| Identificar activos a gestionar | Determinar los activos de mayor importancia, de acuerdo al puntaje obtenido desde los distintos puntos organizacionales: dirección, gestión operativa y personal | | | |
| **Fase 3: Identificar los Riesgos** | | | | |
| Clasificación de Activos | Clasificar los activos críticos, identificados en la fase 2, en las categorías establecidas por el método MAGERIT | 3.5 | 5 | 4.75 |
| Dependencia de Activos | Identificarlos activos y establecer la relación de dependencia | | | |
| Valoración de Activos | Valorar el grado de importancia de cada activo teniendo en cuenta criterios de | | | |

| Proceso | Objetivo | EXPERTO 1 | EXPERTO 2 | EXPERTO 3 |
|---|---|---|---|---|
| | disponibilidad, integridad y confidencialidad. | | | |
| Identificación de las Amenazas y Vulnerabilidades | Identificar las vulnerabilidades y amenazas de los activos valorizados en la actividad anterior. | | | |
| **Fase 4: Análisis de Riesgos** | | | | |
| Determinación de Probabilidad | Determinar el valor de la probabilidad de que una amenaza se materialice a causa de una determinada vulnerabilidad. | 3.33 | 4.67 | 5.00 |
| Análisis de Impacto | Medir los efectos adversos resultantes de la materialización de una amenaza para cada uno de los riesgos identificados para cada activo crítico. | | | |
| Determinación del riesgo | Determinar el nivel del riesgo a través de los valores sensibilidad de activos, análisis de vulnerabilidad y análisis de amenaza | | | |
| **Fase 5: Evaluación del riesgo** | | | | |
| Elaboración de la matriz de clasificación del riesgo | Clasificar a los riesgos según su prioridad de tratamiento | 4 | 4 | 5 |
| Valorización del riesgo | Evaluar mediante la medición de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible, y la | | | |

| Proceso | Objetivo | EXPERTO 1 | EXPERTO 2 | EXPERTO 3 |
|---|---|---|---|---|
| | probabilidad que dicha pérdida o daño llegue a ocurrir. | | | |
| **Fase 6: Políticas y administración de Riesgos** | | | | |
| Plan de seguridad | Identificación de proyectos de seguridad | 4 | 4 | 4 |
| | Plan de Ejecución | | | |
| **Fase 7: Monitorización y Revisión** | | | | |
| Monitoreo | Ejecutar para obtener datos para el procesamiento de los indicadores | 2 | 4 | 4 |
| | Identificar las características del objetivo del proyecto para determinar el indicador de medición | | | |
| | Identificar la medida de lo logrado en la aplicación del procesamiento | | | |
| Revisión | Identificar medidas correctivas para mejorar los resultados obtenidos | | | |

Tabla 79 - Proceso del cálculo de Alfa de Cronbach

| | FASE 1 | FASE 2 | FASE 3 | FASE 4 | FASE 5 | FASE 6 | FASE 7 | TOTAL |
|---|---|---|---|---|---|---|---|---|
| EXPERTO 1 | 3.5 | 4 | 3.5 | 3.33 | 4 | 4 | 2 | 24.33 |
| EXPERTO 3 | 4 | 5 | 4.75 | 5.00 | 5 | 4 | 4 | 31.75 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| EXPERTO 2 | 5 | 5 | 5 | 4.67 | 4 | 4 | 4 | 31.67 |
| ESTADISTICOS | | | | | | | | |
| VARIANZA | 0.58 | 0.33 | 0.65 | 0.78 | 0.33 | 0.00 | 1.33 | |

| | |
|---|---|
| K | 7 |
| ∑Vi | 4.01 |
| Vt | 18.13 |

| | |
|---|---|
| SECCION 1 | 1.17 |
| SECCION 2 | 0.78 |
| ABSOLUTO SECCION2 | 0.78 |

| | |
|---|---|
| α | 0.90884718 |

## Anexo N° 05: Aplicación del método de coeficiente de Kendall para estimar la fiabilidad del modelo propuesto

Tabla 80 Procedimiento de cálculo del coeficiente de Kendall

| | FASE 1 | FASE 2 | FASE 3 | FASE 4 | FASE 5 | FASE 6 | FASE 7 | |
|---|---|---|---|---|---|---|---|---|
| EXPERTO 1 | 3.5 | 4 | 3.5 | 3.33 | 4 | 4 | 2 | |
| EXPERTO 3 | 4 | 5 | 5 | 4.67 | 4 | 4 | 4 | |
| EXPERTO 2 | 5 | 5 | 5 | 4.67 | 4 | 4 | 4 | |
| | 12.5 | 14 | 13.5 | 12.66 | 12 | 12 | 10 | 12.380952 |

$$W = \frac{12S}{m^2(n^3 - n) - mT}$$

| | |
|---|---|
| n | 7 |
| m | 3 |

| | |
|---|---|
| Numerador | 119.14 |
| Denominador | 3024 |

| | |
|---|---|
| W | 0.04 |
| chi-cuadrado | 0.71 |
| gl | 6 |
| Valor de p | 0.994 |

# Anexo N° 06: Documentos que sustentan la aplicación del modelo en el caso de estudio

USAT
Universidad Católica
Santo Toribio de Mogrovejo

EPSEL
R.E. 505677
15 NOV 2017
HORA 10:24
TRAMITE DOCUMENTARIO

Chiclayo, 14 de noviembre de 2017

**CARTA N.° 049 – 2017 – USAT – EP**

**Señor**

**Ing. Mirko Jurado Dueñas**
**Gerente General EPSEL**

**Presente.-**

***Asunto: Apoyo en ejecución de trabajo de investigación***

Es grato dirigirme a usted para expresarle un cordial saludo a nombre de la Escuela de Postgrado de la Universidad Católica Santo Toribio de Mogrovejo y, a la vez, presentarle a los Sres. Edgard Esaú Peña Nuñez, Lissette Angélica Moscoso Anaya y María del Carmen Soto Castrillón (Trabajadora del área de informática de EPSEL), estudiantes del Programa de Maestría en Ingeniería de Sistemas con mención en Dirección Estratégica de TI, solicitando su apoyo que les permita la ejecución del Proyecto de Investigación "Implementación de un modelo de gestión de riesgos de TI que contribuya a la continuidad de la operación de los procesos de gestión comercial de empresas del sector de saneamiento del norte del Perú" cuyos resultados serán compartidos con su representada.

Agradeciendo las facilidades otorgadas a los estudiantes para el logro de sus metas de investigación, hago propicia la ocasión para reiterarle los sentimientos de consideración y estima.

Atentamente,

ESCUELA DE POSTGRADO

Dra. Mirtha Flor Cervera Vallejos
Directora Escuela de Postgrado - USAT

Av. San Josemaría Escrivá de Balaguer N°855. Chiclayo-Perú ▪ Central Telefónica: (074) 606200 - 606217 ▪ Oficina de Información: (074) 606203
PreUSAT: (074) 606217 ▪ Profesionalización: (074) 606204 ▪ Postgrado: (074) 606205 ▪ www.usat.edu.pe ▪ www.facebook.com/usat.peru

## Carta de Revisión y Conformidad

Yo, **José Mario Segura Bernal**, identificado con DNI **42300949**, en calidad de **Jefe de Informática de la Empresa Prestadora de Servicios de Saneamiento de Lambayeque S.A.**, he verificado la información relativa a EPSEL S.A incluida en el **trabajo de investigación "MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE A LA OPERACIÓN DE LOS PROCESOS DE GESTIÓN COMERCIAL DE LAS EMPRESAS DEL SECTOR DE SANEAMIENTO DEL NORTE DEL PERÚ"**, y con la firma de la presente doy conformidad a los valores incluidos en los formatos que se detallan a continuación, debido a que estos se ajustan a la realidad de nuestra empresa. Asimismo dejo constancia de conocer que los datos incluidos en el trabajo en mención solo serán usados con fines educativos.

| Código | Nombre |
|---|---|
| DECI | Formato de definición del contexto interno |
| DECE | Formato de definición del contexto externo |
| IDAC | Formato de identificación de activos críticos |
| IAAC | Formato de Identificación de amenazas por activo crítico |
| DRSA | Formato de Determinación de requisitos de seguridad por activo crítico |
| IEOA | Formato de Identificación de estrategias de protección y vulnerabilidades organizacionales por activo crítico |
| POAC | Formato de Ponderación de activos críticos |
| LCAC | Lita de clasificación de activos críticos |
| DDAC | Diagrama de dependencia de activos críticos |
| VDAC | Formato de Valoración de activos críticos |
| DVDA | Formato de Determinación del valor de la amenaza |
| IDVU | Formato de Identificación de las vulnerabilidades |
| DVVU | Formato de Determinación del valor de la vulnerabilidad |
| MDNR | Matriz del nivel de riesgo |
| MDCR | Matriz de clasificación del riesgo |
| PRDR | Formato de Ponderación del riesgo |
| MDVR | Matriz de valoración del riesgo |
| INDP | Inventario de Proyectos |
| FIPR | Ficha de proyecto |
| Como ejemplo debido a que a la fecha no se ha puesto ningún proyecto en operación, ya que no se han incluido en el plan operativo anual 2018 | |
| CDPE | Cronograma del plan de ejecución |
| LIEP | Lista de control de indicadores a evaluar por proyecto |
| FDMO | Ficha de monitoreo |

Ing. José Mario Segura Bernal
Jefe de Informática
EPSEL S.A.
42300949

## Carta de Revisión y Conformidad

Yo, CPC. WALTHER MARTHIN FAYA INFANTES, identificado con DNI 40780960 , en calidad de GERENTE COMERCIAL **de la Empresa Prestadora de Servicios de Saneamiento de Lambayeque S.A.**, he verificado la información relativa a EPSEL S.A incluida en el **trabajo de investigación "MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE A LA OPERACIÓN DE LOS PROCESOS DE GESTIÓN COMERCIAL DE LAS EMPRESAS DEL SECTOR DE SANEAMIENTO DEL NORTE DEL PERÚ"**, y con la firma de la presente doy conformidad a los valores incluidos en los formatos que se detallan a continuación, debido a que estos se ajustan a la realidad de nuestra empresa. Asimismo dejo constancia de conocer que los datos incluidos en el trabajo en mención solo serán usados con fines educativos.

| Código | Nombre |
|---|---|
| DECI | Formato de definición del contexto interno |
| DECE | Formato de definición del contexto externo |
| IDAC | Formato de identificación de activos críticos |
| IAAC | Formato de Identificación de amenazas por activo crítico |
| DRSA | Formato de Determinación de requisitos de seguridad por activo crítico |
| IEOA | Formato de Identificación de estrategias de protección y vulnerabilidades organizacionales por activo crítico |
| POAC | Formato de Ponderación de activos críticos |
| LCAC | Lista de clasificación de activos críticos |
| DDAC | Diagrama de dependencia de activos críticos |
| VDAC | Formato de Valoración de activos críticos |
| DVDA | Formato de Determinación del valor de la amenaza |
| IDVU | Formato de Identificación de las vulnerabilidades |
| DVVU | Formato de Determinación del valor de la vulnerabilidad |
| MDNR | Matriz del nivel de riesgo |
| MDCR | Matriz de clasificación del riesgo |
| PRDR | Formato de Ponderación del riesgo |
| MDVR | Matriz de valoración del riesgo |
| INDP | Inventario de Proyectos |
| FIPR | Ficha de proyecto |
| Como ejemplo debido a que a la fecha no se ha puesto ningún proyecto en operación, ya que no se han incluido en el plan operativo anual 2018 | |
| CDPE | Cronograma del plan de ejecución |
| LIEP | Lista de control de indicadores a evaluar por proyecto |
| FDMO | Ficha de monitoreo |

EPSEL S.A. GERENCIA COMERCIAL

08/12/17.

CPC. WALTHER MARTHIN FAYA INFANTES
GERENTE COMERCIAL
EPSEL S.A.

Anexo N° 07: Propuestas de cotizaciones para proyectos de seguridad para el tratamiento de riesgos identificados.

TECSUP
Pasión por la Tecnología

## Mantenimiento y Configuración de Equipos de Cómputo

()

La Computadora se ha convertido en una potente herramienta de trabajo para todas las personas, no interesando el área donde trabajen. Actualmente todas las empresas poseen computadoras y esto origina una necesidad de darle mantenimiento y soporte a estos equipos.
Las personas encargadas de dar mantenimiento a las computadoras deben conocer las partes internas que la componen, el software necesario para que trabajen y los periféricos requeridos, y todo ello instalado y configurado de tal manera que aseguren un buen desempeño.
El Programa Integral ha sido diseñado con el propósito de capacitar personas que para desarrollar tareas de mantenimiento y configuración de computadoras y brindar soporte a los usuarios.

### Objetivos

1 Identificar las partes que componen una computadora y la integración entre ellas.
2 Ensamblar una computadora siguiendo un procedimiento estándar.
3 Instalar y configurar software utilitario para la configuración y optimización de la computadora.
4 Brindar un mantenimiento preventivo a los equipos de cómputo.
5 Seleccionar las partes y equipos más adecuados en la integración de computadoras.
6 Especificar mejoras a equipos computacionales (upgrade).
7 Realizar mantenimiento de computadoras portátiles y servidores.

### Modulos

| | NOMBRE | DURACIÓN |
|---|---|---|
| 1 | Arquitectura y Ensamblaje de Computadoras | 36 horas |
| 2 | Software de Mantenimiento y Comunicación en red | 36 horas |
| 3 | Mantenimiento de Equipos de Computo | 42 horas |

### Requsitos

1 Conocimiento básico de Windows.

### Fecha de Inicio

07 Abril 2018

### Cierre de Inscripciones

04 Abril 2018

### Horarios

Sabado 08:00-14:00 horas

### Inversión

Cinco cuotas de S/. 560 ó S/. 2660 al contado

## CAPÍTULO I
## GENERALIDADES

### 1.1. ENTIDAD CONVOCANTE

| | | |
|---|---|---|
| Nombre | : | INSTITUTO NACIONAL MATERNO PERINATAL |
| RUC N° | : | 20144329148 |
| Domicilio legal | : | JR. MIROQUESADA N° 941 - LIMA |
| Teléfono: | : | 3280699 |
| Correo electrónico: | : | lpinedo@inmp.gob.pe |

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del SERVICIO ESPECIALIZADO EN SEGURIDAD INFORMATICA.

### 1.3. VALOR REFERENCIAL

El valor referencial asciende a S/.126,496.00 (Ciento veintiséis mil cuatrocientos noventa y seis con 00/100 Soles), incluido los impuestos de Ley y cualquier otro concepto que incida en el costo total del servicio. El valor referencial ha sido calculado al mes de Agosto 2017.

| ITEM N° | CANTIDAD | UNIDAD MEDIDA | DESCRIPCION | MONTO TOTAL S/. |
|---|---|---|---|---|
| 01 | 1 | SERVICIO | SERVICIO ESPECIALIZADO EN SEGURIDAD INFORMATICA | 126,496.00 |

### 1.4. EXPEDIENTE DE CONTRATACION

El expediente de contratación fue aprobado mediante MEMORANDO N° 0594-2017-OEA-INMP el 21 de Setiembre del 2017

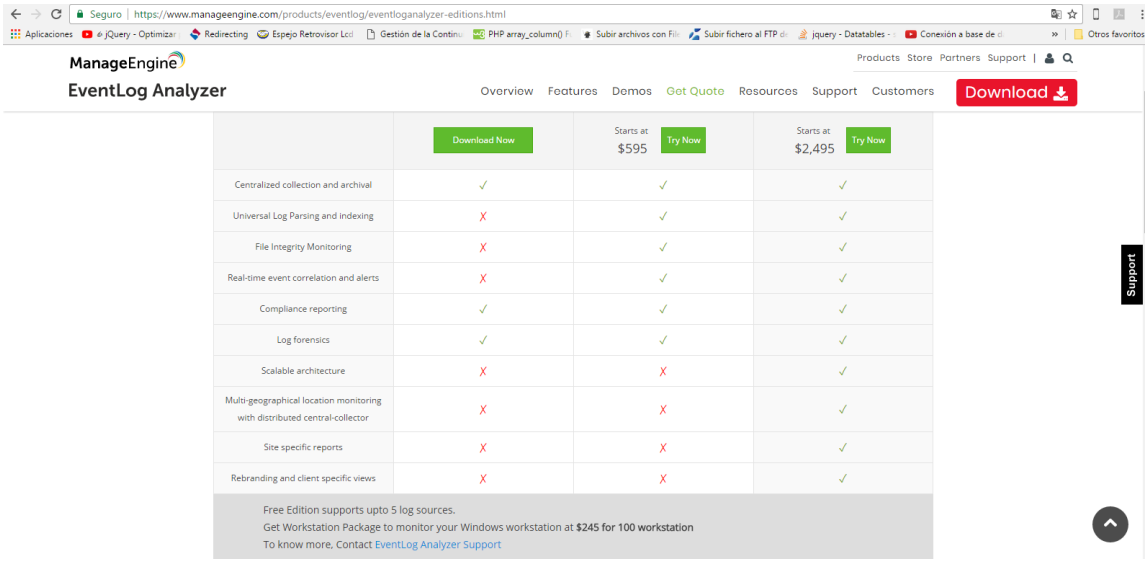
### 1.5. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados.

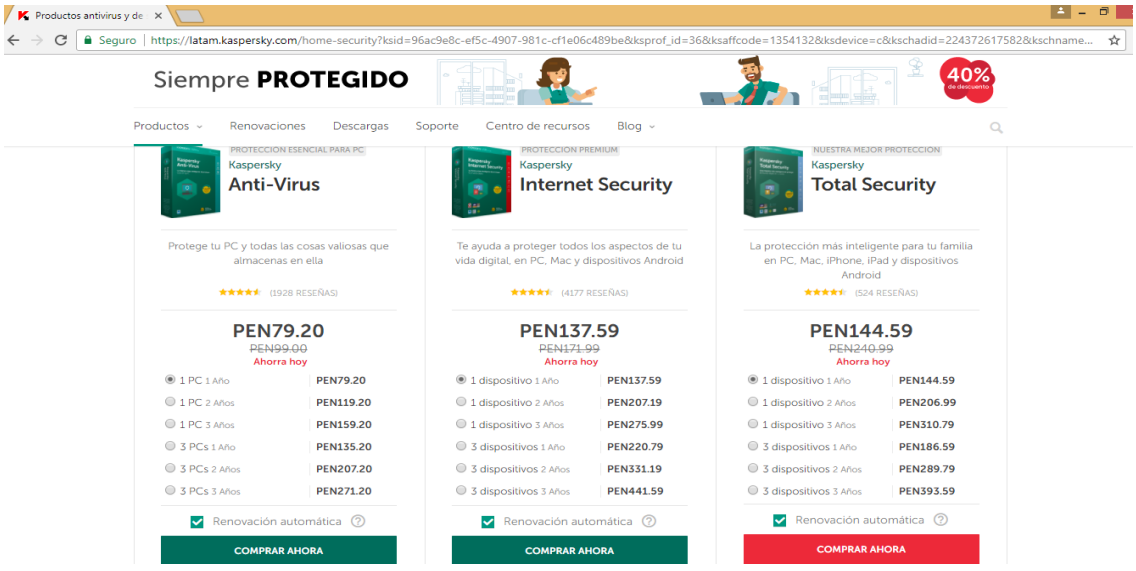
| FUENTE DE FINANCIAMIENTO | AÑO 2017 | AÑO 2018 | MONTO TOTAL |
|---|---|---|---|
| RECURSOS DIRECTAMENTE RECAUDADOS | S/.31,624.00 | S/.94,872.00 | ***S/. 126,496.00*** |

**Importante**

*La fuente de financiamiento debe corresponder a aquella prevista en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el procedimiento de selección.*


Seguro | https://www.manageengine.com/products/eventlog/eventloganalyzer-editions.html
ManageEngine
EventLog Analyzer
Products Store Partners Support
Overview Features Demos Get Quote Resources Support Customers
Download
Download Now
Starts at $595
Try Now
Starts at $2,495
Try Now
Centralized collection and archival
Universal Log Parsing and indexing
File Integrity Monitoring
Real-time event correlation and alerts
Compliance reporting
Log forensics
Scalable architecture
Multi-geographical location monitoring with distributed central-collector
Site specific reports
Rebranding and client specific views
Free Edition supports upto 5 log sources.
Get Workstation Package to monitor your Windows workstation at $245 for 100 workstation
To know more, Contact EventLog Analyzer Support
Support


Seguro | https://azure.microsoft.com/es-es/pricing/details/backup/
Microsoft Azure
VENTAS 0800-56012
MI CUENTA
PORTAL
Por qué Azure Soluciones Productos Documentación Precios Formación Marketplace Partners Soporte técnico Más
CUENTA GRATUITA
Región:
Centro de EE. UU.
Divisa:
Dólar estadounidense (USD)
TAMAÑO DE CADA INSTANCIA
PRECIOS POR MES DE AZURE BACKUP
Instancia < o = 50 GB
$5 + almacenamiento consumido
La instancia es > 50 pero < o = 500 GB
$10 + almacenamiento consumido
Instancia > 500 GB
$10 por cada incremento de 500 GB + almacenamiento consumido
Ejemplo: Si tiene 1,2 TB de datos en una instancia, entonces el costo sería $30 más el almacenamiento consumido. Se le cobraría $10 por dos incrementos de 500 GB y $10 por los 200 GB de datos restantes.


Productos antivirus y de
Seguro | https://latam.kaspersky.com/home-security?ksid=96ac9e8c-ef5c-4907-981c-cf1e06c489be&ksprof_id=36&ksaffcode=1354132&ksdevice=c&kschadid=224372617582&kschname...
Siempre PROTEGIDO
40% de descuento
Productos Renovaciones Descargas Soporte Centro de recursos Blog
PROTECCION ESENCIAL PARA PC
Kaspersky Anti-Virus
Protege tu PC y todas las cosas valiosas que almacenas en ella
(1928 RESEÑAS)
PEN79.20
PEN99.00
Ahorra hoy
1 PC 1 Año PEN79.20
1 PC 2 Años PEN119.20
1 PC 3 Años PEN159.20
3 PCs 1 Año PEN135.20
3 PCs 2 Años PEN207.20
3 PCs 3 Años PEN271.20
Renovación automática
COMPRAR AHORA
PROTECCION PREMIUM
Kaspersky Internet Security
Te ayuda a proteger todos los aspectos de tu vida digital, en PC, Mac y dispositivos Android
(4177 RESEÑAS)
PEN137.59
PEN171.99
Ahorra hoy
1 dispositivo 1 Año PEN137.59
1 dispositivo 2 Años PEN207.19
1 dispositivo 3 Años PEN275.99
3 dispositivos 1 Año PEN220.79
3 dispositivos 2 Años PEN331.19
3 dispositivos 3 Años PEN441.59
Renovación automática
COMPRAR AHORA
NUESTRA MEJOR PROTECCION
Kaspersky Total Security
La protección más inteligente para tu familia en PC, Mac, iPhone, iPad y dispositivos Android
(524 RESEÑAS)
PEN144.59
PEN240.99
Ahorra hoy
1 dispositivo 1 Año PEN144.59
1 dispositivo 2 Años PEN206.99
1 dispositivo 3 Años PEN310.79
3 dispositivos 1 Año PEN186.59
3 dispositivos 2 Años PEN289.79
3 dispositivos 3 Años PEN393.59
Renovación automática
COMPRAR AHORA

CENTRO DE FORMACIÓN EN TURISMO
Unidad de Sistemas e Informática

FICHA TÉCNICA PARA LA PROGRAMACIÓN DE ACTIVIDADES Y PROYECTOS INFORMÁTICOS 2013

**I. Recursos Humanos a Contratar**

Presupuesto total asignado: **S/. 68 909**

| Recursos Humanos | CANTIDAD | PRESUPUESTO ASIGNADO | FUENTE DE FINANCIAMIENTO |
|---|---|---|---|
| Programador Web | 03 | 68 909 | Recursos ordinarios |

**II. Adquisiciones de Hardware**

Presupuesto total asignado: **S/. 187 000**

| Tipo de Equipos | CANTIDAD | PRESUPUESTO ASIGNADO | FUENTE DE FINANCIAMIENTO |
|---|---|---|---|
| Computadoras | 40 | 140 000 | Recursos ordinarios |
| impresoras | 09 | 17 000 | Recursos ordinarios |
| Proyectores | 10 | 30 000 | Recursos ordinarios |

**III. Adquisiciones de Licencias**

Presupuesto total asignado: **S/. 40 000**

| TIPO DE EQUIPO | CANTIDAD | PRESUPUESTO ASIGNADO | FUENTE DE FINANCIAMIENTO |
|---|---|---|---|
| Software Telefonia IP | 01 | 10 000 | Recursos ordinarios |
| Software de Oficina | 120 | 15 000 | Recursos ordinarios |
| Diseño | 3 | 7 000 | Recursos ordinarios |
| Antivirus | 180 | 8 000 | Recursos ordinarios |

**V. Consolidado a Ejecutarse en el año 2013**

Presupuesto total asignado: **S/. 295 909**


Windows Server 2012 Editions
FOUNDATION
ESSENTIALS
STANDARD
DATACENTER
Descripción:
Este Diplomado brinda los conocimientos necesarios para la implementación, administración y mantenimiento de infraestructura de redes y servicios con Microsoft Windows Server 2012.
MÓDULO I: INSTALACIÓN Y CONFIGURACIÓN DE WINDOWS SERVER 2012.
SESIÓN 1 Implementación y administración de windows Server 2012 sesión
SESIÓN 2 Implementación de la virtualización de servidores con Hyper-V
SESIÓN 3 Implementación de Active Directory Domain Services
SESIÓN 4 Administración de los Objetos de Dominio de Active Directory
SESIÓN 5 Implementación de IPv4 Sesión
SESIÓN 6 Implementación de DHCP
SESIÓN 7 Implementación de DNS, WINS
SESIÓN 8 Implementación de directivas de grupo GPOs.
MÓDULO II. ADMINISTRACIÓN DE WINDOWS SERVER 2012.
SESIÓN 1 Gestión de Virtualización – Hyper-V
SESIÓN 2 Gestión de GPOs.
SESIÓN 3 Implementación Acceso Remoto
SESIÓN 4 Implementación IIS, WEB, FTP
PEARSON
ORACLE UNIVERSITY
CERTIPORT
Microsoft
Inicio:
Hora:
Matrícula:
Mensualidad:
www.ceti.org.pe
Informes e Inscripciones :
Elías Aguirre 762 2do Piso
Costado del Banco Financiero
informes@ceti.org.pe
Teléfono: 074 225361
Cel: 978094320 RPM: *664294
CETI
CENTRO DE ENTRENAMIENTO EN TECNOLOGÍAS DE INFORMACIÓN

HC TECNOLOGÍAS Y SERVICIOS S.A.C

Chiclayo, 15 de enero del 2018

# COTIZACIÓN

## PC Completa Intel Core I7 Séptima Generación 8GB RAM 500 GB SSD


### Características Técnicas

- Motherboard GIGABYTE GA-B250M-DS3H, LGA1151
- Procesador Intel Core i7-7700, 3.60 GHz, 8 MB Caché L3, LGA1151
- Memoria Corsair CMV8GX4M1A2133C15, 8 GB, DDR4, 2133 MHz
- Unidad de estado sólido Western Digital Blue, 500GB, SATA 6Gb/s, M.2
- DVD SuperMulti LG GH24NSD1, 24X, interno, SATA.
- Case Thermaltake Versa H23, Mid Tower, 500W, Negro.
- Kit Teclado y Mouse Genius SlimStar C130, USB, Negro
- Monitor Advance A-195MS, 19.5" LED, 1600 x 900.
- UPS Elise AUR-650, interactivo, 650VA, 360W, 162~290 VAC, 6 tomas NEMA

**Inversión: 3580.00 Soles**

**Condiciones de Venta:** Precio Inc. IGV. Pago al contado

**Garantía:** 01 Año (por defectos de fabricación).