Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO(A) DE SISTEMAS

TITULO

LA SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA GESTIÓN DE LOS RIESGOS DE NEGOCIO EN LAS EMPRESAS AGROINDUSTRIALES AZUCARERAS

PRESENTADO POR:

TAPIA CARRILLO JHOELY MAILIS

VIDAL CASTILLO JOSUE LUIS

ASESOR:

Dr. Ing. Ernesto Karlo Celi Arévalo

LAMBAYEQUE – PERÚ

Mayo - 2020

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO(A) DE SISTEMAS

TITULO

LA SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA GESTIÓN DE LOS RIESGOS DE NEGOCIO EN LAS EMPRESAS AGROINDUSTRIALES AZUCARERAS

APROBADA POR LOS MIEMBROS DEL JURADO:

Dr. Ing. EDWARD RONALD HARO MALDONADO

PRESIDENTE DEL JURADO

Mag. Ing. PILAR DEL ROSARIO RÍOS CAMPOS
SECRETARIA

Mag. Ing. OSCAR EFRAÍN CAPUÑAY UCEDA
VOCAL

Dr. Ing. ERNESTO KARLO CELI ARÉVALO
ASESOR

TAPIA CARRILLO JHOELY MAILIS
VIDAL CASTILLO JOSUE LUIS
AUTORES

Lambayeque – Perú

Mayo - 2020

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
DECANATO

ACTA DE SUSTENTACIÓN VIRTUAL N°020-2021-F ICSA-D

Siendo las 8:00am horas del día 15 de diciembre del 2021, se reunieron vía plataforma virtual: meet.google.com/zad-qmfz-kjm, los miembros de jurado de la Tesis titulada: **"LA SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA GESTIÓN DE LOS RIESGOS DE NEGOCIO EN LAS EMPRESAS AGROINDUSTRIALES AZUCARERAS"**, con código de proyecto: **IS-2020-005**, designados por Decreto Directoral N° 039-2020-UNPRG-FICSA-UI, con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

DR. ING. EDWARD RONALD HARO MALDONADO	PRESIDENTE
MG. ING. PILAR DEL ROSARIO RÍOS CAMPOS	SECRETARIO
MG. ING. OSCAR EFRAÍN CAPUÑAY UCEDA	VOCAL

Asesorado por el **DR. ING. ERNESTO CELI AREVALO**

El acto de sustentación fue autorizado por **Decreto Directoral Virtual N° 068-2021-UIFICSA-UNPRG**, la Tesis fue presentada y sustentada por los Bachilleres: **TAPIA CARRILLO JHOELY MAILIS y VIDAL CASTILLO JOSUE LUIS**, tuvo una duración de 90 minutos. Después de la sustentación y absueltas las preguntas y observaciones de los miembros del jurado, se procedió a la calificación respectiva:

TAPIA CARRILLO JHOELY MAILIS	**16**	DIECISEIS	BUENO
VIDAL CASTILLO JOSUE LUIS	**16**	DIECISEIS	BUENO

Por lo que quedan **APTOS** para obtener el Título Profesional de **INGENIERO (A) DE SISTEMAS** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil, de Sistemas y de Arquitectura, de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 11:35 horas, se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

DR. ING. EDWARD RONALD HARO MALDONADO
PRESIDENTE

M.SC. PILAR DEL ROSARIO RÍOS CAMPOS
SECRETARIO

MG. ING. OSCAR EFRAÍN CAPUÑAY UCEDA
VOCAL

DR. ING. ERNESTO KARLO CELI AREVALO
ASESOR

DECANATO

DR. ING. SERGIO BRAVO IDROGO
DECANO

REGISTRO VIRTUAL SUSTENTACIONES INGENIERIA CIVIL
IC_L001_F020

DEDICATORIA

El presente trabajo investigativo lo dedicamos principalmente a nuestros padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos. Ha sido el orgullo y el privilegio de ser sus hijos, son los mejores padres.

Dedicado a Dios, quien como guía estuvo presente en nuestro caminar de vida, bendiciéndonos y dándonos fuerzas para continuar con nuestras metas trazadas sin desfallecer.

AGRADECIMIENTOS

De manera especial a nuestro tutor de tesis, por habernos guiado, no solo en la elaboración de este trabajo de titulación, sino a lo largo de nuestra carrera universitaria y habernos brindado el apoyo para desarrollarnos profesionalmente y seguir cultivando nuestros valores.

A los Catedráticos que nos han visto crecer como persona, y gracias a sus conocimientos hoy podemos sentirnos dichosos y contentos por la culminación de nuestra meta en común.

RESUMEN

Uno de los aspectos más críticos de la administración de una organización es la gestión de sus activos que generan valor a los procesos del negocio. La información, puede considerarse como uno de los activos más críticos que hay que proteger, porque su disponibilidad e integridad, no solo se utiliza como insumo para la toma de decisiones, si no también asegura la continuidad de los procesos.

La gestión de la información no solo implica incorporar tecnologías que le den soporte a su captura, almacenamiento, procesamiento y comunicación; si no también se debe implementar procesos y sistemas que gestionen este recurso para lograr su seguridad. La implementación de sistemas de gestión de la seguridad de la información (SGSI) permite que ésta logre niveles aceptables de confidencialidad, integridad y disponibilidad.

Un proceso de implementación de un SGSI, metodológicamente hablando, implica una serie de actividades y tareas, que van desde la planificación de su alcance hasta la planificación de los planes de mejora continua. Sin embargo, el aspecto más crítico que debe considerarse en la implementación de un SGSI es la gestión de los riesgos. La gestión de los riesgos es una estrategia preventiva que permite identificar y evaluar los diferentes escenarios de riesgo a los que está expuesta la información, en sus diferentes formas de expresión, y las tecnologías que le dan soporte a lo largo de su ciclo de vida. Con esta información, se podrá implantar los controles y salvaguardas necesarias para la mitigación de aquellos niveles de exposición al riesgo que la organización considere no aceptables.

El propósito de este trabajo de investigación se centró en el desarrollo de un modelo de Sistema de gestión de riesgos de seguridad de la información, usando como referencia la norma ISO/IEC 27005, en los procesos productivos de las empresas azucareras de la Región Lambayeque.

Palabras clave: sistema de gestión de riesgos de seguridad de la información, análisis y evaluación de riesgos, activo de TI.

ABTRACT

One of the most critical aspects of the administration of an organization is the management of its assets that generate value to the business processes. Information can be considered as one of the most critical assets that must be protected, because its availability and integrity is not only used as an input for decision-making, but also ensures the continuity of processes.

Information management not only implies incorporating technologies that support its capture, storage, processing and communication; if not, processes and systems that manage this resource must also be implemented to achieve its security. The implementation of information security management systems (ISMS) allows it to achieve acceptable levels of confidentiality, integrity and availability.

An ISMS implementation process, methodologically speaking, involves a series of activities and tasks, ranging from planning its scope to planning continuous improvement plans. However, the most critical aspect to consider in implementing an ISMS is risk management. Risk management is a preventive strategy that allows identifying and evaluating the different risk scenarios to which information is exposed, in its different forms of expression, and the technologies that support it throughout its life cycle. With this information, the necessary controls and safeguards can be implemented to mitigate those levels of risk exposure that the organization considers unacceptable.

The purpose of this research work was focused on the development of an information security risk management system model, using the ISO / IEC 27005 standard as a reference, in the production processes of sugar companies in the Lambayeque Region.

Keywords: information security risk management system, risk analysis and assessment, IT asset.

INDICE

INDICE DE TABLAS

INDICE DE GRÁFICOS

INDICE DE FIGURAS

INTRODUCCION

En la presente tesis, se diseña y desarrolla el modelo para implementar un sistema de gestión de riesgos de seguridad de información para los procesos productivos de las empresas azucareras de la región Lambayeque.

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad.

La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos.

La problemática principal actual de las organizaciones que están en franco desarrollo y que soportan sus procesos de negocio sobre TI, es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a los procesos a pérdidas no solo de información, sino también económica.

Es por ello, que las empresas azucareras de la Región Lambayeque se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

El presente trabajo consta de cuatro capítulos. Ellos son:

En el capítulo I se presenta la descripción de la realidad problemática, el planteamiento del problema científico, la descripción del proyecto y los objetivos.

El capítulo II muestra el marco teórico, en el que están planteadas las bases teóricas relacionadas con un sistema de gestión de riesgos de seguridad de la información

(SGSI), definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación.

En el capítulo III se especifican los métodos utilizados para el desarrollo del trabajo de investigación. También se define la metodología empleada, la cual es la resultante de una revisión de distintas metodologías de gestión de riesgos y de los estándares asociados a la seguridad de la información.

El capítulo IV está destinado a la presentación de los resultados del trabajo de investigación. Así mismo, se aborda la discusión de los resultados a manera de explicación de los mismos, teniendo en cuenta los objetivos de la investigación.

A partir de los resultados obtenidos se han planteado las conclusiones y recomendaciones pertinentes, y finalmente se consigna la bibliografía utilizada y los anexos respectivos.

CAPÍTULO I. EL PROBLEMA

1.1. Descripción de la problemática

Las organizaciones, no importa cuál sea su actividad y tamaño, afrontan una serie de riesgos que pueden afectar a la consecución de sus objetivos. Todas las actividades de una organización están sometidas de forma permanente a una serie de amenazas, lo cual las hace vulnerables, comprometiendo su estabilidad. Accidentes operacionales, enfermedades, incendios, pérdidas de beneficios, catástrofes naturales, etc., son una muestra de este panorama, sin olvidar las amenazas propias del negocio (Torres-Enciso & San Jose-Martí, 2011).

En los modelos promovidos por las normativas internacionales de análisis de riesgos en los sistemas de información y en las tecnologías de la información, los activos están interrelacionados entre sí, de modo que un ataque sobre uno de ellos se puede transmitir a lo largo de toda la red, llegando a alcanzar a los activos más valiosos para la organización. Es necesario entonces, asignar el valor de todos los activos, así como las relaciones de dependencia directas e indirectas entre estos, o la probabilidad de materialización de una amenaza y la degradación que ésta puede provocar sobre los activos. Sin embargo, los expertos encargados de asignar tales valores, a menudo aportan información vaga e incierta (Vicente, Mateos, & Jiménez, 2013).

Las organizaciones cada vez son más conscientes de los impactos que les pueden generar los riesgos referentes a las tecnologías de información (TI). Es frecuente que procesos de diversos sectores económicos reporten pérdidas debido a fallas y/o ataques sobre sus servicios de TI, los cuales afectan seriamente su reputación y su solidez económica y operacional. Existen dos pilares fundamentales para realizar el análisis de riesgos: los estándares y normas, de un lado, y las metodologías, de otro; estos pilares por sí solos no aseguran el éxito si no se articulan adecuadamente (Gomez, Pérez, Donoso, & Herrera, 2010).

Existen numerosas metodologías para la gestión de riesgos de TI, tales como Magerit, Risk IT, Octave, Neozelandesa, Australiana, etc. Así mismo, existen estándares como la familia ISO 27000, ISO 20000, etc., y modelos de gobierno y

gestión de TI como COBIT 5.0, que pueden utilizarse para gestión de riesgos de TI. Sin embargo, sus procedimientos o no son adecuadas para el tamaño de infraestructura de TI o no son adecuados para el grado de madurez de TI o su implementación requiere fuertes inversiones o simplemente no cuentan con herramientas flexibles y adecuables al tipo de organizaciones de nuestro medio.

Hablar sobre gestión de riesgos ya no se limita al enfoque financiero tradicional o de cobertura. La gerencia de riesgos en realidad posee una visión holística de la compañía que contempla aspectos muy variados como la pérdida de control, la seguridad, así como diversas estrategias para prevenir, reducir o transferir el riesgo (Torres-Enciso & San Jose-Martí, 2011).

La actividad agroindustrial es uno de los pilares que sostiene la economía del Perú, por lo que es importante la organización empresarial para alcanzar los logros de la agroindustria como organización para conseguir cumplir su misión y alcanzar su propia visión con objetivos estratégicos, para ello se definen también las acciones, para conseguirlo es importante la planificación empresarial.

La investigación está relacionada con la gestión empresarial en las empresas azucareras de la Región Lambayeque dedicadas al cultivo y atención de la caña de azúcar, dado fundamentalmente por el abastecimiento de recursos para consumo y atracción económica que tiene este producto en el mercado nacional e internacional.

En Perú actualmente la caña de azúcar representa 78% de tierras sembradas en proyecto Olmos, hasta abril, se han sembrado 8,106 hectáreas de caña de azúcar, lo que representa el 78.2% del total sembrado. Es cultivada en la costa, sierra y selva y se siembra y cosecha durante todo el año. El mayor uso industrial de la caña de azúcar es para la producción de azúcar. De las hectáreas sembradas con caña corresponde el 65 % a los 10 ingenios azucareros y el 35 % restante a los sembradores particulares.

Como caso de estudio, se tomó a la Empresa Agroindustrial Pomalca S.A.A, la cual se encuentra ubicada en el Km. 7 de la carretera Chiclayo- Chongoyape en

el distrito de Pomalca provincia de Chiclayo de la Región Lambayeque; dedicándose en su principal renglón a producir azúcar a partir del cultivo de caña de azúcar, así como sus derivados (melaza, chancaca y bagazo), cumpliendo con las normas ambientales y de responsabilidad social; encontrándose a la vanguardia en la aplicación de tecnologías de última generación para los rendimientos de sus cultivos .

En la actualidad la Empresa Agroindustrial Pomalca S.A.A Cotiza en la Bolsa de Valores de Lima con Respaldo del Grupo Inversionista. Desde el ingreso de este grupo empresarial, enormes han sido los esfuerzos para mejorar los campos, la fábrica, la producción de caña y la obtención de azúcar, no obstante, aún se presentan dificultades con el proceso productivo; así como los procesos de apoyo como la logística, el transporte, la gestión de personal, etc. Estos procesos son gestionados y controlados con aplicaciones informáticas que han sido desarrolladas en diferentes plataformas de desarrollo y son independientes entre ellas, en el almacenamiento y procesamiento de la información. Esta situación, no permite integrar la información y muchas veces no existe congruencia en los resultados de los reportes que se emiten.

Además, se ha evidenciado permanentemente problemas con la operación de los equipos informáticos y la infraestructura de red de computadoras con la que cuenta la empresa. Los problemas de caídas o paralizaciones, muchas veces en tiempos prolongados, de los sistemas generalmente se debe a la mala gestión de los servidores o de la red. En los meses de julio y agosto del 2019, se ha registrado dos caídas del sistema informático con una duración que ha superado los cinco (5) días, no permitiendo la operación normal del proceso productivo.

La pérdida de información o su sustracción no controlada, es otro de los problemas que se tienen en la empresa Pomalca. No existen controles para realizar el seguimiento de los documentos generados o para el uso de la información. Los controles de acceso a los sistemas son todavía deficientes, lo que conlleva a que la información puede estar siendo modificada o sustraída sin las autorizaciones respectivas.

Esta situación nos motiva a realizar la presente investigación, con la finalidad de analizar la gestión de riesgos como estrategia para la reducción de incidentes de TI, con un enfoque propositivo. Por ello, nos centraremos en el desarrollo de un framework o marco de trabajo para la gestión de los riesgos operativos de las tecnologías de la información en sus diferentes etapas, como son la identificación, evaluación y su tratamiento

1.2. Objetivos de la investigación

1.2.1. Objetivo general

Desarrollar un modelo de gestión de los riesgos de TI que mejore la gestión de la seguridad de la información en las empresas agroindustriales azucareras.

1.2.2. Objetivos específicos

Los objetivos específicos del estudio son:

1. Definir los criterios generales para incluir la seguridad de la información como parte de la gestión de los procesos de las empresas agroindustriales azucareras.
2. Identificar el alcance de un sistema de gestión de seguridad de la información en base al análisis de procesos de las empresas agroindustriales azucareras.
3. Determinar los dominios de la seguridad de la información que se deben considerar en la gestión de riesgos de TI.
4. Desarrollar un procedimiento para analizar y evaluar los escenarios de riesgo a los que están expuestos los activos de TI.
5. Proponer un conjunto de controles y mecanismos de seguridad para la mitigación de los riesgos de TI no tolerables.

CAPÍTULO II. MARCO TEÓRICO

De la revisión literaria realizada se elaboró los siguientes fundamentos teóricos, que sirvieron de base para el desarrollo de la propuesta del Modelo de Gestión de Riesgos de seguridad de la información.

2.1. El valor de la información en las empresas

Los activos son todos aquellos recursos que tienen algún tipo de valía o que a través de ellos se genera alguna utilidad para la organización, cuando son utilizadas en las diferentes operaciones de negocio. El logro de los objetivos misionales y estratégicos de una organización y su continuo funcionamiento depende mucho de los activos con los que cuenta (Espinoza, Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo, 2017).

La norma ISO/IEC 27002, establece que la información es un recurso que tiene que proteger, porque genera valor directamente a la organización.

En todas las áreas de una empresa y en todos sus niveles jerárquicos, la información, ya sea interna o externa, es uno de los recursos clave, que debe ser debidamente adquirida, procesada, almacenada, explotada y comunicada, con la finalidad de dar un adecuado soporte a los procesos de planeamiento, organización, dirección y control, sobre todo en la toma de decisiones (Carrasco, Impacto del riesgo en el gobierno de las tecnologias de Información y comunicación en la gestión empresarial industrial del sigo XXI, 2016).

La clasificación de los activos tiene muchos enfoques, siendo uno de los más importantes, el que propone la ISO/IEC 27005 (2009), la que clasifica a los activos en dos clases:

- Los activos primarios: Se refiere a los procesos principales de una organización y a la información que resulta de ello. Por ello, es que se debe considerar como parte de las políticas de seguridad, la protección de:
    - Los procesos y principales actividades de negocio
    - Información que resulta de los procesos del negocio

- Los activos de apoyo: Dan soporte a los procesos principales en las diferentes etapas del ciclo de tratamiento de los datos, como: adquisición, almacenamiento, procesamiento, comunicación. Como estos activos trabajan en entornos donde se generan escenarios de riesgo que los pueden afectar y, por ende, también a los activos primarios, es que deben ser considerados en las políticas y procedimientos de seguridad para mitigar los riesgos generados por las amenazas. Estos activos pueden ser clasificados como:
    - Equipamiento terminal (Hardware)
    - Software o aplicaciones informáticas
    - Red de computadoras
    - Personal técnico de TI
    - Entorno de trabajo para las actividades de TI
    - Estructura organizativa del área que gestiona las TI

2.2. El propietario de la información como un activo en la empresa

Lo que establece la NTP-ISO/IEC 27005 (2009), sobre la propiedad de los activos es que le corresponde a la persona responsable del uso, mantenimiento, seguridad y producción de un activo de acuerdo a la función que cumpla, sin la necesidad de ser propietario del mismo. El propietario de la información, por el conocimiento que tiene debe ser el encargado de determinar el valor que tiene el activo. Cada activo debe tener asignado un propietario con la finalidad de definir sus responsabilidades sobre éste y las rendiciones de cuenta necesarias.

2.3. Seguridad de información

La seguridad de la información son el conjunto de medidas de carácter preventivo y reactivo, que realiza una persona, una organización o un sistema, según corresponda, con la finalidad de resguardar y proteger la información que está bajo su gestión, tratando de mantener los niveles de confidencialidad, disponibilidad e integridad aceptables (Aguirre & Palacios, 2014).

La correcta gestión de la información depende de la tecnología que se utilice como soporte, y el aspecto que tiene mayor importancia es la confidencialidad. La información puede ser utilizada de mala manera o malintencionadamente,

como ser divulgada a quien no corresponda, mal utilizada en actos ilícitos, robada, modificada intencionalmente, borrada o eliminada, etc.

La información tiene la característica de lograr un cierto nivel de poder de decisión en quien la gestiona; y según el significado estratégico de la información, ésta debe estar relacionada a ciertos niveles posibles de acceso, clasificándola, como:

a. Crítica: Cuando la información es indispensable para el funcionamiento u operación de la organización.
b. Valiosa: Cuando la información tiene un valor altamente importante para la organización.
c. Sensible: Cuando la información solo debe ser accedida por personas autorizadas

(Talavera Álvarez, 2015)

2.3.1. Sistema de gestión de seguridad de la información

Conocido como SGSI, es el conjunto de estrategias, procesos, estructuras organizativas, procedimientos, funciones, responsabilidades y recursos que se asignan para gestionar la seguridad de los diferentes activos de información, asegurando la continuidad de las operaciones de la organización (ISO 17799:2005; Alexander, 2007).

El proceso de implementación de un SGSI, en base a las recomendaciones de la norma ISO/IEC 27001, pasa por cuatro etapas, conocidas como el Ciclo de Deming, como se muestra a continuación en la gráfica.

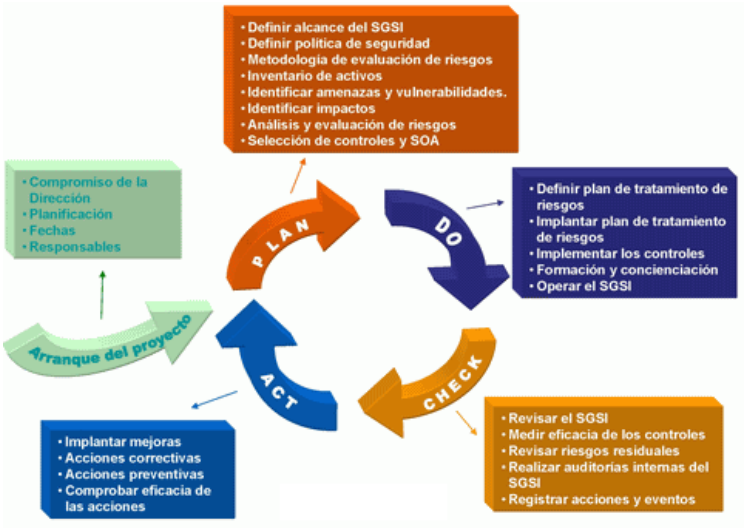

Gráfico N° 1. Etapas del Ciclo de Deming para la implementación de un SGSI

Fuente: http://www.iso27000.es/

2.3.2. Los criterios de seguridad de la Información

Los escenarios de riesgo a los que están expuestos los activos de información puede afectar alguna característica de la información, como: su disponibilidad, confidencialidad o su integridad; lo que puede conllevar a consecuencias significativamente graves para una organización, que en muchos casos puede llegar hasta situaciones irreparables o irrecuperables (Montesino, Baluja, & Porven, 2013).

Estos criterios son la base de la implementación de sistemas de seguridad con el propósito de proteger la información. A continuación, se detalla el fundamento de cada uno de estos criterios:

a. Confidencialidad

El propósito de esta característica de la información, es el aseguramiento de que solo el personal con privilegios definidos para acceder a cierta información específica, lo puedan hacer. No toda la información que se gestiona en una organización debe y puede ser conocida por cualquier persona, si no por un grupo de personas bien identificadas, incluso hasta solo por una persona. Entonces, la organización debe implementar mecanismos para asegurar que el personal que no está autorizado para

acceder a cierta información, no lo puedan hacer. También se debe considerar que esta característica, muchas veces está relacionada a tiempos determinados, que también se debe definir, para que la confidencialidad de la información prevalezca y se mantenga, en su almacenamiento, durante su procesamiento y cuando se transmite por algún medio hacia el usuario o destino final (Condori, 2016).

b. Integridad

Esta característica de la información se refiere a que la información no pueda ser cambiada, alterada o modificada en alguna parte de su estructura o contenido por personas que no tengan el perfil y privilegio autorizado para realizarlo. La integridad está relacionada a garantizar que la información sea exacta y confiable (Condori, 2016).

c. Disponibilidad

Esta característica está relacionada con el aseguramiento de que la información requerida por cualquier usuario esté disponible, siempre y cuando tengan el perfil y el privilegio asignado para ello. La disponibilidad también incluye la protección y resguardo de los activos que contienen, procesan o transmiten la información, para evitar que una amenaza afecte su disponibilidad. Los mecanismos de aseguramiento de la disponibilidad deben contemplar capacidades de recuperar la información para garantizar la continuidad de las operaciones en la organización (Condori, 2016).

2.3.3. Política de seguridad de la información

La política de seguridad de la información es la definición de lineamientos y procedimientos con la finalidad de proteger y salvaguardar la información y los activos que le dan soporte o que los contienen (Hernández, 2016).

La definición de políticas de seguridad de la información tiene como propósito establecer formas de dirección y organización para proteger la información y los activos que los contienen; en base a las normas internas y externas, los procesos del negocio y las capacidades instaladas. Para ello, lo primero que debe realizar la gerencia es el manifiesto de su compromiso y apoyo a la implementación de la seguridad de la información, aprobando, informando y

manteniendo una política de aplicación obligatoria en todas las áreas de la empresa (ISO/IEC 27002, 2013).

Las políticas de seguridad de información es la base de un sistema de seguridad de la información, porque a partir de ellas, se generan los demás documentos de gestión y control, como las normativas y directivas, los procedimientos y guías de trabajo, los formatos de registro de las actividades.

Las políticas cumplen dos roles, según Peltier, Peltier y Blackley (2005):

- Rol Interno: cuando se identifica y define las funciones y responsabilidades de cada uno de los miembros responsables de su cumplimiento y aplicación en la organización; así como, las formas de cómo será evaluado su cumplimiento.
- Rol Externo: cuando se informa a los entes externos de la organización, como clientes, proveedores o cualquier persona externa, la forma cómo ellos pueden acceder y usar la información que se pone a su disposición.

Lo explicado por Hernández Pinto (2016), nos indica que para que una política de seguridad esté bien construida a nivel corporativo, debe estar alineada a la estrategia diseñada para la protección y mantenimiento de los sistemas o aplicaciones informáticas; así como de los recursos asociados, de tal manera que garantice su operación.

Las políticas de abarcan muchos aspectos, por eso es necesario clasificarlas en dominios, como: la seguridad física, la seguridad lógica, la seguridad en los entornos de red de computadoras, la seguridad relacionada con las personas (recursos humanos), la seguridad en las operaciones y en las comunicaciones, etc.

2.3.4. Elementos de un SGSI

La ISO/IEC 27001 establece que un SGSI está conformado por una serie de documentos que describen, explican y guían la construcción de un SGSI de la siguiente manera:

a. **Alcance del SGSI:** documento que describe e identifica las dependencias que serán consideradas en el SGSI, así como sus

delimitaciones y relaciones con otras dependencias, que podrían o no estar consideradas también dentro del alcance del SGSI.

b. **Políticas y objetivos de seguridad:** es un documento que tiene como propósito general establecer el compromiso con de la Dirección la gestión de la seguridad de la información, estableciendo los lineamientos para su organización y dirección. Empieza considerando a la información como un activo importante y crítico que debe protegerse.

c. **Procedimientos y mecanismos de control:** son los documentos que describen los procedimientos y sus normativas internas, relacionados con las funciones de seguridad, indicando los roles y dependencias que participan, el flujo de trabajo, formatos utilizados, excepciones, etc.

d. **Evaluación de riesgos:** Este documento describe la metodología que debe aplicar la empresa en todo su ámbito para colaborar en el análisis de los escenarios de riesgos operativos de TI, evaluando y estimando los valores de cada uno de los componentes que han sido considerados como: los activos de TI, escenarios de riesgo compuesto por las amenazas y vulnerabilidades, los impactos que tendrían los escenarios de riesgo y la probabilidad de ocurrencia de los mismos; así como la estimación de los niveles de exposición al riesgo. Sirve como guía para identificar los escenarios de riesgo y sus niveles de exposición actuales para discriminar cuáles son los que están en rangos de aceptabilidad de los que no lo están.

e. **Planificación del tratamiento de los riesgos:** este documento contiene la planificación de la implementación de controles, salvaguardas y mecanismos de seguridad, de cualquier tipo, en la empresa con el propósito de mitigar los escenarios de riesgos que están fuera de los rangos de tolerancia establecidos por la misma empresa. También define las estrategias de su implementación y el seguimiento que se hace a estos elementos para evaluar su efectividad. Se complementa con una serie de informes de los procedimientos documentados para evaluar de la eficacia de cada uno de los controles implantados.

f. **Registros de control:** son los documentos que dejan evidencias del cumplimiento de las actividades de control.

g. **Declaración de aplicabilidad:** (más conocido como SOA -Statement of Applicability). Es un documento que contiene definidos los objetivos de los controles en la organización relacionados con la seguridad de la información; así como los procedimientos de aplicación de los controles, con la finalidad de evaluar las brechas de seguridad en cada dominio o ámbito de seguridad de la información. La ISO/IEC 27002 define una lista de controles y objetivos de control que sirven de guía para definir cuáles son incluidos o excluidos en esta evaluación.

2.3.5. Proceso de implementación de un SGSI según ISO/IEC 27003

Los siguientes pasos son expuestos por Robles & Rodríguez de Roa (2006), tomando como referencia la ISO/IEC 27003:

PASO 1: Inicio del proyecto

Lo que se busca en esta etapa es asegurar la efectividad y el éxito del proyecto de implementación del SGSI. Por ello, incluye el compromiso de la dirección y la conformación de los equipos de trabajo.

Se debe declarar que la Dirección tiene el compromiso de apoyar el logro de los objetivos de la seguridad de la información, en todos los niveles de trabajo: operativo (tecnología, personal, procedimientos, etc.), técnico (capacitación, capacidades instaladas, etc.), económico y presupuestario. Generalmente, este compromiso se expresa en un plan de trabajo.

La norma establece que el equipo de trabajo es dirigido por un comité de dirección del proyecto, liderado por un director ejecutivo (representante de la dirección), un director del proyecto y los responsables de las diferentes dependencias, áreas o unidades operativas y funcionales de la organización.

PASO 2: Determinar el alcance del SGSI

Esta etapa es importante para lograr los objetivos del proyecto. En esta fase se realizan las siguientes tareas:

- Identificar las dependencia, áreas o unidades operativas que serán consideradas dentro del SGSI; describiendo las funciones, sobre todo las críticas.
- Identificar las características de la empresa, como su tamaño, giro de negocio, estructura organizativa, ubicación, etc. También se identifican los activos o inventario de activos que serán considerados en el SGSI: datos críticos en cualquier formato, tecnología.
- Identificar y describir las relaciones que tiene la empresa con otras organizaciones, proveedores, alianzas estratégicas u otros sistemas externos.
- Analizar la aplicabilidad de los controles en la empresa, utilizando el SOA (Declaración de aplicabilidad).
- Describir el contexto de la seguridad que existe actualmente implementada en la empresa y la planificación que se haya realizado sobre implementaciones futuras.
- Recopilar documentación relacionada con la seguridad, como estándares, directivas, normativas, procedimientos existentes, manuales, etc. Para analizar su incorporación en el proyecto.
- Realizar un inventario de documentos por área, como:
    - política de seguridad específicas
    - Normas y procedimiento administrativos y/o técnicos.
    - Documentos sobre análisis y evaluación de riesgos en cada una de ellas y sus correspondientes planes de tratamiento de riesgos.
    - Registros y documentos sobre controles implementados, como: informes, auditoría, registros de incidencias, etc.

PASO 3: Evaluación de riesgos

En esta etapa se realiza la evaluación de los escenarios de riesgo en cada una de las áreas involucradas en el SGSI, llegando a estimar los niveles de riesgo. Cada área debe tener su propia matriz de riesgos por las particularidades que pueda tener en la gestión de riesgos, escenarios de riesgos identificados y la tecnología que utiliza. El análisis debe considerar mínimo los riesgos asociados a las características de seguridad exigidas por la normatividad: confidencialidad, integridad y disponibilidad de la información.

PASO 4: Tratamiento y administración del riesgo

Esta etapa contempla la selección de los mecanismos de seguridad, salvaguardas y controles para mitigar aquellos escenarios de riesgo que están fuera de los rangos de tolerancia. Así mismo, se define la estrategia de su administración y seguimiento. Normalmente, estas decisiones toman como base cierta información, como:

- La política de seguridad de la información que tiene la empresa inicialmente.
- La definición de los niveles de seguridad requerido y aceptados por la empresa.
- Los informes de la evaluación de riesgos donde muestran los niveles de exposición al riesgo encontrados.
- Los reglamentos y normativas relacionadas con la gestión de TI.
- Las regulaciones y normativas relacionadas al negocio y sus procesos.

En el tratamiento del riesgo se aplican estrategias, como: reducción del riesgo, aceptación del riesgo, evitar el riesgo o transferir el riesgo.

PASO 5: Formación y sensibilización

Luego de la implementación de los mecanismos de seguridad y los controles, la norma establece que el personal debe ser, primero informado de esta implementación y, segundo, determina que se deben realizar actividades de formación y educación de ser necesario para la correcta aplicación de los controles y actividades de sensibilización para su oportuno y efectivo cumplimiento.

PASO 6: Documentación e implantación del SGSI

Todos los resultados obtenidos en las fases anteriores deben ser documentados, por ser necesarios, previo a la implementación del SGSI. Esta documentación está definida en niveles por la norma, de la siguiente manera:

Tabla N° 1. Niveles de documentación en seguridad de la información

Nivel	Documento requerido	Contenido
Nivel 1	Manual de política de seguridad de la información	El manual contiene, la declaración de políticas de seguridad de la información, los resultados de la evaluación de riesgos, la declaración de aplicabilidad de los controles
Nivel 2	Procedimientos operativos de seguridad de la información	Este documento describe los procedimientos implementados, que expliquen las normativas que lo regulan, la identificación de los roles y funciones, flujo de trabajo, excepciones, etc.
Nivel 3	Formatos para la definición del flujo de trabajo, formularios, etc.	Contiene el detalle del flujo de trabajo y actividades de cada procedimiento de seguridad implementado
Nivel 4	Formatos de registro del cumplimiento de los controles	Son las evidencias que proporcionan las pruebas objetivas y tangibles de la conformidad con las exigencias de la norma.

Fuente: adaptado de (Robles & Rodriguez de Roa, La gestión de la seguridad en la empresa, 2016)

Esta fase se desarrolla en paralelo a las fases anteriores, es decir los documentos necesarios y requeridos por la norma se van creando conforme se va avanzando con el trabajo y actividades de cada fase.

PASO 7: Preparación y auditoría para la certificación del SGSI

Esta fase tiene el carácter voluntario de la empresa si desea obtener la certificación de su SGSI. Para ello debe preparar todos los requerimientos exigidos por la norma ISO/IEC 27001 para lograr este objetivo.

Normalmente se realizan auditorias previas para autoevaluar el estado actual del SGSI e identificar incumplimientos de los requisitos exigidos.

PASO 8: Mejora continua

Esta fase se contempla como una estrategia para evaluar permanentemente los resultados obtenidos por SGSI implementado y realizar las mejoras y correcciones necesarias. Se utiliza como referencia el Ciclo de Deming (Plan-Do-Check-Act).

2.3.6. ISO/IEC 27000

La norma ISO/IEC 27000 define los requisitos para la establecer sistemas de gestión de la seguridad de la información (SGSI), proporcionando un marco o guía de trabajo estandarizado. Comprende normas específicas para los siguientes aspectos:

a. Organización del SGSI.
b. Formas de valoración de los escenarios de riesgos.
c. Controles y sus guías de implementación.

La ISO/IEC 27000 está orientada a trabajar bajo el enfoque por procesos. Establece que toda la organización debe estar involucrada en su implementación, según la función que cumplan dentro de ella, para garantizar un trabajo coordinado y entendido, apoyados por la Dirección, quien lidera el proceso. Esto permitirá que se pueda identificar los riesgos relacionados con la ejecución de todas las actividades del proyecto, incluyendo las medidas para mitigarlos y las formas de evaluar la efectividad de las mismas (Reina & Morales, 2014).

Reina García y Morales Ramírez (2014), señalan que el conjunto de normas ISO/IEC 27000, si bien es cierto, tienen el carácter de aplicación voluntaria, su implementación traería varios beneficios a la organización como: facilitando las relaciones comerciales con otras organizaciones, aumentando su competitividad en el mercado, mejorando la calidad de los servicios y productos, ganando la confianza de los clientes y proveedores, etc.

En nuestra investigación las normas de la familia ISO 27000, que utilizaremos serán las siguientes:

a. ISO/IEC 27001

Es la principal norma de la familia ISO/IEC 27000. En esta norma se establecen los requisitos que tener en cuenta en el proceso de implantación de un SGSI. Las organizaciones toman esta norma como guía para verificar que se han cumplido con las exigencias de un SGSI. Su principal anexo es

el Anexo A, en donde se listan los objetivos de control y los controles que podrían ser considerados en el SGSI (Aguirre Mollehuanca, 2014).

Proporciona una guía modelo para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI, en cualquier tipo o tamaño de organización (ISO/IEC 27001, 2013).

La norma utiliza como referencia el modelo Deming: Plan-Hacer-Verificar-Actuar (PDCA: Plan-Do-Check-Act). La entrada del proceso son las necesidades y perspectivas que tienen los interesados y responsables de la seguridad de información en la organización y, como salida principal, el nivel de satisfacción de aquellas expectativas.

Gráfico N° 2. Procesos de implementación del SGSI en base al modelo PDCA

Fuente: (ISO/IEC 27001, 2013)

Estructura de la norma ISO/IEC 27001:2013

La estructura de la norma ISO/IEC 27001:2013 está constituida por una serie de cláusulas que describen los requisitos o exigencias para la implementación de un SGSI. La tabla siguiente se muestra el catálogo de cláusulas de la norma.

Tabla N° 2. Catálogo de consideraciones de ISO/IEC 27001:2013

0	Introducción a la norma
1	Alcance de la norma
2	Normativas relacionadas
3	Definición de terminología básica
4.1	Conocimiento y entendimiento de la organización y su entorno
4.2	Identificación de las necesidades y expectativas de los interesados o responsables de la seguridad de la información
4.3	Alcance del SGSI
4.4	Definición del SGSI
5.1	Caracterización de los liderazgos y los compromisos necesarios para la implementación del SGSI
5.2	Políticas generales
5.3	Roles, responsabilidades y funciones relacionados a la seguridad de la información
6.1.1	Acciones para la mitigación de los riesgos y oportunidades
6.1.2	Descripción de la evaluación de los riesgos relacionados con la seguridad de la información
6.1.3	Descripción del tratamiento de riesgos en rangos no aceptables
6.2	Objetivos de la seguridad de la información y el planeamiento para su logro
7.1	Recursos asignados
7.2	Competencias exigidas del equipo
7.3	Conocimientos básicos que debe tener el equipo
7.4	Mecanismos de comunicación entre los miembros del equipo
7.5	Documentación del proceso
8.1	Planeación de la operación del SGSI y su control
8.2	Formas de evaluación de riesgos
8.3	Formas de tratamiento de riesgos
9.1	Monitoreo, medición y evaluación de la efectividad de los controles
9.2	Auditoría interna del SGSI
9.3	Revisión de la gestión del SGSI
10.1	Registro de las no conformidades y las actividades de corrección necesarias
10.2	Plan de mejoramiento del SGSI

Fuente: (BSI Group México, 2016)"

b. ISO/IEC 27002 – Guía y buenas prácticas para la implementación de los controles de seguridad de la información

En la norma se define una serie de directrices para realizar la gestión de seguridad de la información, considerando guías para identificar, seleccionar, implementar, ejecutar y gestionar los controles para el tratamiento de los riesgos (ISO/IEC 27002, 2013).

Esta norma puede ser tomada como referencia para:

a. Seleccionar controles como parte del proceso de implementación del SGSI que cumpla con las exigencias establecidas en la ISO/IEC 27001.
b. Implementar controles conocidos y aceptados en la gestión de la seguridad de la información;
c. Desarrollar directrices de gestión de seguridad de la información adecuadas y contextualizadas a la organización.

Como parte de la norma, se describen un conjunto de controles cuyo propósito es la mitigación del impacto de ocurrencia o la probabilidad de ocurrencia de los riesgos a los que está expuesto una organización (ISO/IEC 27002, 2013). La norma cataloga 14 dominios de seguridad de la información, 35 objetivos de control y 114 controles.

Los dominios de seguridad de información que abarca la norma son:

1. Definición de políticas de seguridad de la información
2. Estructura organizativa de la seguridad de la información
3. Seguridad para la gestión de los recursos humanos: antes, durante y después de su ingreso a la organización
4. Gestión de activos de TI
5. Control de acceso lógico a los recursos de información
6. Cifrado de la información
7. Seguridad física y ambiental
8. Seguridad en las operaciones
9. Seguridad en las telecomunicaciones
10. Procesos de adquisición, desarrollo y mantenimiento de los sistemas de información
11. Relaciones con los proveedores
12. Gestión de incidentes relacionados con TI
13. Continuidad del negocio
14. Cumplimiento normativo

c. ISO/IEC 27003 – Guía orientadora para implementar un SGSI

ISO/IEC 27003 es un estándar que define y describe una guía para que las organizaciones la tomen como referencia en el proceso de implantación de

un SGSI. También puede ser utilizada para realizar consultorías (ISOTools Excellence, 2014).

La norma está focalizada a orientar bajo un enfoque metodológico, las acciones a seguir para lograr con éxito, la implementación del SGSI, cumpliendo los requisitos establecidos en la ISO/IEC 27001. (ISOTools Excellence, 2014).

La norma está estructurada de la siguiente manera:

1. Alcance de la norma
2. Normativas tomadas como referencia
3. Términos y definiciones básicas
4. Descripción de la estructura de la norma
5. Forma de aprobación del proyecto para iniciar el proceso de implementación del SGSI.
6. Proceso de definición del alcance del SGSI
7. Identificación y evaluación de requerimientos de seguridad de la información.
8. Proceso de evaluación de los riesgos y el planeamiento de su tratamiento.
9. Diseño del SGSI.

Anexo A: Check list para la verificación del cumplimiento de los pasos de la implementación de un SGSI.

Anexo B: Detalle de los roles y responsabilidades en la estructura organizativa de la seguridad de la información

Anexo C: Detalle de los procesos de auditorías internas del SGSI

Anexo D: Estructura de las políticas de seguridad

Anexo E: Seguimiento y monitoreo del SGSI

2.4. Gestión de riesgos

Alcántara (2015) define la gestión de riesgos como un método para identificar, analizar, estimar y tipificar los riesgos, así como para implementar los controles que permitan mitigar aquellos riesgos que están fuera de los rangos de tolerancia.

La gestión de riesgos contempla:

a. Análisis del riesgo: en esta etapa se identifican los activos que requiere protección, identificando sus vulnerabilidades y las amenazas que pueden afectar. El resultado de esta actividad es la determinación de los niveles de riesgo.
b. Clasificación de los riesgos: en esta etapa se clasifican los riesgos según su nivel de exposición, en aceptables o no aceptables, tomando como referencia los grados de tolerancia establecidos por la organización.

c. Mitigación de los riesgos: Se refiere a la actividad donde se definen e implementas las medidas de protección o salvaguardas para la mitigación de los riesgos fuera de los rangos de tolerancia. En esta etapa también, se aborda el proceso de sensibilización, entrenamiento y capacita los usuarios los mecanismos de seguridad implementados.
d. Control: Es la etapa donde se realiza el seguimiento, monitoreo y evaluación de las medidas de seguridad implementadas para determinar la efectividad y el cumplimiento de las medidas, y en base a ello, realizar las acciones correctivas necesarias para superar las debilidades y sancionar el incumplimiento.

Para realizar gestión de riesgos es esencial tener en cuenta la estructura organizacional, la cultura organizacional, los procesos organizacionales; así como la misión y los objetivos que se hayan planteado lograr. También es importante conocer bajo que marco de referencia se implementará los procesos de la gestión de riesgos (Huamán, 2014).

Huamán (2014) establece que la gestión de riesgos debe garantizar que el impacto sobre la organización, de la materialización de una amenaza, será manejable, dentro de los límites aceptables de costos ocasionados, permitiendo la continuidad del negocio.

Gráfico N° 3. Fases o etapas de un proceso de gestión de riesgos

Fuente: (Huamán, 2014)

2.4.1. Elementos de un modelo de gestión de riesgos de TI

a. Amenaza

Una amenaza entidad, física o lógica, que puede potencialmente originar incidentes no controlados o deseados, ocasionando algún tipo de daño o perjuicio material o no material a la organización, como: pérdida de información, caídas de los sistemas, fallas en los procesos o equipos, etc. (Espinoza, Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo, 2017).

Las amenazas pueden originarse por acción de una persona, ya sea por error o por una acción mal intencionada; por un mal diseño, como fallas en el procesamiento de un programa de computadora; por un hecho industrial o técnico, como un cortocircuito u obsolescencia; surgir de manera natural, como una tormenta, inundación, incendio. La amenaza puede originarse desde una fuente interna o externa a la organización (NTP-ISO/IEC 27005, 2009).

b. Vulnerabilidad

La vulnerabilidad es un estado de ausencia, falta de capacidad o debilidad que puede ser aprovechado por una amenaza para afectar a un activo de información. Por ello, las vulnerabilidades deben ser identificadas, valoradas y priorizadas para planificar las acciones que permitan superar dicha situación de debilidad (Reina & Morales, 2014).

c. Riesgo

Riesgo es la probabilidad de que una o más amenazas aprovechen las debilidades para explotarlas, ocasionando daños o pérdidas en los activos Medina (2007).

El riesgo es un indicador del nivel de exposición que tienen los activos para ser dañados o afectados, si no se implementan mecanismos de protección adecuados (Inteco, 2016).

Halvorson (2018) clasifica a los riesgos en tres tipos, de acuerda a la naturaleza de éstos, de la siguiente manera:

- Riesgos estratégicos, son los que están relacionados a afectar las utilidades o la reputación de la organización. Su origen está en las decisiones del nivel estratégico que pueden ocasionar que los objetivos del negocio no se logren.
- Riesgos tácticos, están relacionados con las debilidades que tienen los sistemas o mecanismos utilizados para vigilar, identificar y controlar de los riesgos. Indirectamente afectan la información.
- Riesgos operacionales, son los que están asociados a las debilidades en los activos, que pueden ocasionar efectos negativos sobre las operaciones o procesos de la organización.

La estimación del daño o pérdida, debido a los riesgos, está relacionado a las respuestas, que los responsables de los activos puedan dar a las siguientes preguntas:

- ¿Qué podría suceder? (Identificación de la amenaza)
- ¿Qué grave podría ser? (Identificación del impacto)

- ¿Con qué frecuencia podría suceder? (Identificación de la frecuencia)
- ¿Con qué certeza se ha respondido las preguntas anteriores? Identificación de la confianza).

(Ozier, Risk Analysis and Assessment" Information Security Management Handbook. 5th edition., 2014)

2.4.2. Proceso para la gestión de riesgos de TI

De acuerdo a Costas (2017), la gestión de los riesgos es una estrategia de carácter preventivo para controlar el desarrollo y funcionamiento de los procesos del negocio, con la finalidad de lograr con los objetivos estratégicos y tener un nivel de resiliencia suficiente para responder oportunamente a cualquier imprevisto.

El propósito de este proceso, es implementar controles que permitan reducir el impacto de las amenazas o reducir su probabilidad de ocurrencia (frecuencia) hasta lograr niveles de riesgo aceptables por la empresa.

Según la tipificación del riesgo, se puede optar por cualquiera de las siguientes estrategias de implementación y tratamiento de los riesgos:

a. Evitar el riesgo, identificando la fuente que genera el riesgo y eliminándolo.
b. Mitigar el riesgo, cuyo propósito sea o reducir la frecuencia de ocurrencia del riesgo o reducir el impacto en la organización.
c. Transferencia del riesgo a un tercero especializado, como: un seguro que cubra los riesgos identificados.
d. Aceptación del riesgo: cuando se reconoce la existencia de un riesgo, pero por economía o capacidades instaladas, solo se decide monitorearlo.

En la ISO/IEC 27005 se identifican etapas para gestionar los riesgos de seguridad de la información: (1) contextualización del entorno de generación del riesgo, (2) análisis y estimación del riesgo, (3) tratamiento del riesgo, (4) cálculo del riesgo residual, (5) comunicación del riesgo y (6) monitoreo y seguimiento del riesgo.

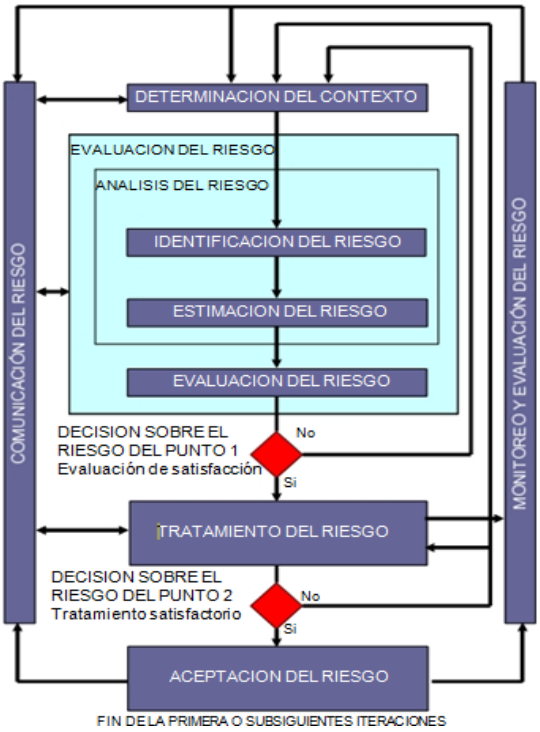

Gráfico N° 4. Proceso de gestión del riesgo de seguridad de la información

Fuente: (ISO/IEC 27005, 2011)

En la figura observamos que el proceso de gestión de la seguridad de la información es un proceso constante e interactivo. La idea es que, en cada interacción, los resultados que se obtienen de la evaluación del riesgo permitan tener información detallada de la efectividad de las medidas de seguridad implementadas y de sus controles, para lograr un balance entre el tiempo empleado para la gestión de los riesgos y el que se emplea para identificar y seleccionar los controles necesarios y adecuados.

Determinar el contexto del riesgo, evaluar los riesgos identificados, desarrollar el plan de tratamiento de los riesgos y aceptar el riesgo son actividades que se ejecutan como parte de la fase del “plan” del SGSI. Las acciones de mitigación de los riesgos y la implementación de los controles corresponden a la fase de

“hacer”. Los exámenes y evaluación de los mecanismos de seguridad y los controles corresponden a la fase de “verificar”. La fase “actuar”, contempla las acciones de mejora continua de los controles y mecanismos de seguridad, en base a los resultados de las actividades de la fase de “actuar”.

A continuación, se relaciona las fases del ciclo de Deming con el proceso de gestión de los riesgos.

Tabla N° 3. Relación del SGSI y con la gestión de riesgos

Proceso del SGSI	Proceso de Gestión del Riesgo de TI
Plan	Evaluar y definir el contexto de los riesgos. Analizar y evaluar los riesgos identificados Diseñar e desarrollar un plan de tratamiento del riesgo. Definir la estrategia de implementación de controles
Hacer	Implementar los mecanismos de seguridad y los controles que han sido definidos en la planificación del tratamiento del riesgo.
Verificar	Monitorear y hacer seguimiento de los niveles de riesgo.
Actuar	Mejorar los mecanismos de seguridad y los controles; así como, las debilidades del proceso de gestión de riesgos.

Fuente: (ISO/IEC 27005, 2011)

2.4.3. Metodología Magerit para análisis de riesgos

Magerit es una metodología española para implementar un sistema de gestión de riesgos derivados del uso de tecnologías de la información, como parte del gobierno de las TI (Magerit, 2012).”

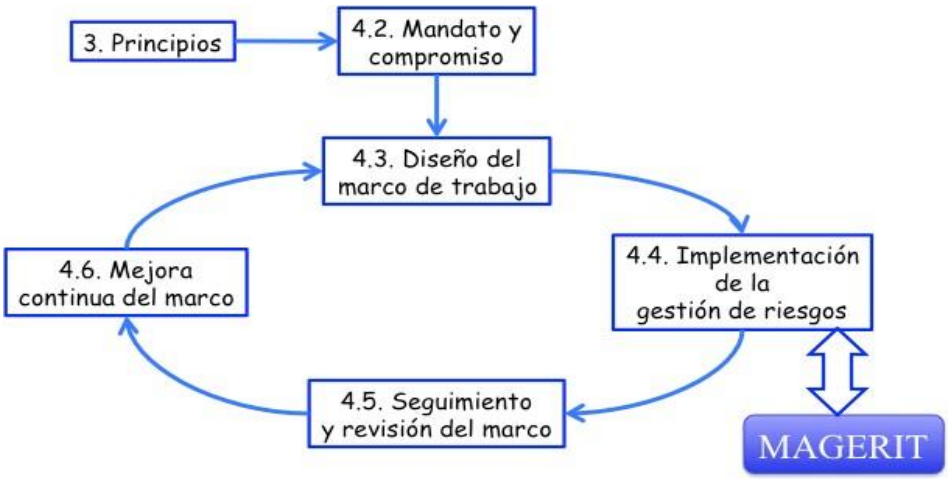

Gráfico N° 5. ISO 3100 como marco de referencia para la gestión de riesgos

Fuente: (Magerit, 2012)

Magerit, propone un método para el análisis de los riesgos y la planificación de medidas que permitan mantener los riesgos bajo control (Espinoza Aguinaga, 2013).

La metodología define las etapas siguientes:

1. Planificación de la gestión de riesgos, donde se establecen los requisitos de inicio del proceso.
2. Análisis de riesgos, donde se identifican y valoran los activos de TI que serán considerados en el proceso de gestión de riesgos.
3. Tratamiento de riesgos, donde se identifican los servicios, funciones y métodos de las salvaguardas que permitirán reducir el riesgo detectado.
4. Selección de salvaguardas, donde se evalúan las salvaguardas para seleccionar las más adecuadas para su implementación.

2.5. Ciclo de Deming

La implementación de un SGSI no consiste solo en instalar equipos de seguridad o contratar una empresa especializada que se encargue la implementación de controles y su monitoreo. Un SGSI integra una serie de estrategias, estructuras organizativas, procesos, normativas, registros, etc. que en conjunto conforman un sistema que mejora continuamente para alcanzar un

nivel óptimo de protección de la información (Robles & Rodriguez de Roa, La gestión de la seguridad en la empresa, 2016).

Por ello, es que las normativas relacionadas a la seguridad de la información, como son la familia de normas ISO/IEC 2700x, contemplan un marco de referencia conocido como Modelo del PDCA (Planificar-Hacer-Evaluar-Corregir); modelo popularizado por W. Edwards Deming, como el "Ciclo Deming", con el propósito de lograr este objetivo. Es un modelo relacionado a la gestión de la calidad ISO 9001 (Robles & Rodriguez de Roa, La gestión de la seguridad en la empresa, 2016).

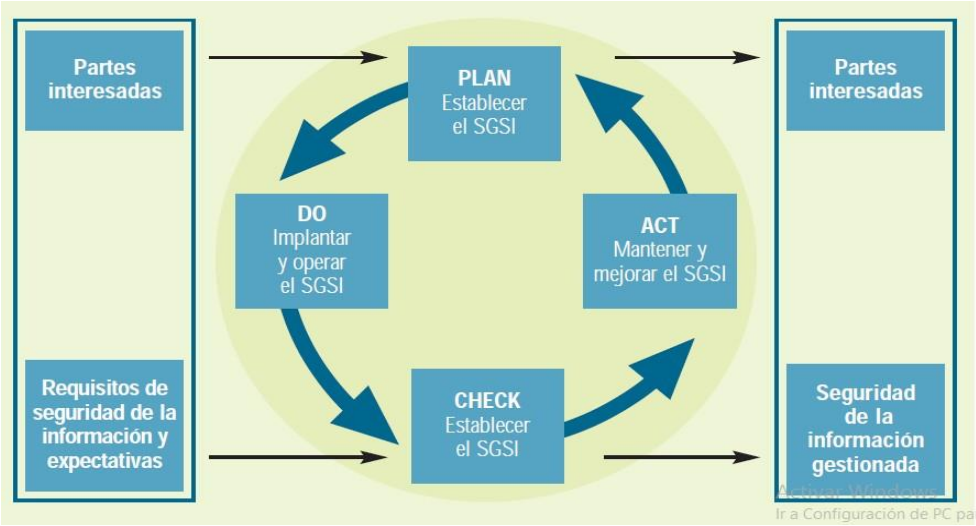

Gráfico N° 6. Ciclo Deming

Fuente: (Robles & Rodriguez de Roa, La gestión de la seguridad en la empresa, 2016)

Las etapas del modelo PDCA se describen a continuación:

a. Plan. En esta etapa se planifica, define y establece la necesidad del un SGSI, considerando el entorno y contexto bajo el cual se desenvuelve la organización, como su estructura organizativa, rubro o giro del negocio, normativas, etc. También se identifican las políticas generales de seguridad y los objetivos que se pretenden lograr con la implementación del SGSI. Otro aspecto importante de esta fase es el establecimiento de métodos para identificar, analizar y evaluar los riesgos, la selección de los objetivos de control y sus correspondientes controles para el tratamiento de los riesgos. Como producto final de esta fase se realiza la declaración

de aplicabilidad, es decir, se define que dominios de seguridad abarcará el SGSI.

b. Do (Hacer o implementar). Esta etapa contempla el desarrollo e implementación de un plan a medio y largo plazo para el tratamiento adecuado de los riesgos. En esta fase, se identifican, evalúan y seleccionan los controles que se implementarán para lograr los objetivos de control definidos en la fase de planificación. En esta fase, también se realizan las actividades de formación de las personas para generar concienciación y conocimiento, que garantice la correcta implementación de los controles.

c. Check (Verificar). En esta etapa se realizan las actividades de seguimiento, monitorización y revisión los mecanismos de protección implementados; así como de los controles. Incluye actividades de auditorías internas del SGSI y evaluación de los controles.

d. Act (Actuar y mejorar). En la etapa anterior se detectan las debilidades en el SGSI. Estas debilidades deberán ser superadas mediante las acciones y medidas correctivas o preventivas apropiadas que se planifiquen y ejecuten en esta etapa con fines de mejorar el SGSI.

2.6. Definición de términos

- **Aceptación o tolerancia del riesgo:** Conocida también como tolerancia al riesgo. Es la definición de los umbrales que dividen los niveles de riesgo en aceptables y no aceptables para la organización.
- **Activo:** Es la información, en cualquier formato, y el equipamiento que lo contiene, que tiene valía para la organización.
- **Amenaza:** Es la causa con potencial para generar incidentes de seguridad inesperados, ocasionando algún daño en los sistemas, aplicaciones, servicios.
- **Análisis de riesgo:** Es un método establecido por la organización para identificar y tipificar riesgos asociados a la seguridad de la información.
- **Control:** Son los diferentes mecanismos, que una organización diseña e implementa, para el tratamiento de los riesgos de seguridad de la información. Estos mecanismos incluyen: políticas, estructuras

organizativas, normativas, procesos, etc.; es decir, que pueden ser de diferente naturaleza: procedimientos administrativos, tecnológicos, legales, de gestión, etc.

- **Declaración de aplicabilidad (SOA):** Es la definición y documentación de los objetivos de control y controles que serán aplicados en una organización como parte de la gestión de riesgo.
- **Evaluación del riesgo:** Es un método establecido por la organización para estimar o calcular el nivel de exposición al riesgo, tomando como referencia un criterio que permite identificar su nivel de importancia o gravedad.
- **Evento de seguridad de información:** Es un hecho, suceso u ocurrencia sobre un equipo, sistema, aplicación, servicio, que define un estado de potencial o posible riesgo que está fuera de los parámetros establecidos en las políticas o controles de seguridad de la información.
- **Gestión del riesgo:** Es el conjunto de acciones, actividades, estructuras organizativas, y funciones planificadas y aplicadas para planificar, organizar, dirigir y controlar los riesgos dentro de una organización. Normalmente utilizan marcos de referencia aceptados y contextualizados al tipo, tamaño y giro de negocio.
- **Incidente de seguridad de información:** Es un evento o conjunto de eventos imprevistos, con el potencial de afectar significativamente la seguridad de la información y comprometer la continuidad de los procesos del negocio.
- **Política de seguridad de la información:** Son los lineamientos generales, establecidos por los entes de más alto nivel de una organización, dirigir la gestión de riesgos.
- **Riesgo residual:** Es el nivel de riesgo que se logra después de aplicar las medidas de seguridad y controles en la fase de tratamiento de los riesgos.
- **Riesgo:** Es la estimación o medición de la magnitud del daño que puede ocasionar una amenaza.
- **Tratamiento del riesgo:** Es el procedimiento seguido para determinar e identificar los riesgos que están dentro o fuera de la aceptabilidad, con la finalidad de seleccionar las medidas de seguridad y controles necesarios para mitigar los riesgos no tolerables.
- **Vulnerabilidad:** Es un estado de debilidad que tiene un activo específico o un conjunto de activos, que una amenaza puede aprovechar para materializarse.

CAPITULO III: MÉTODOS Y MATERIALES

3.1. Formulación del problema

¿De qué manera se relaciona la gestión de la seguridad de la información con la gestión de riesgos de TI en las empresas agroindustriales azucareras?

3.2. Tipo de investigación

Este trabajo de tesis se ha tipificado como **descriptiva propositiva no experimental,** utilizándose un paradigma mixto para el tratamiento de los datos, es decir, se obtuvieron datos de carácter cualitativo y cuantitativo.

a. La investigación es de tipo **descriptiva**, porque en la fase exploratoria, cuyo propósito fue familiarizarse y conocer cómo se gestiona la seguridad de la información en la empresa para obtener información de la propia realidad sobre el objeto de estudio, determinando sus causas y efectos, se utilizó un enfoque descriptivo analítico diagnóstico; y en un segundo momento, se utilizó un enfoque descriptivo narrativo estructurado para explicar la funcionalidad y operatividad de cada uno de los componentes que se consideraron en el modelo de SGSI propuesto, y que metodológicamente fueron desarrollados en el marco metodológico que se construyó para este fin, tomándose como guía las normas de la familia ISO/IEC 2700x y la metodología española Magerit.

b. La investigación es de tipo **propositiva** porque se desarrolló una propuesta de SGSI fundamentada en la necesidad o el vacío que tiene la empresa en relación a la gestión de la seguridad de la información para superar los problemas que tienen actualmente y las deficiencias encontradas. Sin embargo, no se pretende intervenir en la realidad, por cuanto los resultados de la investigación quedarán a modo de propuesta.

c. La investigación es de tipo **no experimental** porque el modelo de SGSI propuesto no fue evaluado para identificar sus efectos de la realidad, sino que fue evaluado a través de un juicio de expertos del tipo Delphi, en la que personas con autoridad y responsabilidades en seguridad de la información dentro de la empresa, valoraron el cumplimiento de cada uno de los criterios que se desearon lograr con la propuesta, en relación a los marcos de referencia teóricos y los estándares utilizados como guía.

3.3. Método de investigación

En la investigación se aplicaron los siguientes métodos:

a. **Descriptivo.** Este método permitió desarrollar el diagnóstico de la problemática de la empresa en relación a la seguridad de la información y para describir cada uno de los componentes que conforman la propuesta de SGSI, utilizándose la investigación bibliográfica, como artículos, normas y estándares, con el propósito de tener un entendimiento y conocimiento más claro y amplio del tema de investigación, y con ello, efectuar un análisis más profundo; así como, para recomendar las acciones de mejora.
b. **Analítico.** El análisis realizado en la investigación permitió identificar los componentes principales de los marcos de referencia utilizados, como son la ISO/IEC 27000 y la metodología Magerit, comprenderlos y aplicarlos como guía para la construcción del modelo propuesto.
c. **Sintético.** A partir del diseño teórico de la investigación, se realizó una síntesis para la construcción del modelo de SGSI y su correspondiente marco metodológico, contextualizado a la realidad de la empresa.
d. **Inductivo**. A través de este método se realizaron las conclusiones de carácter general tomando como base los resultados obtenidos y la información descrita en los hechos de carácter particular en la empresa, tomada como caso de estudio.
e. **Deductivo**. Se aplicó para llegar a las particularidades necesarias para adecuar el modelo de SGSI al contexto de la empresa tomada como caso de estudio, a partir de las buenas prácticas que proponen los marcos de referencia ISO/IEC 27000 y la metodología Magerit.
f. **Estadístico.** En la descripción del problema de la investigación, se realizó el procesamiento estadístico de datos, como parte del diagnóstico situacional.

3.4. Técnicas, instrumentos, equipos y materiales de recolección de datos

Las técnicas aplicadas en la investigación para la recogida de la información fueron: entrevistas y análisis documental con la finalidad de conocer e identificar los aspectos más relevantes sobre seguridad de la información y las causas que lo ocasionan. Del mismo modo, se realizó un trabajo de campo, para encontrar información histórica que permitió realizar valoraciones, evaluaciones o tomar algunas decisiones en las tareas de la metodología desarrollada, donde se hacía necesario, para demostrar la funcionalidad y operatividad del modelo propuesto.

a. **La entrevista estructurada o formal**. Esta técnica se aplicó para obtener información del personal que tiene autoridad y responsabilidad en la gestión de la seguridad de la información en la empresa, a partir la elaboración de una guía de entrevista.

b. **Revisión bibliográfica y documental**. Se realizó el análisis documental de material sobre gestión de la seguridad de la información y la gestión de los riesgos de TI para el diseño teórico de la investigación.

c. **La encuesta.** La técnica de la encuesta se utilizó en el proceso de valoración del modelo de SGSI, por parte de los expertos.

d. **La observación directa.** Para algunas tareas del proceso metodológico que se desarrolló en la construcción de la propuesta de SGSI, fue necesario realizar un trabajo de campo, a través de la observación directa, con la finalidad de analizar el funcionamiento de la empresa y describir la situación actual del sistema de gestión de la seguridad de la información en la empresa.

3.5. Metodología para la implementación del modelo de gestión de riesgos de TI

La familia de normas ISO/IEC 2700x y la metodología Magerit, se utilizaron como guía para la construcción del modelo de SGSI propuesto. Así mismo, para la implementación del modelo se diseñó la siguiente metodología:

Fase 1: Inicio del proyecto
Fase 2: Determinación del alcance del SGSI propuesto
Fase 3: Análisis y evaluación de los escenarios de riesgos de TI
Fase 4: Tratamiento de los riesgos de TI
Fase 5: Estructuración de las políticas de seguridad de la información

3.5.1. Tareas de la Fase 1: Inicio del proyecto

En esta etapa se definieron los requisitos y condiciones iniciales y básicas que deben tenerse en cuenta para la construcción del modelo de gestión de seguridad de la información en la empresa.

Los aspectos considerados como condiciones iniciales son:

a. Identificación del proyecto
b. Justificación del proyecto
c. Definición de las políticas generales de seguridad de la información
d. Determinación de los procesos para el alcance del proyecto

3.5.2. Tareas de la Fase 2: Definición del alcance del SGSI

La norma ISO 27001, determina que el alcance de un SGSI se realiza tomando como referencia el contexto y entorno de la organización, considerando su estructura organizativa, procesos, activos, tecnología y otros elementos relacionados (NTP-ISO/IEC 27001, 2014).

El propósito de definir el alcance del SGSI, es identificar los activos de TI que serán considerados en la evaluación de los riesgos, independientemente de su ubicación, quienes son los responsables de su gestión o quienes tiene los privilegios para su uso.

Las tareas consideradas en esta fase se describen a continuación:

a. Identificación de procesos de negocio: Para la identificación de los procesos negocio se utilizó la técnica de mapeado de procesos y sub procesos. Los procesos que deberán ser considerados en el alcance del SGSI serán los procesos misionales o principales.

b. Definición del catálogo de activos de TI: A partir de los procesos de negocio identificados dentro del alcance del SGSI, se identifica el catálogo o inventarios que dan soporte a los procesos considerados en la selección.

Para la catalogación del inventario se utilizará el siguiente formato:

- Denominación del activo de TI
- Categoría del activo de TI. Para categorizar a los activos se utilizaron las siguientes nominaciones: (1) Información, (2) Software, (3) Hardware, (4) Servicios y (5) Personal

- Clasificación. Para la clasificación de los activos de TI, se utilizó un criterio de accesibilidad, de la siguiente manera: (1) Confidencial, (2) Uso Interno y (3) Público
- Frecuencia de uso. Para determinar la frecuencia de uso y explotación del activo de TI, se utilizó la siguiente nominación: (1) Diario, (2) Mensual, (3) Anual y (4) Otro
- Ubicación del activo. Dependiento del tipo de activo, la ubicación puede ser física o lógica
- Usuario responsable del uso o explotación del activo de TI
- Responsable de la custodia del activo de TI
- Responsable del activo de TI
- Criticidad del activo. Para valorar de la criticidad o importancia de los activos de TI, se utilizó la escala: (1) Alto, (2) Medio o (3) Bajo
- Procesos relacionados. Se identificaron los procesos que están relacionados con cada activo de TI.

c. Identificación de brechas de seguridad de la información: Uno de los aspectos importantes en la definición del alcance del SGSI es determinar qué aspectos de la seguridad de la información están siendo cubiertos o no cubiertos actualmente, así como identificar en qué medida se realiza.

Para el análisis de brechas se aplicará un método descriptivo comparativo entre la situación real de la seguridad de la información en la empresa y las buenas prácticas de seguridad o controles que propone la norma ISO/IEC 27002. Para este propósito se elaboró como instrumento un Check List de cumplimiento de la norma mencionada.

Tabla N° 4. Check List para identificar brechas de seguridad de la información

Ítem	Dominio	Cumple (S/N)	Nivel de cumplimiento
1	Política de seguridad de la información		
2	Organización de la seguridad de la información		
2	Gestión de activos		
3	Seguridad ligada a los Recursos Humanos		
4	Seguridad física y del entorno		
5	Gestión de las comunicaciones y las operaciones		
6	Control de accesos		
7	Adquisición, desarrollo y mantenimiento de sistemas de información		
8	Gestión de incidentes de seguridad de la información		
9	Gestión de la continuidad del negocio		
10	Conformidad		

Fuente: elaboración propia"

3.5.3. Tareas de la Fase 3: Análisis y evaluación de escenarios de riesgo de TI

Para la definición de las tareas de la Fase 3, se tomó como referencia la metodología Magerit, identificándose los componentes que deberán ser considerados en el análisis y evaluación de los riesgos de TI.

En la gráfica siguiente se aprecia que los elementos de un modelo de gestión de riesgos de TI, según la metodología Magerit, son:

- Los activos de TI
- La estimación de la criticidad de los activos de TI
- Las amenazas que pueden afectar los activos de TI
- El impacto en el negocio debido a la ejecución de una amenaza
- La frecuencia de una amenaza

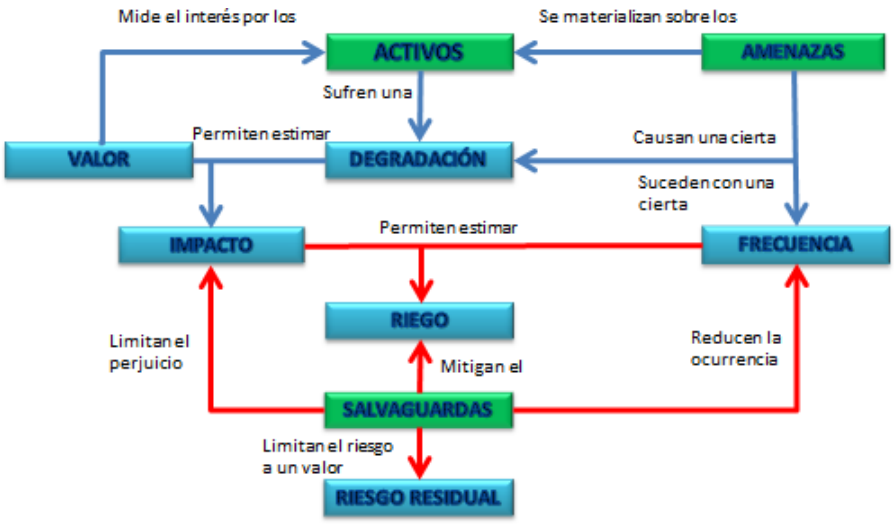

Gráfico N° 7. Elementos de la gestión de riesgos de TI

Fuente: (Magerit - Libro 1, 2012)

En base al modelo de gestión de riesgos de TI mostrado y el marco teórico referente a gestión de riesgos, se definieron las siguientes tareas:

a. Inventario de activos

Se analizarán los procesos de negocio que han sido definidos dentro del alcance del SGSI, para identificar los activos de información y de TI que serán considerados en la evaluación de riesgos.

El inventario de activos debe considerar las categorías de activo propuesto en la metodología Magerit.

El formato para el registro del inventario de activos se muestra a continuación.

Tabla N° 5. Tabla de referencia para la tipificación de los activos de TI

Tipo	Código	Detalle
Activo de información (I)	I1	Información electrónica
	I2	Información escrita
	I3	Documentos administrativos en papel
	I4	Documentos en formato digital (.doc. pdf, etc.)
Activo de software (SW)	SW1	Sistemas operativos
	SW2	Aplicaciones comerciales y utilitarios
	SW3	Aplicaciones desarrolladas por terceros
	SW4	Aplicaciones desarrolladas a medida
	SW5	Sistemas DBMS
	SW5	Otro tipo de aplicaciones
Activo de hardware (HW)	HW1	Equipo de procesamiento
	HW2	Equipo de comunicaciones
	HW3	Medio de almacenamiento
	HW4	Mobiliario y equipamiento
	HW5	Otros equipos
Servicios terceros (S)	S1	Procesamiento y comunicaciones
	S2	Servicios generales
	S3	Otros servicios

Fuente: Elaboración propia, adaptado de (Magerit - Libro 1, 2012)"

Así mismo, para cada activo se debe registrar la siguiente información:

- Clasificación: Confidencial, Restringido (o de uso interno), Público
- Frecuencia de uso: Anual, Mensual, Diario
- Ubicación física o lógica
- Usuario responsable de su uso
- Usuario responsable de su custodia
- Usuario responsable del activo
- Procesos donde se usa el activo
- Valor del activo. Para la valoración del activo se utilizará la siguiente tabla de referencia:

b. Determinación de la criticidad de los activos de TI

Cada uno de los activos de TI inventariados fueron evaluados para determinar su nivel de criticidad.

Para determinar el nivel de criticidad de los activos inventariados se evaluó y valoró las características de seguridad de la información considerados por la ISO 27001 como son: confidencialidad, integridad y disponibilidad. Para la valoración de los tres criterios mencionados se utilizó una escala de 1 a 3, en la que cada nivel de la escala representa el nivel de afectación del criterio de seguridad en caso de que el activo evaluado sea impactado negativamente por algún evento o incidente de seguridad de la información (amenaza).

La siguiente tabla muestra las escalas de valoración de cada uno de las tres características de seguridad de la información.

Tabla N° 6. Escala para la valoración de los criterios de seguridad de la información en los activos de TI

Criterio	Valor en escala	Descripción
Disponibilidad	1	No existe riesgo en el funcionamiento de la empresa en relación a sus operaciones, aspectos legales, reputación, si el activo no está disponible o se destruye.
	2	Puede paralizar parcialmente el funcionamiento de la empresa, ocasionando impactos leves en los procesos, reputación y aspectos legales en la empresa, si el activo no está disponible o se destruye.
	3	Puede paralizar significativamente el funcionamiento de la empresa, ocasionando impactos negativos en las operaciones, aspectos legales y reputacionales, si el activo no está disponible o se destruye.
Integridad	1	No existe riesgo en el funcionamiento de la empresa en relación a sus operaciones, aspectos legales, reputación, si el activo no está completo o está modificado.
	2	Puede paralizar parcialmente el funcionamiento de la empresa, ocasionando impactos leves en los procesos, reputación y aspectos legales en la empresa, si el activo no está completo o está modificado.
	3	Puede paralizar significativamente el funcionamiento de la empresa, ocasionando impactos negativos en las operaciones, aspectos legales y reputacionales, si el activo no está completo o está modificado.
Confidencialidad	1	No existe riesgo en el funcionamiento de la empresa en relación a sus operaciones, aspectos legales, reputación, porque el activo es de conocimiento público.
	2	Puede paralizar parcialmente el funcionamiento de la empresa, ocasionando impactos leves en los procesos, reputación y aspectos legales en la empresa, porque el activo podrá ser utilizado o divulgado hacia o entre el personal de la empresa
	3	Puede paralizar significativamente el funcionamiento de la empresa, ocasionando impactos negativos en las operaciones, aspectos legales y reputacionales, porque el activo contiene información muy sensible de la empresa

Fuente: Desarrollo propio, basado en las escalas de valoración de la metodología Magerit"

Para estimar el nivel de criticidad de los activos de TI se utiliza la siguiente relación:

Criticidad del activo = valor de confidencialidad + valor de integridad + valor de disponibilidad

(fórmula N° 1)

c. Identificación de las amenazas y vulnerabilidades

Para la tarea de identificación de amenazas, consideradas como eventos que pueden que causar un incidente imprevisto o que puede degradar los activos de TI, se tomará como referencia el

catálogo de amenazas propuesto en la metodología Magerit, bajo la siguiente clasificación:

- Amenazas del tipo natural (algún tipo de sismo, incendio natural, tormentas, etc.)
- Amenazas del tipo industrial (fuego, explosiones, corto circuito, sobrecalentamiento, etc.)
- Amenazas de origen humano (descuidos, mal intensiones, irresponsabilidades, incumplimiento de funciones, etc.)
- Amenazas del tipo tecnológico (fallas en la red, fallas en la BD, virus, hackeo, etc.)
- Amenazas de origen operacional (mala logística, fallas en el proceso, obsolescencia, etc.)
- Amenazas del tipo social (huelgas, vandalismo, protestas, etc.)

Del mismo modo, para la tarea de identificación de vulnerabilidades, consideradas como las debilidades, incongruencias, ausencias, fallas, etc., en los mecanismos de seguridad, que pueden ser aprovechadas por las amenazas, se utilizó la siguiente clasificación:

- Debilidades en el control de accesos
- Debilidades en la seguridad ligada a los Recursos Humanos
- Debilidades en la seguridad física y del entorno
- Debilidades en la gestión de las comunicaciones y las operaciones
- Debilidades en el adquisición, desarrollo y mantenimiento de sistemas de información”

d. Estimación del impacto

Para estimar el impacto de una amenaza se utilizará una escala de cinco ítems. Los criterios para la valoración de estos escenarios de riesgo han sido tomados de la metodología Magerit (Magerit - Libro 1, 2012): en base a los objetivos de la investigación, seleccionándose los siguientes:

- Continuidad o interrupción de los servicios

- Economía de la empresa e intereses comerciales
- Seguridad.

Tabla N° 7. Escala de valoración del impacto de una amenaza

Nivel de impacto	Continuidad de los servicios	Economía de la empresa e intereses	Seguridad
5: Muy Alto	Ocasiona interrupciones serias en las actividades de la empresa, generando mala reputación en los clientes. Ocasiona destrucción de los equipos o en las instalaciones	Ocasiona pérdidas económicas muy elevadas. Ocasiona incumplimientos muy graves con las obligaciones y responsabilidades contractuales importantes	Causan incidentes muy graves relacionados con la seguridad No se puede realizar seguimiento o investigación de los incidentes.
4: Alto	Ocasiona interrupciones graves en las actividades de la empresa, con paralizaciones en la prestación de algunos servicios. Ocasionan incidentes que demandan tiempos y costos considerables de recuperación	Ocasiona pérdidas económicas graves. Ocasiona incumplimientos serios con algunas obligaciones contractuales importantes	Causan incidentes serios relacionados con la seguridad Hay dificultad para realizar el seguimiento o investigación de los incidentes.
3: Medio	Ocasiona interrupciones en las actividades de la empresa generando condiciones operativas negativas que aumentan la carga de trabajo y disminuyen su eficiencia	Ocasiona pérdidas económicas significativas. Ocasiona incumplimientos significativos con algunas obligaciones contractuales	Causan incidentes significativos relacionados con la seguridad Se puede realizar seguimiento o investigación de los incidentes.
2: Bajo	Ocasiona interrupciones en las actividades de la empresa generando algunas interferencias en los servicios, continuando con procedimientos de emergencia	Ocasiona ciertas mermas en los ingresos. Ocasionan incumplimientos leves en las obligaciones contractuales	Causan incidentes de seguridad con poca repercusión en los activos de información.
1: Muy Bajo	Ocasionan interrupciones en las actividades de poca importancia	Ocasionan pérdidas económicas mínimas. Causa incidencias de pequeño valor comercial	Causan incidentes de seguridad de casi nula repercusión en los activos de información.

Fuente: Elaboración propia, tomando como referencia la propuesta de la metodología Magerit"

e. Estimación de la probabilidad de ocurrencia

Para estimar de la probabilidad de ocurrencia de una amenaza se utilizó como referencia la siguiente tabla, donde se muestra una escala de valoración en cinco niveles:

Tabla N° 8. Escala de valoración para la probabilidad de ocurrencia

Nivel	Descripción del nivel
5: Muy Alto	Ocurre de manera diaria Los mecanismos de seguridad implantados son inexistentes o ineficientes.
4: Alto	Ocurre de manera semanal Los mecanismos de seguridad implantados poco eficientes.
3: Medio	Ocurre de manera mensual Los mecanismos de seguridad implantados a veces pueden impedir la amenaza
2: Bajo	Ocurre de manera anual Los mecanismos de seguridad implantados son eficientes para impedir una amenaza
1: Muy Bajo	Ocurre más de una vez al año Los mecanismos de seguridad implantados son altamente eficientes que casi siempre impiden una amenaza

Fuente: Elaboración propia"

f. Estimación del nivel de exposición al riesgo

La estimación de los niveles de riesgos de TI sirve para determinar qué tan expuesta está la empresa en cada uno de los escenarios de riesgos. El análisis debe considerar las vulnerabilidades y amenazas identificadas para cada activo de TI.

Para realizar este cálculo se utilizará las siguientes fórmulas:

$$\text{Criticidad del activo} = C + I + D \quad \text{(fórmula N° 2)}$$

$$\text{Riego} = \text{Criticidad} + (\text{Probabilidad} * \text{Impacto}) \quad \text{(fórmula N° 3)}$$

Se estableció una escala para determinar los niveles de tolerancia a los riesgos. Cada nivel corresponde a un rango de valores de los niveles de riesgo.

Tabla N° 9. Escala para determinar el nivel de tolerancia a los riesgos

Nivel	Descripción del nivel
Totalmente Tolerable o Aceptable (TT)	4 – 15
Con regularidad es Tolerable o Aceptable (RT)	16 – 25
No es Tolerable o No es Aceptable (NT)	26 – 40

Fuente: Elaboración propia

Para los niveles de riesgo que se encuentran fuera de los rangos de tolerancia “Regularmente Tolerable” o “No Tolerable”, deberán ser tratados mediante acciones para redefinir salvaguardas y controles.

Para los niveles de riesgo que se ubiquen en el rango de “Totalmente Tolerable”, son opcionales para ser tratados.

3.5.4. Tareas de la Fase 4: Tratamiento y control del riesgo

a. Identificación de los mecanismos de seguridad para la mitigación de los riesgos no tolerables

En esta tarea se identifican las medidas de seguridad que implantará la organización para la reducción del riesgo. Estas medidas pueden ser tecnológicos o administrativos. Algunos escenarios de riesgo se pueden con los mecanismos de seguridad existentes; sin embargo, otros escenarios de riesgo, requieren de elementos técnicos o tecnológicos.

b. Definición de la estrategia de tratamiento de los mecanismos de seguridad y controles

Las estrategias para el tratamiento de los mecanismos de seguridad y controles han sido clasificadas de la siguiente manera:

a. **Reducción del riesgo (R):** Esta estrategia se aplica generalmente cuando se cuenta con la capacidad instalada necesaria (personal calificado, infraestructura y normativas) y la economía suficiente para la implementación de los mecanismos de seguridad y controles.

b. **Aceptar el riesgo (A):** Esta estrategia se aplica generalmente cuando NO se cuenta con la capacidad instalada necesaria (personal calificado, infraestructura y normativas) y ni con la economía suficiente para la implementación de los mecanismos de seguridad y controles.
c. **Transferencia del riesgo (T):** Esta estrategia se aplica generalmente cuando se cuenta NO se cuenta con la capacidad instalada necesaria (personal calificado, infraestructura y normativas), pero si con la economía suficiente para la implementación de los mecanismos de seguridad y controles transfiriendo a una tercera parte especializada.
d. **Evitar el riesgo (E):** Esta estrategia generalmente se aplica cuando el origen de la amenaza puede ser eliminado, para evitar la presencia del riesgo.

c. Estimación del riesgo residual

El riesgo residual se estima luego de la implementación de los mecanismos de seguridad y los controles, utilizando las mismas relaciones o fórmulas para la estimación del riesgo efectivo.

Riego Residual = Criticidad + (Probabilidad Residual * Impacto Residual)
(fórmula 4)

Para los riesgos que resulten nuevamente regularmente tolerable o no tolerable se debe redefinir nuevamente salvaguardas. Los riesgos que resulten totalmente tolerables, son considerados riesgos despreciables, y no requieren más acciones, que el monitoreo periódico.

d. Plan de tratamiento de riesgos

Para cumplir con esta tarea se debe realizar lo siguiente:

- Elaborar un plan para el tratamiento de los riesgos donde se definan los objetivos de seguridad que se desean lograr, se organicen un conjunto de actividades para la implantación de los mecanismos de seguridad y sus respectivos controles, asignándoles los recursos necesarios, definiendo los roles y funciones a las personas encargadas de su ejecución.
- Ejecutar las actividades del plan de tratamiento de riesgos que permitan alcanzar los objetivos planteados, monitoreando y evaluando la efectividad de los mecanismos de seguridad, los gastos ejecutados y el cumplimiento de las responsabilidades asignadas.

CAPITULO IV: RESULTADOS Y DISCUSIÓN

4.1. Desarrollo del modelo de SGSI

4.1.1. Fase 1: Inicio del proyecto

El propósito de esta tarea es determinar los requisitos y condiciones iniciales y básicas que deben considerarse para la construcción del modelo de gestión de seguridad de la información en la empresa.

En esta tarea se realizaron entrevistas a las personas que tienen la autoridad y responsabilidad de la seguridad de la información en las diferentes áreas de la empresa y se revisó la documentación relacionada a ello. Los resultados de este levantamiento de información, permitió definir las siguientes características iniciales para la construcción de la propuesta de SGSI.

Tabla N° 10. Condiciones iniciales para el inicio del proyecto de SGSI

Identificación del proyecto
Modelo de gestión de seguridad de la información basado en las normas ISO/IEC 2700x y la metodología Magerit, para mitigar los riesgos de TI en la empresa.
Justificación del proyecto
La empresa necesita de un sistema de gestión de seguridad de la información (SGSI) que permita identificar, analizar y tratar de manera orgánica y sistematizada los escenarios de riesgo de tecnologías de la información que amenazan a los activos de información y que como consecuencia puedan impactar negativamente en las operaciones del negocio, afectar económica y financieramente a la empresa o puedan causar mala reputación en los clientes. El SGSI debe contemplar las políticas, métodos y lineamientos para diseñar los procedimientos que permitan identificar, analizar y evaluar los riesgos operativos de TI, identificar las amenazas y las vulnerabilidades relacionados con los activos de información, determinar los niveles de exposición a los riesgos identificados, tratar los riesgos de TI a través de controles para salvaguardar los activos de información que dan soporte a los procesos del negocio, debidamente alineados a los objetivos y políticas de seguridad de la información de la empresa.
Definición de las políticas generales de seguridad de la información
La empresa Agroindustrial Pomalca SAA ha definido los siguientes requisitos básicos de seguridad de la información, en concordancia con la ISO/IEC 27001, los cuales serán considerados como línea base en el desarrollo de la propuesta de SGSI: a. Las políticas para la seguridad de la información deben ser aprobadas por la gerencia de la empresa. Luego de su aprobación deberán ser publicadas y comunicadas a todos los empleados de la empresa, porque tienen el carácter de aplicación obligatoria. b. Las políticas para la seguridad de la información deben ser revisadas anualmente. En el

caso de incidentes extraordinarios o escenarios donde amerite un cambio de las políticas de seguridad o cuando ocurran cambios significativos en los procesos, infraestructura o procedimientos; con la finalidad de asegurar su pertinencia, vigencia, efectividad, conveniencia y mejora continua.

c. La responsabilidad primera de la seguridad de la información será asignada a una Oficialía de seguridad de la información, debiéndose declararse y definirse roles y funciones para todo el personal de la empresa.
d. El acceso a los recursos de información y a la infraestructura de red de la empresa deberá ser controlado y documentarse las acciones de los usuarios con la información de la empresa, con la finalidad de permitir posteriormente su trazabilidad y seguimiento. Para ello, debe definirse y actualizarse en base a los perfiles de los usuarios de TI, según sus funciones dentro de la empresa.
e. Deben identificarse áreas de acceso restringido donde se encuentren activos críticos o información sensible en cualquier formato. Para ello, se establecerán mecanismos de seguridad y perímetros de seguridad.
f. Se deben generar copias de respaldo de la información y de las aplicaciones de negocio en intervalos de tiempo aceptables, con la finalidad de contar con las contingencias necesarias frente a eventos no controlados.
g. En relación a la gestión de incidentes de seguridad de la información, se debe definirse y formalizarse los procedimientos y la asignación de responsabilidades de manera orgánica, para asegurar una respuesta rápida y efectiva a los incidentes imprevistos de seguridad de la información, registrando las ocurrencias para generar una base de conocimientos.

Determinación de los procesos para el alcance del proyecto

El proyecto de construcción del SGSI debe considerar los siguientes procesos de la empresa:

- Atención de requerimientos
- Gestión de proyectos y soluciones
- Desarrollo de soluciones
- Producción y soporte
- Monitoreo de aplicaciones

Para esta primera etapa no se consideran los procesos de gestión documental (secretaría) gestión de personal (planillas), gestión logística, gestión administrativa, gestión financiera contable, afiliación de clientes, servicios al cliente, gestión de cartera de clientes, cobranza, investigación tecnológica, control de calidad.

4.1.2. Fase 2: Determinación del alcance del sistema de gestión de riesgos propuesto

Para la identificación del alcance del SGR se utilizó un método descriptivo de los procesos del negocio a través del mapeado de los procesos de TI con la finalidad de identificar sus subprocesos, interrelaciones entre éstos. Este análisis de realizó con parte de la estrategia para definir el catálogo de activos críticos de TI.

La técnica utilizada para el mapeado de los procesos de TI fue las entrevistas y la observación en campo, en un trabajo colaborativo con los empleados de la empresa.

a. Identificación de procesos de negocio

Para el análisis de procesos de las empresas tipo del sector agroindustrial de azúcar, primero se elaboró un diagrama de bloques para identificar los principales componentes que intervienen en todo el circuito de producción y comercialización del producto. El diagrama siguiente muestra los principales componentes de este circuito:

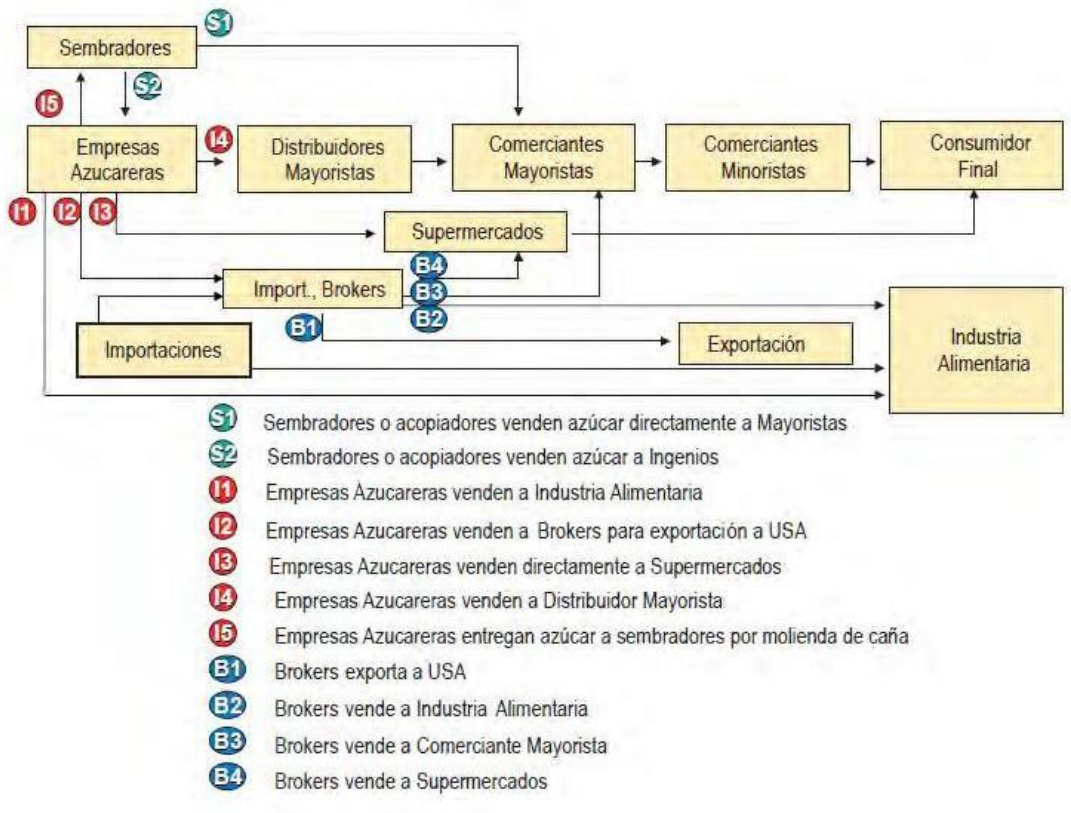

Gráfico N° 8. Diagramas de bloques del circuito de producción y comercialización del azúcar

Fuente: Desarrollo propio

En el diagrama se observa que, de acuerdo al objetivo de la investigación, el análisis se focaliza en el bloque “Empresas Azucareras”, las cuales se encargan del proceso productivo y de la venta inicial del azúcar y sus productos derivados.

En base a ello, se describió el proceso de producción de azúcar de caña, tomando como referencia el proceso de la empresa Agroindustrial Pomalca SAA.

Proceso de fabricación de azúcar

1. **Recepción, descarga y alimentación de la caña**

   Esta área del departamento de maquinaria recibe el nombre de Batey, las cañas a moler son transportada por diversos medios (remolques, camiones, vagones de ferrocarril, etc.), las cuales son pesadas en básculas anexas a las fábricas, posteriormente las cañas se descargan a través de diferentes medios: Grúa Cañera, Grúa Puente, Volteadores Laterales o directamente a los conductores de caña.

Figura N° 1. Carga de la caña en camiones

Figura N° 2. Transporte de la caña a la fábrica

Figura N° 3. Descarga de la caña, usando grúas

El conductor principal de caña, que es largo y lleva la caña a la fábrica, el ancho del conductor es siempre igual al largo de las mazas de los molinos, el conductor consta de dos partes: una horizontal y una inclinada (15 a 22 grados), es movido por un motorreductor de velocidad variable.

Sobre el conductor de caña en muchos ingenios montan los niveladores de caña cuya función consiste en distribuir y en cierto modo nivelar la caña en el conductor.

El nivelador consiste de un eje colocado transversalmente al conductor, en el cual van brazos curvos los que giran en sentido inverso al conductor. La uniformidad del colchón en el conductor permite variaciones mínimas de velocidad para la alimentación de caña a molinos.

2. Extracción del jugo

La caña es desmenuzada con cuchillas rotatorias y una desfibradora antes de molerla para facilitar la extracción del jugo que se hace pasándola en serie, entre los filtros, o mazas de los molinos. Se

utiliza agua en contracorriente para ayudar a la extracción que llega a 94 o 95% del azúcar contenida en la caña. El remanente queda en el bagazo residual que es utilizado como combustible en las calderas, así como materia prima para la fabricación de tableros de bagazo. Esta constituye la primera etapa del procesamiento de fabricación de azúcar crudo.

En las prácticas de molienda, más eficientes, más del 95 % del azúcar contenido en la caña pasa a guarapo; este porcentaje se conoce como la extracción de sacarosa (por de la extracción, o más sencillamente, la extracción).

3. Molinos y conductores

La caña, una vez preparada según los pasos anteriores, cae al primer molino, de éste a través de un conductor intermedio pasa a un segundo molino y así sucesivamente atraviesa hasta el último molino según el tamaño de la batería (4 a 7 molinos los más usados).

El molino consta normalmente de 3 cilindros (2 inferiores y 1 superior entre y arriba de los dos primeros), su misión es la extracción del jugo de la caña, en un principio estos cilindros eran lisos pero posteriormente y hasta la fecha se datan de ranuras (o rayados), pues esto ayuda a la extracción y al agarre del bagazo, al pasar entre los cilindros (mazas) las ranuras varían en su paso y su altura pero en la actualidad se están optando por generalizar a los tamaños mayores usados (2” o 3”) de paso.

Figura N° 4. Extracción del jugo de caña

Inicialmente los cilindros o mazas de un molino eran fijos unos respecto a otros, éstos presentan serios problemas pues al pasar cuerpos extraños (piedras, pedazos de acero, etc.) su soporte, llamada virgen, cedía y ocasionaba grandes problemas además la presión que se ejercía sobre el bagazo quedaba determinada por la altura del colchón de caña a la entrada del molino. Para solucionar esto se comenzó la búsqueda de presiones elásticas, lo que condujo a la colocación de resortes de alto calibre sobre la maza superior, la cual podía levantarse o bajar (flotación), como medio para presionar sobre los apoyos del cilindro superior y es lo utilizado hasta la fecha.

4. Conductores

Son los encargados de llevar el bagazo de un molino a otro, existen varios tipos: los de cadena de arrastre o de rastrillo, los de tablilla persiana, de banda, etc.

Figura N° 5. Conductores de bagazo

Estos están provistos de clutch (o debería de estarlo) los cuales detienen el conductor intermedio (que también son movidos por el mismo molino) cuando cuerpos extraños como metal o piedras pasan a través del mismo o cuando se produce atoramiento o atascamiento (tacos), en los molinos, por tal su funcionamiento debe estar en la mejor forma. Las piedras y los metales causan daño en los cilindros

sobre todo en la destrucción de los dientes lo que ocasiona problemas en la extracción y elevados costos de reparación.

Para el mejoramiento de la extracción de jugo del bagazo se adopta (generalmente antes del último molino) la adición de agua al bagazo, en los molinos anteriores se echa jugo diluido del molino al cual precede y a esto se le llama imbibición (simple o compuesta). La imbibición suele causar problemas pues para el molino se hace más difícil tomar el bagazo imbíbido que seco.

Figura N° 6. Adición de agua al bagazo

5. Purificación del guarapo, clarificación

El jugo de color verde oscuro procedente de los molinos es ácido y turbio. El proceso de clarificación (o defecación), diseñado para remover las impurezas tanto solubles como insolubles, emplea en forma general, cal y calor agentes clarificante. La lechada de cal, alrededor de 16 (0,5 kg) (CaO) por tonelada de caña, neutraliza la acidez natural del guarapo, formando sales insolubles de calcio. El jugo clarificado transparente y de un color parduzco pasa a los evaporadores sin tratamiento adicional.

6. Evaporación

El jugo clarificado, que tiene más o menos la misma composición que el jugo crudo extraído, excepto las impurezas precipitadas por el tratamiento con cal, contiene aproximadamente un 85 % de agua. Dos terceras partes de esta agua se evapora en evaporadores de vacío de múltiple efecto, con esta operación se convierte en matadura. Los

evaporadores trabajan en múltiples efectos, y el vapor producido por la evaporación de agua en el primer efecto es utilizado para calentar el segundo y así, sucesivamente, hasta llegar al quinto efecto que entrega sus vapores al condensador. El condensador es enfriado por agua en recirculación desde el estanque de enfriamiento. Todo este proceso de ebullición ocurre al vacío.

Figura N° 7. Evaporadores del jugo de caña

7. Clarificación del jugo crudo

El proceso es similar a la fosfatación del refundido en unas refinerías de azúcar. En este caso, se añaden al jarabe o meladura cal y ácido fosfórico, luego se airea junto con la adición de un polímero floculante.

8. Cristalización

La meladura pasa a los tachos donde continúa la evaporación de agua, lo que ocasiona la cristalización del azúcar. Es decir que, al seguir eliminando agua, llega un momento en el cual la azúcar disuelta en la meladura se deposita en forma de cristales de sacarosa. Los tachos trabajan con vacío para efectuar la evaporación a baja temperatura y evitar así la caramelización del azúcar.

En este momento se añaden semillas a fin de que sirvan de medio para los cristales de azúcar, y se va añadiendo más jarabe según se evapora el agua. El crecimiento de los cristales continúa hasta que se llena el tacho.

La templa (el contenido del tacho) se descarga luego por medio de una válvula de pie a un mezclador o cristalizador.

9. Centrifugación o purga; reebullicion de las mieles

En los tachos se obtiene una masa, denominada masa cocida, que es mezcla de cristales de azúcar y miel. La separación se hace por centrifugación en las maquinas destinadas a esa labor. De las centrífugas sale azúcar cruda y miel. La miel se retorna a los tachos para dos etapas adicionales de cristalización que termina con los conocimientos, o melaza. El azúcar de tercera se utiliza como pie para la cristalización del segundo conocimiento y el azúcar de segunda para el conocimiento de primera.

Figura N° 8. Reebullición de mieles

El tambor cilíndrico suspendido de un eje tiene paredes laterales perforadas, forradas en el interior con tela metálica, entre éstas y las paredes hay láminas metálicas que contienen de 400 a 600 perforaciones por pulgada cuadrada. El tambor gira a velocidades que

oscilan entre 1000-1800 rpm. El revestimiento perforado retiene los cristales de azúcar que puede lavar con agua si se desea. El licor madre, la miel, pasa a través del revestimiento debido a la fuerza centrífuga ejercida (de 500 hasta 1800 veces la fuerza de la gravedad), y después que el azúcar es purgado se corta, dejando la centrífuga lista para recibir otra carga de masa cosida. Las máquinas modernas son exclusivamente del tipo de alta velocidad (o de una alta fuerza de gravedad) provistas de control automático para todo ciclo. Los azúcares de un grado pueden purgarse utilizando centrífugas continuas.

10. Almacenamiento a granel del azúcar

Es regla general, almacenar el azúcar terminado en grandes depósitos o silos. Los depósitos o silos no solo permiten que se empaquen únicamente durante el día, también dan por resultados altos ahorros, ya que el empacado se puede efectuar en respuesta a los seguimientos de los empaques de jugo de empacar el azúcar conforme se produce y almacena el producto empaquetado.

Figura N° 9. Empaque del azúcar

Figura N° 10. Almacenamiento del azúcar

11. Refinación

El azúcar de primera es refundida o redisuelta con agua; luego es aireado en un recipiente a presión y pasa a las clarificadoras donde las impurezas flotan y el licor clarificado es extraído por la parte inferior.

El licor clarificado es pasado por los filtros de lecho profundo donde se eliminan el resto de las impurezas, y de allí el filtrado es entregado a los tachos de refino. Igual que en los tachos de crudo en estos tachos se elimina agua y se obtiene azúcar refinada cristalizada. La miel es retornada al conocimiento de crudo para mezclarse con la meladura y la azúcar húmeda de las centrifugas pasa a los secadores y de allí al envase.

Luego, se elaboró el mapa de procesos, con la finalidad de identificar los procesos que dan soporte a todo el proceso de producción del azúcar y derivados, en la empresa Agroindustrial Pomalca SAA, clasificándolos en: operativos, estratégicos, de control y de apoyo.

En el gráfico siguiente se visualiza el mapa de procesos de la empresa Agroindustrial Pomalca SAA

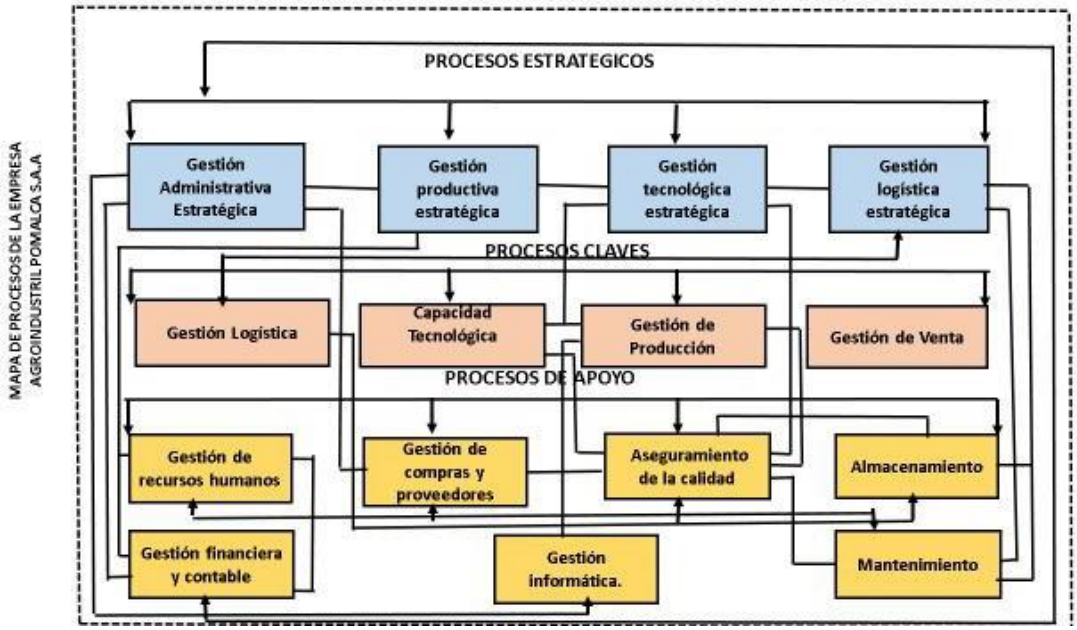

Gráfico N° 9. Mapeado de procesos de la empresa Agroindustrial Pomalca SAA

Fuente: Desarrollo propio

Finalmente, se elaboró el mapa de procesos de TI que dan soporte a los procesos misionales, lo que serán considerados como el alcance del SGSI:

Área de desarrollo:

- Atención de requerimientos
- Gestión de proyectos y soluciones
- Desarrollo de soluciones

Área de producción

- Producción y soporte de TI
- Monitoreo de aplicaciones

A partir de esta delimitación, se elaboraron los subprocesos de las áreas de desarrollo y de producción, las que se muestran a continuación:

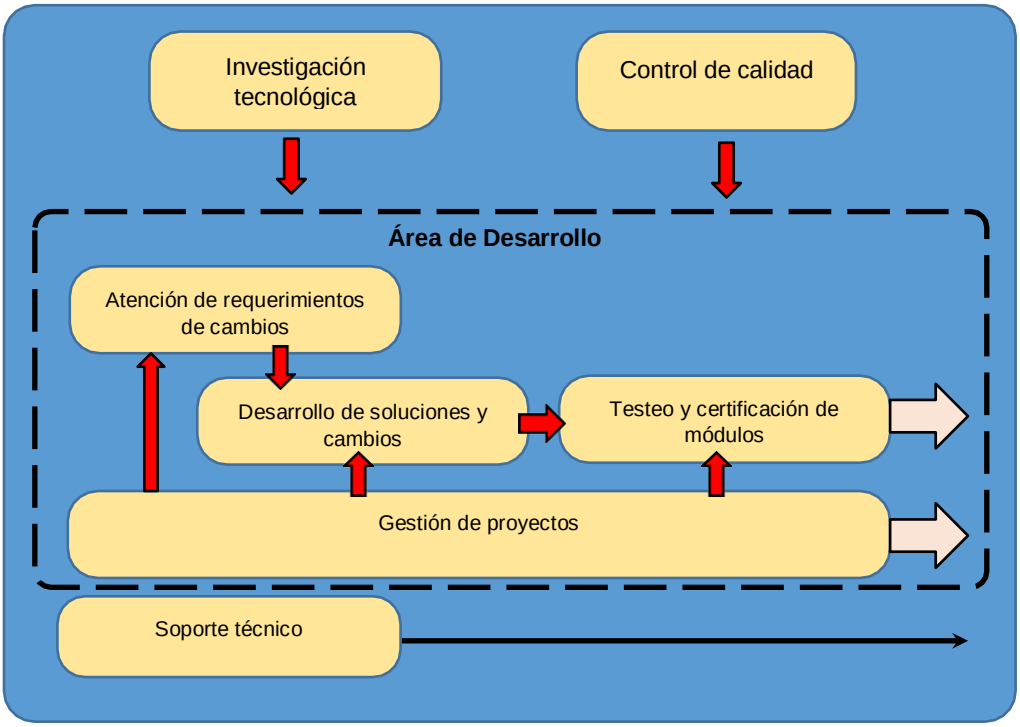

Gráfico N° 10. Mapeado de los procesos del Área de Desarrollo

Fuente: Desarrollo propio

Tabla N° 11. Descripción de los procesos/subprocesos del Área de Desarrollo

	Procesos	Subprocesos	
		Desarrollo	Documento de soporte
AREA OPERATIVA DE DESARROLLO	Investigación tecnológica		Plan de TI
	Atención de requerimientos de cambios	Registro de requerimientos	Ficha de requerimientos
		Autorización de cambio	Ficha de requerimientos
	Desarrollo de soluciones y cambios	Distribución y asignación del trabajo	Plan de trabajo
		Codificación	Librerías de código, estructura de datos, BD
		Gestión de cambios	Ficha de registro de cambios: scripts, datos y carga de datos
		Gestión de versiones	Librería de versiones
		Actualización de manuales y documentación técnica	Manuales
	Testeo y certificación de módulos	Validación funcional Pruebas de integridad	Plan de pruebas Informe de pruebas
	Gestión de proyectos	Gestión de actividades y tiempos Gestión de riesgos	Procedimientos establecidos Documentación de seguimiento
	Soporte técnico	Mantenimiento correctivo Mantenimiento preventivo planificado	Plan de mantenimiento

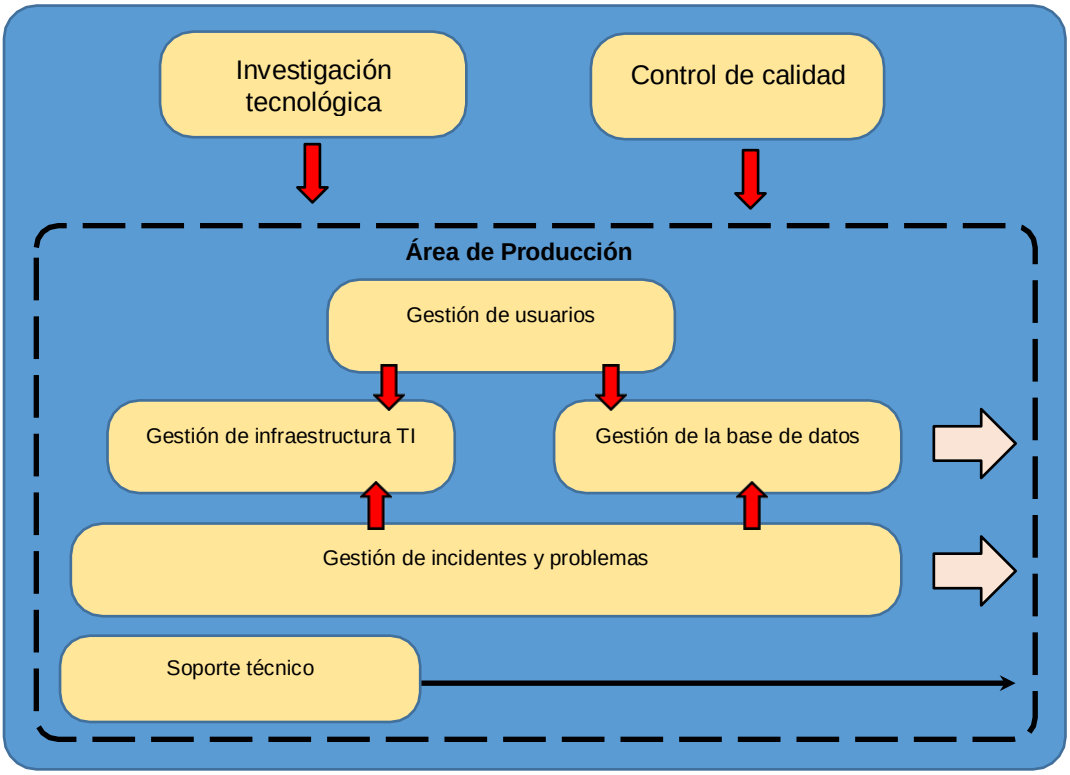

Gráfico N° 11. Mapeado de los procesos de Producción y Soporte de TI

Fuente: Desarrollo propio

Tabla N° 12. Descripción de los procesos/subprocesos del Área de Producción y soporte de TI

	Procesos	Subprocesos	
		Desarrollo	Documento de soporte
AREA OPERATIVA DE PRODUCCIÓN Y SOPORTE DE TI	Investigación tecnológica		Plan de TI
	Gestión de usuarios	Gestión de perfiles de usuario	Procedimiento y reglamento
		Altas, bajas y modificación de cuentas de usuario	Procedimiento y reglamento
	Gestión de infraestructura de TI	Gestión de configuraciones	Procedimiento (no formalizado)
		Gestión antimalware	Procedimiento (no formalizado)
		Gestión de la red	Procedimiento (no formalizado)
		Gestión de página Web	Procedimiento (no formalizado)
		Gestión de telefonía IP	Procedimiento (no formalizado)
	Gestión de base de datos	Gestión de dominios	Procedimiento (no formalizado)
		Gestión de respaldos	Procedimiento y reglamento
	Gestión de incidentes y problemas de TI	Gestión de incidentes Gestión de problemas	Procedimiento (no formalizado)
	Soporte técnico	Mantenimiento correctivo Mantenimiento preventivo planificado	Plan de mantenimiento

b. Catálogo de activos de TI

El catálogo inventariado de los activos de TI se obtuvo del análisis de los procesos en la tarea anterior.

En base a la estructura de catalogación definida en el ítem 2.6.2. b, se realizó la catalogación y el inventario de los activos de TI. El inventario se realizó independientemente para cada una de las áreas consideradas en el alcance del SGSI y el tipo de activo.

Tabla N° 13. Inventario de activos de Información del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Procedimientos y reglamentos de desarrollo	ID		X		X				Carpeta de Documentos de gestión	Personal TI Personal empresa	Jefe TI	Jefe TI		X		X	X	X	X	X
2	Planes de desarrollo (Actividades, tareas, asignación de trabajo)	ID		X			X			Carpeta de proyectos	Personal TI	Jefe TI	Jefe TI		X		X				
3	Cotizaciones y cuadros de evaluación	ID		X					X	Carpeta de Documentos de gestión	Jefe TI	Jefe TI	Jefe TI			X	X	X			X
4	Hojas de requerimientos y cambios aprobadas	ID			X				X	Carpeta de Documentos de gestión	Jefe TI Jefe Desarrollo	Jefe Desarrollo	Jefe Desarrollo	X			X	X			
5	Documentos técnicos de desarrollo (análisis, diseño)	ID		X					X	Carpeta de Documentos de gestión	Jefe Desarrollo Analistas programadores	Jefe Desarrollo	Analistas programadores		X			X	X	X	
6	Registros de Control de Cambios (scripts, BD, carga data)	ID	X				X			Carpeta Control de Cambios	Jefe Desarrollo Analistas programadores Oficial de seguridad	Jefe Desarrollo	Oficial de seguridad	X			X		X		
7	Manuales de usuario	ID			X	X				Carpeta Control de Cambios	Personal empresa	Jefe Desarrollo	Analistas programadores		X			X	X		

8	Informes de las pruebas de testeo y certificación	ID		X					X	Carpeta de Documentos de gestión	Jefe Desarrollo Analistas programadores Jefe de Producción y Soporte	Jefe Desarrollo	Analistas programadores		X			X	X	X	
9	Documentos de versiones de software	ID	X						X	Carpeta Control de Cambios	Jefe TI Jefe Desarrollo	Jefe TI	Jefe Desarrollo	X			X		X		
10	Documentación del personal (HV)	ID			X				X	Carpeta de Documentos de gestión	Administración Jefe de RRHH Jefe TI	Jefe RRHH	Jefe RRHH			X	X				

Tabla N° 14. Inventario de activos de Software del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	.Net, ASP	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X	X	
2	Eclipse (Java)	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X	X	
3	Drupal	SWD		X					X	Servidor	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X					X	X	
4	Aplicativos .Net	SWD		X						PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X	X	
5	Aplicativos Java	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X	X	
6	Aplicativos Visual Basic	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X	X	
7	Cristal Report	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte		X			X	X	X	

8	Modelador datos - Erwin	SWD		X					X	PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X		X	X		
9	Aplicativo graficador – Visio	SWD		X					X	PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X		X	X		
10	Oracle BD	SWD		X		X				Servidor de BD	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X			X		X	X	
11	DB2	SWD		X		X				Servidor de BD	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X			X		X	X	
12	MySQL	SWD		X		X				Servidor de BD	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X			X		X	X	
13	Open Project	SWD		X					X	PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X	X				
14	MS Office	SWD		X		X				PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte		X		X	X	X	X	
15	Aplicativo Virtualización	SWD		X					X	PCs	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte			X			X		
16	Aplicativo – Registro Requerimientos	SWD		X		X				Servidor	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X			X	X			
17	Aplicativo – Control de cambios	SWD		X		X				Servidor	Jefe del área de desarrollo y analistas programadores	Producción y Soporte	Producción y Soporte	X			X		X		

Tabla N° 15. Inventario de activos de Hardware del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	PC (6)	HWD		X		X				Área de desarrollo	Personal TI	Producción y Soporte	Producción y Soporte		X		X	X	X	X	X
2	Servidor Java Desarrollo	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte		X				X		
3	Servidor BD Desarrollo	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte		X				X		
4	Servidor Linux Desarrollo	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte		X				X		
5	Impresora (3)	HWD		X		X				Área de desarrollo	Jefe Desarrollo Analistas programadores	Producción y Soporte	Producción y Soporte			X	X	X	X	X	X

-

Tabla N° 16. Inventario de activos de Servicios del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Internet	SD		X		X				Sala de servidores	Personal	Producción y Soporte	Producción y Soporte			X	X		X		

Tabla N° 17. Inventario de personal del Área de Desarrollo

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Proyectos	Atención requerimientos	Desarrollo y Cambios	Testeo y certificación	Mantenimiento
1	Jefe de TI	CD												X			X	X			
	Jefe de Desarrollo (1)	CD												X				X	X	X	
	Analistas programadores Senior (2)	CD												X				X	X	X	X
	Analistas programadores Junior (2)	CD												X				X	X	X	X
	Practicante de Desarrollo (2)	CD														X					

Tabla N° 18. Inventario de activos de Información del Área de Producción y Soporte de TI

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Procedimientos y reglamentos de Producción y Soporte	IPS		X		X				Carpeta de Documentos de gestión	Personal TI Personal empresa	Jefe TI	Jefe TI		X		X	X	X	X	X
2	Planes de desarrollo (Actividades, tareas, asignación de trabajo)	IPS		X		X				Carpeta de proyectos	Personal TI	Jefe TI	Jefe TI		X		X				X
3	Plan de Mantenimiento preventivo	IPS		X			X			Carpeta de proyectos	Personal TI Responsable de Soporte	Jefe TI	Jefe TI		X		X				X
4	Registro de incidentes y problemas	IPS	X			X				Carpeta de Documentos de gestión	Servis Desk	Servis Desk	Oficial de seguridad			X	X			X	
5	Hojas de requerimientos y cambios aprobadas	IPS	X						X	Carpeta de Documentos de gestión	Gestor BD Gestor Networking	Gestor Networking	Gestor Networking	X			X		X		
6	Registro de usuarios	IPS	X						X	Carpeta de Documentos de gestión	Gestor BD Gestor	Gestor BD	Gestor BD		X			X			
7	Perfiles de usuario	IPS		X					X	Carpeta Control de Cambios	Gestor BD Gestor	Gestor BD	Jefe TI	X			X	X	X		
8	Estructura de base de datos	IPS	X						X	Carpeta Control de Cambios	Gestor BD	Gestor BD	Jefe TI		X				X		

9	Bitácora de accesos	IPS	X			X				Carpeta de Documentos de gestión	Gestor BD	Gestor BD	Oficial de seguridad		X				X		
10	Informes de las pruebas de testeo y certificación	IPS		X					X	Carpeta de Documentos de gestión	Gestor BD Gestor Networking	Jefe Producción	Gestor Networking		X		X		X		
11	Configuración de equipos	IPS	X					X		Carpeta Control de Cambios	Gestor Networking	Jefe Producción	Gestor Networking	X			X				
12	Inventario de HW y SW	IPS	X					X		Carpeta Control de Cambios	Responsable de Soporte	Jefe Producción	Jefe TI	X			X				X
13	Información de respaldos y copias de seguridad	IPS	X				X			Carpeta de Documentos de gestión	Gestor BD	Jefe Producción	Jefe TI			X	X		X		
14	Documentación del personal (HV)	IPS			X				X	Carpeta de Documentos de gestión	Administración Jefe de RRHH Jefe TI	Jefe RRHH	Jefe RRHH			X	X				

Tabla N° 19. Inventario de activos de Software del Área de Producción y Soporte de TI

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Drupal	SWP		X					X	Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X			X				
2	Cristal Report	SWP		X		X				PCs	Gestor BD	Producción y Soporte	Producción y Soporte		X		X				
3	Oracle BD	SWP		X		X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X					X		
4	DB2	SWP		X		X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X					X		
5	MySQL	SWP		X		X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X					X		
6	Activate Directory	SWP	X			X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X				X	X		
7	MS Office	SWP		X		X				PCs	Personal TI	Producción y Soporte	Producción y Soporte		X		X	X	X	X	X
8	Aplicativo Virtualización	SWP		X		X				Servidor	Gestor Networking	Producción y Soporte	Producción y Soporte	X			X				
9	Aplicativo – Bitácora	SWP	X			X				Servidor	Gestor BD	Producción y Soporte	Producción y Soporte	X			X	X	X		
10	Aplicativo – Control de cambios	SWP	X			X				Servidor	Gestor Networking Gestor BD	Producción y Soporte	Producción y Soporte	X			X		X		
11	Sistema operativo	SWP		X		X				Servidor	Gestor Networking	Producción y Soporte	Producción y Soporte	X			X				

Tabla N° 20. Inventario de activos de Hardware del Área de Producción y Soporte de TI

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	PC (5)	HWP		X		X				Área de Producción	Personal Producción y Soporte	Jefe de Producción	Jefe de Producción		X		X	X	X	X	X
2	Servidor Aplicaciones	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X		X		
3	Servidor BD (2)	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X	X	X		
4	Servidor de Dominio	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
5	Servidor Web	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
6	Servidor Antimalware	HWP		X		X				Sala de servidores	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
7	Switch Core	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
8	Switch troncales (7)	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking	X			X				
9	Switch de borde (11)	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking		X		X				
10	Router	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking				X				
11	Servidor Pruebas	HWP		X					X	Área de Producción	Usuarios TI	Gestor Networking	Gestor Networking		X		X		X		
12	Impresora (3)	HWP		X		X				Área de Producción	Personal Producción y Soporte	Jefe de Producción	Jefe de Producción			X	X	X	X	X	X

Tabla N° 21. Inventario de activos de Servicios del Área de Producción y Soporte de TI

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Internet	SP		X		X				Sala de servidores	Personal	Gestor Networking	Jefe de Producción y Soporte			X	X		X		
2	VPN	SP		X		X				Sala de servidores	Personal	Gestor Networking	Jefe de Producción y Soporte			X	X		X		

Tabla N° 22. Inventario de personal del Área de Producción y Soporte de TI

Ítem	Denominación del activo	Tipo	Clasificación			Frecuencia de uso				Ubicación Física/Lógica	Usuario	Custodio	Responsable	Valoración			Procesos relacionados				
			Uso Confidencial	Uso interno	Uso Público	Uso Diario	Uso Mensual	Uso Anual	Otro					Alto	Medio	Bajo	Gestión de Infraestructura	Gestión de usuarios	Gestión de BD	Gestión de incidentes	Mantenimiento
1	Jefe de Producción y Soporte	CP												X			X	X	X	X	
2	Gestor Networking	CP												X			X			X	
3	Gestor de BD	CP												X				X	X		
4	Técnico de soporte técnico (8)	CP												X						X	X
5	Practicante de Desarrollo (6)	CP														X					

c. Identificación de brechas de seguridad de la información

Esta tarea consistió en realizar un análisis de cumplimiento de las buenas prácticas definidas en la ISO/IEC 27002, con la finalidad de determinar las brechas existentes actualmente en relación a la seguridad de la información.

Este análisis formó parte de la definición del alcance del SGSI y para determinar cuáles son los dominios de seguridad y los objetivos de control que serán considerados en la propuesta (Nivel de aplicabilidad SOA).

Para desarrollar la tarea se tuvo como insumo los resultados del levantamiento de información que se realizó para identificar los las acciones que actualmente está realizando la empresa para proteger los activos de información. Los objetivos de control que no fueron considerados en el análisis se deben a que la empresa los considera como parte de su seguridad de la información.

A continuación, se muestran los resultados del análisis de aplicabilidad:

Tabla N° 23. Definición del alcance de aplicabilidad de los controles de acuerdo a la ISO/IEC 27002

Ítem	Objetivo de control establecido por la norma ISO 27002	Control definido para el logro del objetivo de control	Verificación del cumplimiento del control	Grado de cumplimiento del control
5. Establecimiento de la política de seguridad de la información				
5.1	**Definición, aprobación, documentación, publicación y difusión de la política de seguridad de la información**			
5.1.1	Elaboración de un documento de políticas de seguridad de la información	La política de seguridad de la información debe ser aprobada por la Dirección; así como publicada y difundida para el conocimiento de los empleados	SI	50%
5.1.2	Revisión planificada y periódica de las políticas de seguridad de la información	La Dirección a quien corresponda, debe revisar la efectividad de las políticas de seguridad de la información, en los tiempos establecidos. Del mismo modo, cuando la empresa realice cambios en sus procesos, normativas, tecnología, etc. se debe revisar de manera planificada los cambios necesarios en la política de seguridad de la información.	NO	
6. Estructura organizativa de la seguridad de la información				
6.1	**Mecanismos de organización interna de la seguridad de la información**			
6.1.1	Establecimiento del compromiso con la seguridad de la información por parte de la Dirección	El compromiso de la Dirección en relación a la seguridad de la información debe evidenciarse a través de la declaratoria de este compromiso y en acciones evidenciables, como: asignación de presupuestos, definición de roles y funciones, definición de una estructura organizativa, capacitación, etc.	SI	60%
6.1.2	Coordinación del trabajo en relación a la seguridad de la información	Debe evidenciarse la definición de mecanismos de coordinación para tratar los temas y acciones de seguridad de la información, según las funciones que cumplen los responsables.	NO	
6.1.3	Identificación, definición y asignación de funciones sobre la seguridad de la información	Debe definirse las funciones para cada uno de los roles responsables de seguridad de la información, las cuales deberán estar expresamente aprobadas, documentadas y difundidas	NO	
6.1.4	Procedimiento para autorizar los permisos y privilegios de uso y tratamiento de la información	Debe diseñarse, documentarse y aprobar un procedimiento que establezca el flujo de autorización de los permisos y privilegios de uso y tratamiento de la información.	NO	
6.1.5	Establecimiento de acuerdos de confidencialidad de la información con los trabajadores	Se debe establecer e implementar acuerdos de confidencialidad de la información con cada trabajador de acuerdo a la función que cumple, las mismas que debe ser revisadas en tiempos definidos.	NO	

6.1.6	Mecanismos de comunicación y coordinación con autoridades	Se debe establecer formas de comunicación y coordinación con los responsables de la seguridad de la información.	NO	
6.1.7	Mecanismos de comunicación y coordinación con grupos de interés	Se debe establecer formas de comunicación y coordinación con grupos de interés internos o externos en relación a la seguridad de la información	NO	
6.1.8	Realización de revisiones de la seguridad de la información	Se debe planificar revisiones del sistema de seguridad de la información en forma periódica, a través de auditorías internas o externas	NO	
6.2	**Seguridad relacionada con los permisos de acceso a terceros**			
6.2.1	Identificación de riesgos de acceso a los recursos de información por parte de terceros	Debe considerarse como parte de la gestión de riesgos los escenarios de riesgos que provienen de los accesos a la información o a los dispositivos de tratamiento de la información que se le asignan a terceros, para identificar los niveles de exposición y definir los controles.	NO	
6.2.2	Condiciones de seguridad de la información en contratos con los clientes	Cuando se realicen contratos con los clientes sobre los servicios brindados o productos ofertados, debe establecerse cláusulas específicas sobre al acceso a la información en caso sea necesario.	NO	
6.2.3	Condiciones de seguridad de la información en contratos con terceros	Cuando se realicen contratos con terceros, en los cuales se tenga que compartir información o acceder a recursos de tratamiento de información, se debe contemplar cláusulas específicas sobre seguridad de la información para establecer las condiciones de uso y tratamiento de la información. Se debe asegurar posteriores malentendidos entre las partes. También debe establecerse las acciones sancionadoras y legales; así como compensaciones en caso de incumplimientos.	NO	
7. Condiciones de seguridad de la información en la gestión de activos				
7.1	**Asignación de responsabilidades sobre los activos**			
7.1.1	Elaboración del inventario o catálogo de activos tecnológicos y de recursos de información.	Los activos de TI deben estar identificados y catalogados en un inventario, donde se identifique las características más importantes y los responsables de los mismos. Del mismo modo, la información, en cualquiera de sus formas, debe ser catalogada, según su nivel de uso.	SI	80%
7.1.2	Definición y asignación de responsabilidades y propietarios de los activos tecnológicos	La organización debe definir y asignar responsabilidades de propiedad, uso, protección, mantenimiento, etc., de cada uno de los activos de TI	NO	

7.1.3	Uso aceptable de los activos tecnológicos	Se debe establecer directrices, reglamentos operativos y procedimientos para el uso y tratamiento aceptable de la información y los recursos de tratamiento de la información.	SI	70%
7.2	**Clasificación de la información**			
7.2.1	Directivas para la clasificación de la información	Debe elaborarse directivas para que las diferentes áreas clasifiquen la información en base al valor que tiene, criticidad y uso legal.	NO	
7.2.2	Lineamientos para identificar, etiquetar y manejar la información	De acuerdo a la clasificación que se le dé a la información, se debe establecer formas de identificación y procedimientos para su protección y uso.	NO	
8. Consideraciones de seguridad de la información en relación a la gestión de los recursos humanos				
8.1	**Consideraciones de seguridad de la información antes de la contratación del nuevo personal**			
8.1.1	Definición de funciones específicas y responsabilidades en el control	La organización debe tener claramente definida y documentada, las funciones y responsabilidades en materia de seguridad de la información que se le asignarán a los empleados en cada puesto de trabajo, así como al personal que pertenece a contratistas terceros.	NO	
8.1.2	Verificación de la información de las personas antes del contrato	Debe evidenciarse que se revisan los antecedentes legales, profesionales, éticos de las personas que están siendo evaluadas para contratación.	SI	80%
8.1.3	Definición de las condiciones y obligaciones laborales en relación a la seguridad de la información.	Los contratos con nuevos empleados, terceros contratistas y usuarios deben contemplar cláusulas específicas en materia de seguridad de la información en donde se establezcan las formas y condiciones de uso de la información y los recursos para su tratamiento.	SI	80%
8.2	**Consideraciones de seguridad de la información durante el desempeño de funciones del personal**			
8.2.1	Verificación del cumplimiento de las obligaciones y responsabilidades	Debe evidenciarse acciones que realizan los responsables de la seguridad de la información para verificar el cumplimiento de las políticas, normativas y procedimientos de seguridad de la información por parte del personal, contratistas y usuarios de partes terceras.	NO	
8.2.2	Acciones de entrenamiento, formación, educación de los empleados para asegurar la concienciación en materia de seguridad de la información	Debe evidenciarse que se ha planificado, ejecutado y evaluado los resultados de los procesos de entrenamiento, formación y educación en relación a las políticas, procedimientos y normativas de seguridad de la información de la organización.	NO	

8.2.3	Definición de procesos y acciones disciplinarias	Se debe establecer con claridad los procesos y acciones disciplinarias en caso de incumplimiento de las políticas, procedimientos y normativas en materia de seguridad de la información.	NO	
8.3	**Consideraciones de seguridad de la información cuando existe cese o fin de un contrato o cambio de funciones del personal**			
8.3.1	Responsabilidades en la terminación del contrato	Debe estar claramente definidas las obligaciones y responsabilidades, tanto del empleado que cesa o termina su contrato, como del empleado que cambia de funciones o puesto de trabajo, en materia de seguridad de la información.	NO	
8.3.2	Devolución/restitución de activos tecnológicos	Debe estar establecido el procedimiento para la devolución de los recursos tecnológicos; así como de la información que le fue asignado a un empleado, contratista o usuario tercero para la ejecución de su trabajo durante su contrato.	NO	
8.3.3	Procedimiento para la eliminación de permisos sobre los activos	Debe estar debidamente establecido y documentado el procedimiento para la eliminación de los privilegios de acceso a la información y recursos de tratamiento de la información en forma oportuna, cuando un empleado, contratista o usuario de una parte tercera, cesa sus funciones o termina su contrato	NO	
9. Mecanismos de seguridad física y del entorno				
9.1	**Identificación y definición de las áreas seguras o de acceso restringido**			
9.1.1	Definición y determinación de perímetros de seguridad física	Las áreas que hayan sido identificadas como de acceso restringido o seguras porque contienen información sensible y/o recursos de tratamiento de la información críticos, debe contar con mecanismos de protección para fijar perímetros de seguridad, como: puertas controladas, muros o barreras de protección, cámaras de vigilancia, etc.	SI	60%
9.1.2	Implementación de controles para el acceso físicos de personas a las áreas seguras o de acceso restringido	Debe implementarse mecanismos de seguridad para controlar el acceso físico del personal autorizado a las áreas seguras o de acceso restringido	SI	50%
9.1.3	Protección de las oficinas, ambientes de trabajo o instalaciones	Debe implementarse mecanismos de seguridad para proteger los recursos y áreas de trabajo, como oficinas, salas de reuniones, despachos, etc.	SI	60%
9.1.4	Implementación de mecanismos de protección ante amenazas ambientales y externas	Debe implementarse mecanismos de seguridad para proteger a las personas, activos de información y recursos tecnológicos de incidentes como desastres naturales o sismos, incendios, inundaciones, explosiones, huelgas, etc.	SI	75%
9.1.5	Definición de lineamientos para el trabajo en áreas restringidas	Se establecerse formas y condiciones de trabajo en las áreas restringidas, de manera clara y documentada.	SI	60%

9.1.6	Implementación de mecanismos de control de acceso en áreas para el público, recepción o áreas de carga	Se debe implementar mecanismos de control para evitar accesos físicos no autorizados a través de las áreas para atención al público, o en las zonas donde se recibe o se despacha envíos	NO	
9.2	**Seguridad del equipamiento tecnológico**			
9.2.1	Protección de los equipos tecnológicos en zonas seguras	Se debe identificar zonas seguras para la ubicación de los equipos tecnológicos para evitar riesgos relacionados con accesos no autorizados, robos, sustracciones, manipulación no autorizada, etc.	SI	70%
9.2.2	Protección en el suministro de energía eléctrica	Se debe implementar mecanismos de protección contra fallas en el abastecimiento del suministro eléctrico, como sobrecargas, cortocircuitos, interrupciones del fluido eléctrico.	NO	
9.2.3	Protección en el cableado eléctrico y de datos	Se debe implementar mecanismos de protección del cableado eléctrico y de datos para protegerlos de interrupciones por manipulación intensional o no intensional, interceptaciones	SI	80%
9.2.4	Planificación del mantenimiento de los equipos tecnológicos	Debe elaborarse y ejecutarse un plan de mantenimiento preventivo de los equipos tecnológicos para asegurar su correcto funcionamiento	SI	80%
9.2.5	Definición de medidas para proteger los equipos fuera de las áreas seguras	Se debe establecer medidas para su uso fuera de las áreas seguras o de la organización.	SI	55%
9.2.6	Procedimientos de destrucción y de reutilización de equipos tecnológicos	Debe definirse procedimientos documentados para la eliminación de la información de los equipos tecnológicos que serán dados de baja o reutilizados en otras tareas.	NO	
9.2.7	Medidas para la salida y traslado de activos de TI fuera de la organización	Se debe establecer medidas para el registro controlado de la salida y traslado de activos de TI (información, equipos, software) fuera de las áreas seguras o de la organización.	NO	
10. Consideraciones de seguridad de la información en la gestión de las comunicaciones y las operaciones				
10.1	**Mecanismos de seguridad en los procedimientos operativos**			
10.1.1	Elaboración de procedimientos operacionales documentados	Se debe elaborar documentos que describa el flujo de trabajo de los procedimientos operativos, los mismos que deben ser difundidos y conocidos por todo el personal.	SI	30%
10.1.2	Mecanismos de control de los cambios	Se debe implementar mecanismos de registro y seguimiento de los cambios que se realicen en los recursos tecnológicos y en las aplicaciones que gestionan la información.	NO	

10.1.3	Identificación de las funciones y tareas que deberán ser segregadas	Se debe analizar e identificarlas funciones y tareas que deberán ser segregadas para evitar o disminuir las posibilidades de acciones no autorizadas en el tratamiento de la información o mal uso de los activos de información.	NO	
10.1.4	Separación de las áreas de trabajo para el desarrollo de sistemas, desarrollo de pruebas y producción	Las áreas de trabajo donde se realizan las labores de desarrollo de software, pruebas y producción de las mismas, deberán estar separadas para evitar accesos no autorizados o manipulación de los recursos de información de manera no autorizada.	SI	70%
10.2	**Mecanismos de seguridad en la provisión de servicios de terceros**			
10.2.1	Entrega de los servicios contratados con terceros	Se debe definir las formas de entrega de los servicios por parte de terceros; así como los niveles de entrega, implantándose controles para el seguimiento del cumplimiento de los mismos.	NO	
10.2.2	Revisión y seguimiento de los servicios contratados con terceros	Se debe revisar los controles de seguimiento del cumplimiento de los servicios entregados por terceros y los niveles entregados, a través de informes, registros de seguimiento y auditorías de manera regular.	NO	
10.2.3	Mecanismos de control de los cambios en los servicios contratados con terceros	Debe implementarse controles que permitan comunicar, registrar y hacer seguimiento a los cambios realizados en los servicios entregados por terceros, incluyendo acciones de mantenimiento y la mejoras, con la finalidad de evaluar los riesgos asociados a los cambios.	NO	
10.3	**Planificación y definición de criterios para la aceptación de sistemas antes de su puesta en producción**			
10.3.1	Evaluación de las capacidades	Se debe implementar mecanismos de evaluación permanente del comportamiento de los recursos consumidos por los sistemas para determinar sus capacidades actuales y realizar proyecciones que permitan asegurar las capacidades necesarias en el futuro.	NO	
10.3.2	Evaluación de los sistemas antes de su puesta en producción	Debe establecerse criterios para la aceptación de las modificaciones realizadas en los sistemas en producción, nuevas versiones o nuevos sistemas antes de ponerlos en producción, estableciendo los procedimientos para realizar su evaluación.	NO	
10.4	**Mecanismos de protección contra malware**			
10.4.1	Procedimientos para la gestión de código malicioso	Debe implementarse procedimientos para detectar y prevenir la utilización de código malicioso por parte de los usuarios; así como, para recuperar los estados correctos de la información.	SI	90%
10.4.2	Controles contra código móvil	Se debe implantar mecanismos para detectar o evitar el uso de aplicaciones móviles no autorizadas dentro de los ambientes de la organización.	NO	

10.5	**Mecanismos para la generación de respaldos de la información y aplicaciones**			
10.5.1	Generación de copias de respaldo de la información y aplicaciones	Se debe establecer procedimientos operativos para la generación de las copias de seguridad de la información y las aplicaciones, estableciendo frecuencias, responsabilidades, formas de etiquetado, ambientes de custodia, traslado; las cuales deben ser evaluadas o comprobadas con regularidad.	SI	90%
10.6	**Mecanismos de seguridad en la gestión de la red de computadoras**			
10.6.1	Implementación de mecanismos de monitoreo de amenazas en la red de computadoras	Debe implementarse mecanismos de monitoreo permanente, ya sea por software o hardware, para identificar potenciales amenazas sobre las aplicaciones y sistemas que se gestionan a través de la red; así como sobre la información que circula sobre ella.	NO	
10.6.2	Seguridad de los servicios de red	Todos los servicios implementados sobre la red de computadoras por la organización o a través de contrato con terceros, deben ser monitoreados y controlados, para asegurar los niveles de servicio o detectar eventos fo autorizados o fuera de los parámetros establecidos.	NO	
10.7	**Utilización de los soportes de información**			
10.7.1	Gestión de los recursos o medios removibles	Debe gestionarse mecanismos de control para asegurar la utilización correcta y autorizada de recursos o medios removibles.	NO	
10.7.2	Procedimientos para la destrucción o eliminación de medios removibles de soporte de información	Debe establecerse procedimientos para asegurar que los medios removibles que fueron utilizados como soporte secundario de la información y que se les da de baja, sean destruidos, eliminando previamente y de manera segura, la información que contenía.	NO	
10.7.3	Procedimientos el tratamiento y el almacenamiento de la información	Debe establecerse procedimientos para asegurar que el tratamiento y el almacenamiento de la información sea correcta y segura, evitando mal uso, fuga o revelación no autorizada de la información.	NO	
10.7.4	Mecanismos de protección de la documentación técnica de los sistemas	Debe establecerse controles para la elaboración, realización de cambios, difusión y almacenamiento de documentación técnica de los sistemas, para evitar mal uso, robo o divulgación no autorizada.	NO	
10.8	**Medidas de seguridad para el intercambio de información**			

10.8.1	Definición de procedimientos para la seguridad en el intercambio de información	Debe implementarse políticas y procedimientos para proteger el intercambio de información a través de los medios de comunicación.	NO	
10.8.2	Condiciones para el intercambio de información	Debe definirse las condiciones para el aseguramiento de la información en los acuerdos de intercambio de información y de software entre las partes.	NO	
10.8.3	Medidas de protección de los medios físicos que contienen información cuando son movilizados	Debe establecerse medidas de protección para los dispositivos o recursos físicos que contienen información cuando se trasladan fuera de los ambientes de la organización.	NO	
10.8.4	Medidas de seguridad en el uso de mensajes electrónicos	Debe establecerse medidas que aseguren el correcto envío y recepción de mensajes electrónicos.	NO	
10.8.5	Protección de los sistemas de información interconectados entre negocios	Debe implementarse mecanismos de seguridad para asegurar que el intercambio de información a través de aplicaciones o sistemas de información con otras organizaciones sea seguro.	NO	
10.9	**Protección de los servicios o aplicaciones de negocio electrónico**			
10.9.1	Protección de las aplicaciones de comercio electrónico	Debe implementarse sistemas de protección de la información que circula a través de las aplicaciones de comercio electrónico que utilizan redes públicas, con l finalidad de evitar actividades fraudulentas, revelación o modificación de la información.	NO	
10.9.2	Protección de las transacciones realizadas en línea	Debe implementarse mecanismos para asegurar que la información transmitida en transacciones en línea no llegue incompleta, o sea revelada, modificada o copiada de manera no autorizada, o llegue a destinos no correctos.	NO	
10.9.3	Protección de la información pública	Debe implementarse mecanismos que aseguren que la información que se difunde de manera pública no sea modificada sin autorización, esté siempre disponible.	NO	
10.10	**Acciones de monitoreo y seguimiento de actividades**			
10.10.1	Generación de bitácoras o registros de auditoría	Todas las actividades realizadas por los usuarios de TI deben ser registradas desde su logueo para realizar el seguimiento o investigaciones futuras en registros de auditoría y mantenidas durante periodos previamente definidos. También deben registrarse las excepciones y las incidencias con la información.	NO	
10.10.2	Monitoreo del uso de los recursos de tratamiento de la información	Debe definirse procedimientos formales para realizar el monitoreo del uso de los recursos de tratamiento de la información, los cuales deben ser revisados periódicamente.	NO	

10.10.3	Protección de registros de auditoría, monitoreo y bitácoras	Debe implementarse mecanismos de protección de los registros de auditoría, monitoreo y bitácoras para evitar accesos no autorizados y mala manipulación.	NO	
10.10.4	Monitoreo de las actividades de los administradores y operadores de los sistemas	Debe generarse registros automáticos de las actividades que realizan los administradores y operados de la base de datos, red, dominios, etc. para investigaciones futuras.	NO	
10.10.5	Registro de errores, fallas o caídas en los sistemas	Todo incidente de falla, error o caída de algún sistema físico o lógico debe ser registrado, posteriormente analizado, investigado para realizar las mejoras necesarias.	NO	
10.10.6	Sincronización de los relojes de los sistemas	Debe asegurarse que existe sincronía entre los relojes de los diferentes sistemas y aplicaciones para asegurar la precisión de tiempo en la realización de las transacciones.	NO	
11. Consideraciones de seguridad de la información en el control de accesos				
11.1	**Política para control de acceso**			
11.1.1	Control de acceso a los recursos de tratamiento de información y a los activos de información	La organización debe tener una política general que establezca y precise las condiciones para establecer el control de acceso a los recursos de tratamiento de información y a los activos de información.	SI	90%
11.2	**Gestión de acceso de los usuarios**			
11.2.1	Identificación de usuarios para los accesos	Debe definirse los procedimientos formales para la asignación, modificación y retiro de código de identificación de los usuarios y su contraseña de acceso a los recursos de tratamiento de información y a los activos de información.	SI	100%
11.2.2	Administración de los perfiles de usuario y privilegios de acceso	Debe definirse un catálogo de perfiles de usuario, estableciendo para cada caso los privilegios de acceso a la información y a los recursos de tratamiento de información.	SI	90%
11.2.3	Administración de las claves de acceso o contraseñas de usuario	Debe definirse un procedimiento para la generación y cambio de las claves de acceso o contraseñas de usuario.	SI	90%
11.2.4	Revisión de los permisos perfiles de usuario y privilegios de acceso	Debe planificarse revisiones periódicas de los perfiles de usuario y privilegios de acceso.	SI	75%
11.3	**Control de las responsabilidades asignadas a los usuarios**			
11.3.1	Uso de las contraseñas	Debe realizarse actividades de concientización a los usuarios en buenas prácticas para el cumplimiento de los controles de uso y cambio de sus claves o contraseñas de acceso.	SI	100%

11.3.2	Equipos desatendidos	Debe realizarse actividades de concientización a los usuarios en buenas prácticas para asegurar la información cuando tienen sus equipos desatendidos (cuando no lo están utilizando).	SI	50%
11.3.3	Política de escritorios y pantallas limpias	Debe realizarse actividades de concientización a los usuarios en buenas prácticas para mantener su puesto de trabajo limpio de papeles y para mantener "pantalla limpia" de los recursos de tratamiento de la información cuando no lo están utilizando.	SI	40%
11.4	**Medidas para controlar el acceso a la red**			
11.4.1	Medidas de seguridad para el uso de los servicios de la red	Debe definirse los servicios de la red de datos a los que tiene acceso cada usuario, según su perfil de usuario.	SI	80%
11.4.2	Identificación y autenticación de los usuarios en acceso remotos	Debe implementarse métodos para identificar y autenticar a los usuarios cuando acceden a los activos de información o recursos de tratamiento de información de manera remota.	NO	
11.4.3	Identificación y autenticación de equipos conectados a la red	Debe implementarse métodos para identificar y autenticar automáticamente los equipos cuando se conectan a la red, ya sea por su posición y por identificación de un equipo específico.	SI	100%
11.4.4	Mecanismos para la protección de los puertos	Debe implementarse métodos para configurar el acceso físico y lógico a través de los puertos de la red; y su correspondiente monitoreo.	NO	
11.4.5	Segregación de la red en grupos	Para mejorar la seguridad en la red en relación a los accesos a la información y recursos de tratamiento de información, se debe segregar la red en grupos de servicios de información, usuarios según su función o sistemas de información.	SI	70%
11.4.6	Control de acceso de los usuarios a la red	El acceso a la información y a los recursos de tratamiento de la información dentro de la red, debe estar definido para cada usuario.	NO	
11.4.7	Control del direccionamiento en la red	Debe asegurarse que los enrutamientos a la información y recursos de tratamiento de la información dentro de la red, estén debidamente asignados para evitar accesos o autorizados.	NO	
11.5	**Control de acceso a los sistemas operativos**			
11.5.1	Control de inicio de las sesiones en las estaciones de trabajo	Se debe controlar el inicio del trabajo en las estaciones de trabajo, estableciendo un procedimiento de acceso al sistema operativo de manera segura.	SI	80%
11.5.2	Procedimiento de identificación del usuario y autenticación de su identidad	Se debe controla el acceso a las estaciones de trabajo identificando al usuario con un identificador único y autenticar su identidad con alguna técnica adecuada.	SI	100%

11.5.3	Gestión de las contraseñas de los usuarios	Debe contarse con mecanismos de administración de las contraseñas de los usuarios para asegurar que se cumplan con las características exigidas y de manera interactiva.	SI	90%
11.5.4	Uso de aplicaciones o utilidades en las estaciones de trabajo	Se debe controlar el uso de aplicaciones o utilidades que permitan al usuario cambiar la configuración de sus estaciones de trabajo o invalidar los controles, restringiendo su instalación o ejecución.	NO	
11.5.5	Desconexión de sesiones por inactividad.	Se debe configurar las estaciones de trabajo para que se desconecten automáticamente cuando se detecte inactividad por un periodo determinado.	NO	
11.5.6	Tiempos definidos de conexión de las estaciones de trabajo	Se debe configurar los tiempos de conexión de las estaciones de trabajo a las aplicaciones o red en base a los horarios de trabajo.	NO	
11.6	**Mecanismos para el control de los accesos a la información y aplicaciones**			
11.6.1	Control de acceso restringido a la información y aplicaciones	El acceso a la información y a las aplicaciones debe ser controlada y restringida de acuerdo a la función que cumple cada usuario en cada estación de trabajo.	NO	
11.6.2	Protección de los sistemas críticos y sensibles	Los sistemas que gestionan información sensible y crítica para la organización deben estar instalados en estaciones de trabajo aislados y deben ser de uso dedicado.	NO	
11.7	**Mecanismos de control para el trabajo mediante computación móvil y teletrabajo**			
11.7.1	Control en el trabajo remoto por aplicaciones móviles	Debe implementarse medidas de seguridad, como procedimientos y planes operativos, para controlar el trabajo que se realiza de manera remota a través de aplicaciones móviles	NO	
11.7.2	Control en el teletrabajo	Debe implementarse medidas de seguridad, como procedimientos y planes operativos, para controlar las actividades de teletrabajo.	NO	
12. Consideraciones de seguridad de la información en el desarrollo de sistemas de información				
12.1	**Implementación de condiciones de seguridad en los sistemas de información**			
12.1.1	Especificaciones de los requisitos de seguridad en los sistemas de información	En el proceso de desarrollo de los sistemas de información debe considerarse el análisis y especificación de requerimientos de seguridad, como control de accesos, identificación de usuarios, niveles de acceso, registros de auditoría, validaciones, etc.	NO	
12.2	**Mecanismos para asegurar el procesamiento correcto en las aplicaciones**			
12.2.1	Ingreso de los datos validados	Los sistemas de información y las aplicaciones deben contar con módulos de validación de los datos que son ingresados.	NO	

12.2.2	Procesamiento correcto de datos	Los sistemas de información y las aplicaciones deben contar con módulos que detecten cualquier error o anomalía en los resultados del procesamiento de los datos, provenientes de acciones mal intencionadas o malos diseños en el sistema.	NO	
12.2.3	Control para asegurar la integridad en la mensajería	Los sistemas de información y las aplicaciones deben contar con módulos que aseguren la autenticidad e integridad de los mensajes que resultan de las aplicaciones.	NO	
12.2.4	Salida de datos validada	Los sistemas de información y las aplicaciones deben contar con módulos que validen las salidas, como reportes y consultas que se realicen para garantizar que los resultados del procesamiento y almacenamiento de datos es correcto.	NO	
12.3	**Mecanismos para la encriptación de los datos**			
12.3.1	Especificaciones para el uso de métodos criptográficos	Se debe definir lineamientos para determinar la información que debe ser encriptada, el momento en qué debe ser encriptada y el método que se utilizará.	NO	
12.3.2	Uso de claves o llaves para la encriptación	En el caso de que se utilice métodos criptográficos, se definir un sistema de administración de las claves o llaves como apoyo al proceso de encriptación.	NO	
12.4	**Mecanismos de seguridad de los archivos de los sistemas**			
12.4.1	Control en la instalación de software	Deben definirse políticas y procedimientos de seguridad para asegurar que solo se instalen aplicaciones autorizadas en los sistemas operativos	NO	
12.4.2	Procedimientos de seguridad con los datos de prueba	La generación de datos de prueba utilizados en el desarrollo de los sistemas, debe ser controlado, a través de procedimientos de generación controlada de los datos	SI	80%
12.4.3	Acceso al código fuente	Debe implementarse medidas que aseguren el acceso controlado a las librerías del código fuente de los sistemas y aplicaciones.	SI	70%
12.5	**Condiciones de seguridad en el desarrollo de software**			
12.5.1	Control de cambios	Todos los cambios realizados en el código fuente, estructuras de datos y documentación técnica durante el proceso de desarrollo de software debe ser controlado, a través del registro de los cambios	SI	70%
12.5.2	Revisión de los cambios en los sistemas antes de puesta en producción	Debe implementarse procedimientos de prueba de los cambios realizados en los sistemas antes de su puesta en producción, para verificar su integridad y correcta funcionalidad.	SI	90%

12.5.3	Restricciones en cambios de los sistemas	Debe asegurarse que los cambios realizados en los sistemas correspondan únicamente a los solicitados y autorizados.	SI	90%
12.5.4	Control para la salida no autorizada de información de los sistemas	Debe implementarse mecanismos de control para evitar la salida no autorizada de información relacionada a los sistemas de información, como: código fuente, datos, base de datos, manuales, documentación técnica, etc.	NO	
12.5.5	Control del desarrollo de software tercerizado	Cuando el desarrollo de software es tercerizado debe implementarse mecanismos de monitoreo y seguimiento del proceso.	NO	
12.6	**Gestión de vulnerabilidades técnicas**			
12.6.1	Gestión de las vulnerabilidades relacionadas con el soporte tecnológico de las aplicaciones	Durante el proceso de desarrollo de software se debe analizar e identificar las vulnerabilidades que pueda tener el soporte tecnológico de los sistemas, para implementar las salvaguardas o controles necesarios.	NO	
13. Medidas de seguridad de la información en la gestión de incidentes				
13.1	**Procedimiento de comunicación y registro de incidentes o eventos**			
13.1.1	Canales de comunicación para el reporte de incidentes de seguridad de la información	Debe definirse los canales de comunicación que se utilizarán para reportar, comunicar y registrar los incidentes de seguridad oportunamente	NO	
13.1.2	Reporte de debilidades de seguridad	Cualquier indicio o sospecha de debilidades en alguno de los sistemas o aplicaciones debe ser oportunamente informado y registrado por el personal que lo detecte, como personal de la empresa, contratistas o personal de terceros.	NO	
13.2	**Proceso de la gestión de los incidentes de seguridad de la información**			
13.2.1	Responsabilidades y procedimientos	Se debe implementar un sistema de gestión de incidentes en las que se defina roles, responsabilidades y los procedimientos para la atención oportuna y efectiva de los incidentes de seguridad de la información reportados.	SI	70%
13.2.2	Base de datos de conocimiento	La gestión de incidentes debe generar información que sea debidamente registrada en una base de datos de conocimiento para mejorar los procedimientos, tiempos de atención o la investigación de los incidentes.	NO	
13.2.3	Investigación de los incidentes	Se debe considerar procesos de investigación de los incidentes de seguridad, como parte de la gestión de incidentes, recopilando las pruebas necesarias para su análisis y seguimiento.	NO	
14. Medidas de seguridad de la información para la continuidad del negocio				

14.1	**Condiciones de seguridad de la información para asegurar la continuidad del negocio**			
14.1.1	Sistema de continuidad del negocio	Se debe incorporar como parte de la seguridad de la información un sistema de continuidad del negocio que asegure la activación de procesos de gestión de crisis y vuelta a la normalidad, definiendo los roles, funciones y procedimientos.	NO	
14.1.2	Análisis de impacto en el negocio	El sistema de continuidad, debe contemplar la identificación de los eventos que pueden ocasionar interrupciones en los procesos o servicios, evaluando el impacto sobre el negocio: económica, reputacional, operativa, etc.	NO	
14.1.3	Plan de gestión de crisis y de vuelta a la normalidad	El sistema de continuidad debe contener planes que permitan reaccionar oportunamente frente a una crisis ocasionada por algún evento imprevisto; así como la activación de otros planes que permitan volver a la normalidad de operación.	NO	
14.1.4	Marco de referencia para la continuidad del negocio	El sistema de continuidad de negocio; así como los planes que incluye, deben ser implementados en base a estándares o marcos de referencia aceptados que aseguren el cumplimiento de los requisitos de seguridad de la información.	NO	
14.1.5	Plan de pruebas de los controles y actividades del sistema de continuidad del negocio	Los controles y actividades definidas en el sistema de continuidad del negocio deben ser revisadas periódicamente y de manera inopinada para constatar su correcto funcionamiento en los tiempos de respuesta establecidos.	NO	
15. Condiciones para el cumplimiento y conformidad normativa				
15.1	**Acatamiento de los aspectos legales**			
15.1.1	Identificación de la normativa legal vigente	La organización debe identificar todo el contexto normativo, interno y externo, bajo el cual se desenvuelve el negocio para asegurar su cumplimiento durante la prestación de los servicios o en las responsabilidades y obligaciones contractuales.	NO	
15.1.2	Cumplimiento de la normativa relacionada a la propiedad intelectual y los derechos de autor	El proceso de desarrollo de software debe considerar el uso adecuado de material de referencia para no incumplir con la normativa vigente, en relación a la propiedad intelectual y los derechos de autor.	NO	
15.1.3	Protección de la documentación sensible de la organización	Se debe tomar medidas para proteger la documentación y los registros relacionados con contratos, reglamentos, planes, etc., de mala manipulación, sustracción, destrucción o falsificaciones.	NO	

15.1.4	Protección de la información personal	La información de las personas naturales o jurídicas; así como su privacidad, deben ser protegidas contra actos no autorizados de uso, divulgación, modificación, etc.	NO	
15.1.5	Control contra el uso no autorizado de los recursos de tratamiento de datos	Debe implementarse mecanismos de control que aseguren o impidan el mal uso no autorizado de los recursos tecnológicos para la manipulación de la información.	NO	
15.1.6	Control del uso de encriptación de datos	La encriptación de los datos sólo debe aplicarse para los casos específicos definidos en las políticas y normativas de la empresa.	NO	
15.2	**Cumplimiento de las políticas y normativas técnicas y de seguridad**			
15.2.1	Cumplimiento de los controles de seguridad de la información	Debe asegurarse que todo el personal de la empresa, contratistas y usuarios terceros cumplan con las condiciones de seguridad de la información establecidas en las políticas, normativas y procedimientos; de acuerdo a las funciones, responsabilidades y obligaciones asignadas.	NO	
15.2.2	Cumplimiento de los controles técnicos	Debe asegurarse que los sistemas de información y recursos de tratamiento de los datos estén ejecutando correctamente los controles técnicos implementados.	NO	
15.3	**Realización de auditorías a los sistemas de información**			
15.3.1	Planificación y prácticas de auditorías a los sistemas de información	Debe planificarse auditorías a los sistemas de información para revisar el cumplimiento de las actividades de control y la efectividad de los controles. Durante la ejecución de las auditorías debe asegurarse que no interrumpa las operaciones.	NO	
15.3.2	Control de acceso a los registros de auditoría de los sistemas de información	Debe implementarse controles para asegurar que el acceso a las bitácoras o registros de auditoría de los sistemas de información lo realice solo el personal autorizado, para evitar eliminaciones, modificaciones o uso indebido.	NO	

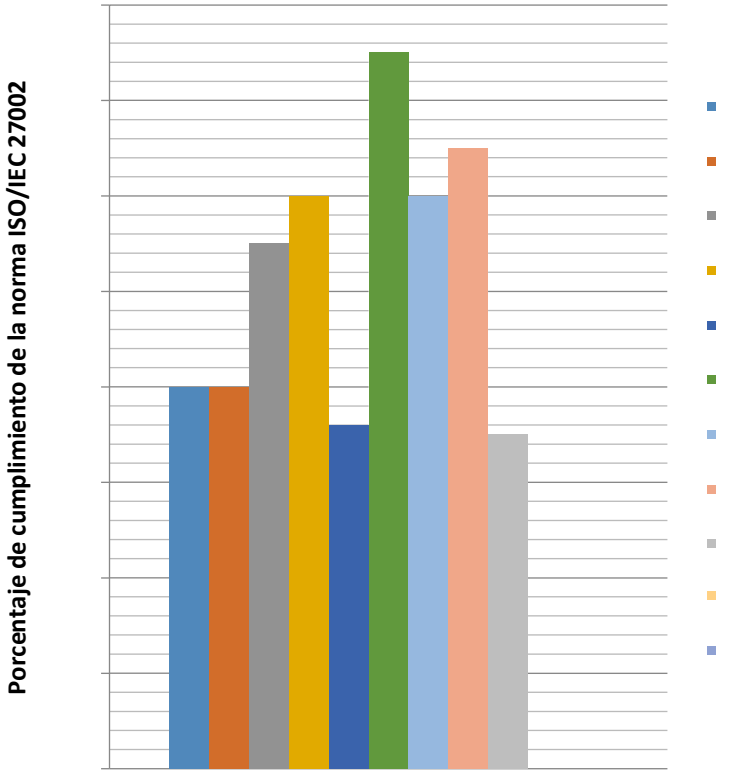

Gráfico N° 12. Porcentajes de cumplimiento de los controles de seguridad de la información, por dominio

Fuente: Elaborado por los investigadores

4.1.3. Fase 3: Análisis y evaluación de los escenarios de riesgos de TI

Para esta fase se aplicó la metodología descrita en el acápite 3.6.3.

Los elementos considerados para este análisis son:

a. Activos. Los activos considerados para el análisis y evaluación de riesgos fueron categorizados de acuerdo a la tabla N° 5.
b. Estimación de la criticidad de los activos de TI. Para esta tarea, se evaluaron las características de aseguramiento de la información (Confidencialidad, Integridad y Disponibilidad) utilizando como referencia la Tabla N° 6. Para esta estimación se aplicó la formula N° 1.
c. Identificación de vulnerabilidades y amenazas. Esta tarea se realizó conjuntamente con el personal de cada una de las áreas de los dos procesos seleccionados en el alcance del SGSI, en

un trabajo colaborativo. Se tomó como referencia la clasificación de las amenazas y vulnerabilidades descrita en el ítem 3.6.3.

d. Estimación del impacto. Se utilizó la escala y criterios de la Tabla N° 7. Esta actividad se realizó en trabajo colaborativo con el personal de cada una de las áreas consideradas en el alcance de la investigación.
e. Estimación de la frecuencia de las amenazas. Se utilizó los niveles de probabilidad de ocurrencia definidos en la Tabla N° 8. Esta actividad se realizó en trabajo colaborativo con el personal de cada una de las áreas incluidas en el alcance de la investigación.
f. Estimación del nivel de exposición al riesgo. Para esta estimación se aplicó la formula N° 3.
g. Determinación del nivel de tolerancia al riesgo. Se aplicó los niveles de riesgo definidos en la Tabla N° 9.

Lo resultados de esta tarea fueron:

Tabla N° 24. Análisis y evaluación de riesgos de TI del Área de Desarrollo – Activos de Información

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Procedimientos y reglamentos de desarrollo	1	3	3	7	No se realizan actualizaciones o revisiones de los procedimientos y reglamentos de manera planificada	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación física y digital relacionada a los procedimientos y normativas de desarrollo, están bajo la custodia del Jefe de Desarrollo. Las normativas y directivas de procedimientos se asignan al personal en base a la función que cumplen. Toda la documentación de procedimientos y normativas tienen copias, resguardadas por el administrador.	5	4	27	NT
							Modificación parcial o total de la información de manera intencional o por error		2	4	8	TT
							Eventos de desastres naturales, industriales o de origen social, como: incendios, terremotos, explosiones, huelgas, etc.		1	4	4	TT
							Pérdida o sustracción de información		3	4	12	TT
2	Planes de desarrollo (Actividades, tareas, asignación de trabajo)	1	1	3	5	No existe documentación sobre metodologías o procesos o estandarización del desarrollo del software. No se lleva el control de versiones. No se lleva el control de cambios.	Sustracción no autorizada y divulgación de documentación sensible por el personal	Se realizan solo reuniones de coordinación para el desarrollo de los proyectos de software. Se firman actas. El custodio de las versiones es el jefe de desarrollo.	2	3	11	TT
							Modificación parcial o total de la información de manera intencional o por error		3	3	9	TT
							Eventos de desastres naturales, industriales o de origen social, como: incendios, terremotos, explosiones, huelgas, etc.		1	3	3	NT
							Pérdida o sustracción de información		3	3	9	TT
3	Cotizaciones y cuadros de evaluación	1	1	2	4	No se ha estandarizado el proceso de cotización de los proyectos de software. Las	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen	2	3	10	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						cotizaciones realizadas forman parte de la documentación del proyecto.	Modificación parcial o total de la información de manera intencional o por error	procedimientos de seguridad para protegerlos	3	2	6	TT
							Eventos de desastres naturales, industriales o de origen social, como: incendios, terremotos, explosiones, huelgas, etc.		1	2	2	NT
							Pérdida o sustracción de información		2	2	4	TT
4	Hojas de requerimientos y cambios aprobadas	2	2	1	5	No existen controles de cambios en los proyectos, por lo que cada desarrollador cumple con la función asignada sin registrar los cambios realizados.	Procesamiento erróneo por parte del personal de Desarrollo	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	4	4	21	RT
							Información no disponible, en desuso u obsoleta		3	3	9	TT
							Modificación parcial o completa de la información, de manera intencional o por error		4	4	16	RT
5	Documentos técnicos de desarrollo (análisis, diseño)	2	2	3	7	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	4	5	27	NT
							Procesamiento erróneo por parte del personal de Desarrollo		4	5	20	RT
							Accesos a los activos de información de manera no autorizada		2	4	8	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						documentación de los proyectos de software No se ha estandarizado el procedimiento de pruebas No existe un procedimiento estandarizado de control de cambios o versiones	Sustracción no autorizada de documentación sensible		3	4	12	TT
							Errores en la ejecución de las pruebas unitarias		4	5	20	RT
							Información no disponible, en desuso u obsoleta		3	3	9	TT
							Modificación parcial o completa de la información, de manera intencional o por error		3	4	12	TT
6	Registros de Control de Cambios (scripts, BD, carga data)	3	3	3	9	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software No se ha estandarizado el procedimiento de pruebas No existe un procedimiento estandarizado de control de cambios o versiones	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	3	4	21	RT
							Procesamiento erróneo por parte del usuario		4	5	20	RT
							Información no disponible, en desuso u obsoleta		2	3	6	TT
							Accesos a los activos de información de manera no autorizada		2	3	6	TT
							Sustracción no autorizada de documentación sensible		2	4	8	TT
							Modificación parcial o completa de la información, de manera intencional o por error		3	3	9	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
7	Manuales de usuario	1	1	2	4	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software No existe un procedimiento estandarizado de control de cambios o versiones	Sustracción no autorizada y divulgación de documentación sensible por el personal	La documentación de los proyectos de software es gestionada por el jefe del proyecto, pero no existen procedimientos de seguridad para protegerlos	5	3	19	RT
							Información no disponible, en desuso u obsoleta		4	3	12	TT
							Accesos a los activos de información de manera no autorizada		3	2	6	TT
							Sustracción no autorizada de documentación sensible		5	3	15	TT
							Modificación parcial o completa de la información, de manera intencional o por error		2	3	6	TT
8	Informes de las pruebas de testeo y certificación	3	3	3	9	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software No se ha estandarizado el procedimiento de pruebas El ambiente para realizar las pruebas no es independiente de la red	Sustracción no autorizada y divulgación de documentación sensible por el personal	Los desarrolladores gestionan la documentación de las pruebas realizadas, pero no existen procedimientos de seguridad para protegerlos	3	4	21	RT
							Procesamiento erróneo por parte del usuario		4	5	20	RT
							Información no disponible, en desuso u obsoleta		2	4	8	TT
							Accesos a los activos de información de manera no autorizada		2	3	6	TT
							Sustracción no autorizada de documentación sensible		3	4	12	TT
							Modificación parcial o completa de la información, de manera intencional o por error		3	3	9	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
9	Documentos de versiones de software	3	3	3	9	No existen acuerdos de confidencialidad con los empleados de la empresa La documentación se elabora bajo ciertos criterios generales porque no existe una metodología aprobada para el desarrollo de software No existe mecanismos que controlen de accesos a la documentación de los proyectos de software	Sustracción no autorizada y divulgación de documentación sensible por el personal	Cuando se cierra un proyecto, toda la documentación se almacena en un armario sin protección bajo la custodia del jefe de Desarrollo	3	4	21	**RT**
							Información no disponible, en desuso u obsoleta		4	3	12	**TT**
							Accesos a los activos de información de manera no autorizada		2	3	6	**TT**
							Sustracción no autorizada de documentación sensible		3	4	12	**TT**
10	Documentación del personal (HV)	1	2	2	5	La actualización y gestión documentación referida al legajo personal de los empleados no está reglamentada. Por tanto, son fácilmente accesibles, muchas veces están desactualizados	Información no disponible, en desuso u obsoleta	La documentación del legajo de los trabajadores y sus contratos las gestiona el administrador de la empresa.	3	2	11	**TT**
							Modificación parcial o completa de la información, de manera intencional o por error		2	4	8	**TT**

Tabla N° 25. Análisis y evaluación de riesgos de TI del Área de Desarrollo – Activos de Software

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas y entornos de desarrollo	1	3	4	8	No se cuenta con procedimientos formalizados, estandarizados y documentados para la solución de incidentes y problemas de configuraciones	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	Se lleva un registro de los errores cometidos en relación a las configuraciones e instalaciones de las herramientas y entornos de desarrollo	2	3	14	TT
						Soporte técnico de las actualizaciones de las herramientas tardía	Aplicativos (tools) de desarrollo de software obsoletas, discontinuadas o no vigentes		2	3	14	TT
						No se cuenta con un procedimiento formalizado, aprobado y documentado para cambios de versiones	Puesta en producción de versiones no autorizadas o no probadas o en desuso		2	4	16	RT
						No existen controles para instalaciones de software	Instalación de aplicativos no autorizados o no licenciados		2	4	16	RT
						Incompatibilidad de las versiones de los nuevos sistemas con el software base en las estaciones	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones		2	5	18	RT
						Cantidad de licencias de software de desarrollo limitada	Indisponibilidad, limitaciones o deficiencias en el software de desarrollo		2	3	14	TT
						Poca experiencia del personal de soporte para resolver problemas de configuraciones o cambios de versiones	Pérdida o eliminación de archivos del entorno de desarrollo		2	3	14	TT
2	Software de ofimática	1	1	4	6	Diferentes versiones instaladas de las aplicaciones	Procedimientos de instalación de software con errores	Se trabaja con software de ofimática descargable y se actualiza con parches	2	2	10	TT
							Infección por malware		2	2	10	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
							Baja performance en el funcionamiento del software de ofimática por falta de mantenimiento		2	2	10	TT
							Baja performance en el funcionamiento del software de ofimática por configuración incorrecta del software		2	2	10	TT
							Daño en los archivos o en su contenido		2	2	10	TT
							Pérdida del software de instalación		2	2	10	TT
							Posibilidad de uso o modificación de la información de manera no autorizada		2	2	10	TT
3	Aplicativos para modelamiento	1	2	3	6	Aplicaciones o herramientas CASE para las fases de análisis y diseño no licenciadas u obsoletas	Procedimientos de instalación de software con errores	Se lleva un registro de los modelamientos desarrollados en carpetas anexadas a cada proyecto	2	1	8	TT
							Infección por malware		2	2	10	TT
							Baja performance en el funcionamiento de las aplicaciones de modelamiento por configuración incorrecta del software por falta de mantenimiento		3	2	12	TT
							Baja performance en el funcionamiento de las aplicaciones de modelamiento por configuración incorrecta del software		3	1	9	TT
							Indisponibilidad, limitaciones o deficiencias en el software de desarrollo		3	1	9	TT
							Pérdida del software de instalación		2	2	10	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
							Posibilidad de uso o modificación de los archivos de modelamiento de manera no autorizada		2	2	10	TT
4	Motores de base de datos	3	4	4	11	No se cuenta con procedimientos formalizados, estandarizados y documentados para la solución de incidentes y problemas de configuraciones	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	Se generan copias de respaldo de la BD periódicamente. El custodio es el Jefe de Desarrollo Se lleva un registro de los errores en los motores de BD	2	5	21	RT
						Sistema antimalware obsoleto	Infección por malware		1	5	16	RT
						No se cuenta con procedimientos ni ambientes dedicados a las pruebas del software antes de puesta en producción	Indisponibilidad o inoperatividad de los sistemas por caída de los motores de base de datos o de los servidores que los administran		2	5	21	RT
						Poca experiencia del personal de soporte para resolver problemas de configuraciones o cambios de versiones	Deficiencias o caídas de los sistemas o aplicaciones por falta de mantenimiento de los motores de BD		2	5	21	RT
						Asignación de privilegios de acceso a los recursos de información mal configurado	Posibilidad de uso o modificación de los datos de los sistemas y aplicaciones de manera no autorizada		2	5	21	RT
						Soporte técnico de las actualizaciones de las herramientas tardía	Aplicativos (tools) de desarrollo de software obsoletas, discontinuadas o no vigentes		2	3	17	RT
						No se cuenta con un procedimiento formalizado, aprobado y documentado para cambios de versiones	Puesta en producción de versiones no autorizadas o no probadas o en desuso		2	4	19	RT
						No existen controles para instalaciones de software	Instalación de aplicativos no autorizados o no licenciados		2	5	21	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						Incompatibilidad de las versiones de los nuevos sistemas con el software base en las estaciones	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones		2	5	21	RT
						Cantidad de licencias de software de desarrollo limitada	Indisponibilidad, limitaciones o deficiencias en los motores de BD		2	5	21	RT
						Poca experiencia del personal de soporte para resolver problemas de configuraciones o cambios de versiones	Pérdida o eliminación de archivos de la BD		2	5	21	RT
5	Herramientas de gestión de proyectos	1	1	4	6	Aplicativos de gestión de proyectos no licenciados u obsoletos	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	Se generan copias de respaldo de los archivos generados con las herramientas de gestión de proyectos. El custodio es el Jefe de cada proyecto	2	2	10	TT
							Infección por malware		3	1	9	TT
							Baja performance en el funcionamiento de las aplicaciones y herramientas de gestión de proyectos por falta de mantenimiento		3	1	9	TT
							Baja performance en el funcionamiento de las aplicaciones y herramientas de gestión de proyectos por configuración incorrecta del software		3	1	9	TT
							Pérdida del software de instalación		2	2	10	TT
							Posibilidad de uso o modificación de los datos de los sistemas y aplicaciones de manera no autorizada		3	1	9	TT
6	Software de Virtualización	1	2	3	6	Incompatibilidad o poca capacidad de terminales para trabajar en ambientes virtuales	Baja performance de las estaciones de trabajo virtuales	Se lleva un registro de los errores en el funcionamiento del software de virtualización	2	3	12	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
7	Aplicativos	2	4	4	10	Poca experiencia del personal de soporte para instalar nuevos sistemas	Procedimientos de instalación de software con errores	Se ha definido perfiles de usuario de acuerdo a la función que desempeña. Sin embargo, los procedimientos no están documentados	3	3	19	RT
						No existe procedimientos formalizados, aprobados y documentados de gestión de cambios	Cambio de la versión del software base no controlada con repercusión en los sistemas		3	3	19	RT
						No se cuenta con documentación técnica de los sistemas y aplicaciones en producción	Poco entendimiento de la funcionalidad de los sistemas por parte de los desarrolladores		3	3	19	RT
						No se ha estandarizado la codificación en el proceso de desarrollo	Malas prácticas en el desarrollo de software		3	3	19	RT
						No existe procedimientos de seguridad para el acceso o asignación del código fuente en el proceso de desarrollo	Sustracción parcial /total de los archivos de código fuente de los sistemas o aplicaciones		3	5	25	RT
						No se cuenta con equipos servidores para contingencias en el área de desarrollo Los procedimientos de pruebas y testeo antes de producción se realizan en el mismo servidor de producción	No continuidad de los proyectos de desarrollo de software o de la atención de requerimientos de cambio		3	5	25	RT
						Sistema antimalware obsoleto	Infección por malware		2	5	20	RT
						No se cuenta con procedimientos de actualización de perfiles de usuario y de asignación de privilegios	Accesos, uso o manipulación de aplicativos de manera no autorizada		3	5	25	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						Aplicaciones específicas no integradas a los sistemas principales	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración		4	3	22	RT
						No se cuenta con un procedimiento para la atención de requerimientos de cambios formalizado, aprobado y documentado	Aplicaciones y sistemas puestos en producción sin pruebas y testeos		4	5	30	NT

Tabla N° 26. Análisis y evaluación de riesgos de TI del Área de Desarrollo – Activos de Hardware

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	PCs/Laptops	2	3	3	8	Ausencia de programa de mantenimiento preventivo	Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos	El acceso a los equipos terminales es asignado a los empleados de acuerdo al proyecto al que están asignados	2	3	14	TT
						No se cuenta con procedimientos e instructivos de uso adecuado de los equipos terminales	Mal uso de los equipos terminales		3	2	14	TT
						No se cuenta con contactos de proveedores especializados No se programa el mantenimiento de los equipos anualmente Sistema eléctrico antiguo	Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos		3	2	14	TT
						No se cuenta con un plan de mantenimiento No se cuenta con catálogo de contacto de proveedores especializados	Fallas técnicas de los equipos terminales		2	3	14	TT
						No se cuenta con contactos de proveedores especializados para repuestos Los equipos no cuenta con garantía	Caída del equipo por obsolescencia		2	3	14	TT
						Sistema antimalware obsoleto	Caída parcial o total del equipo por efecto de malware		2	3	14	TT
						Los equipos no están configurados para prevenir instalaciones de aplicativos o	Instalación de aplicaciones no autorizadas		3	3	17	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						software no autorizado						
						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	13	TT
						No se aplica políticas de escritorio limpio y pantalla bloqueada	Revelación de información sensible		5	2	18	RT
						No se han definido perfiles de usuario. No existen procedimientos para la asignación de privilegios de acceso según el perfil de usuario	Acceso no autorizado a los equipos terminales		5	3	23	RT
						No se aplica políticas de escritorio limpio y pantalla bloqueada	Revelación de información sensible		3	1	11	TT
						No existe o debilidades en los controles de acceso físico a las áreas seguras	Pérdida o hurto de recursos de tratamiento de datos		5	3	23	RT
2	Servidores	2	3	5	10	No se cuenta con un plan de mantenimiento No se cuenta con catálogo de contacto de proveedores especializados Los equipos críticos no cuentan con garantía o está vencida	Fallas técnicas en los equipos críticos		2	5	20	RT
						No se cuenta con sistema de alertas de sobrecarga de accesos concurrentes y sobre	Indisponibilidad de la infraestructura de almacenamiento secundario		3	5	25	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						almacenamiento						
						El sistema UPS del área de desarrollo no está correctamente dimensionado para soportar toda la carga de abastecimiento de energía de los equipos conectados. Los servidores no cuentan con UPS dedicado	Indisponibilidad del equipo crítico por caída del fluido eléctrico		2	5	20	**RT**
						Sistema antimalware obsoleto	Caída parcial o total del equipo por efecto de malware		3	5	25	**RT**
						No se cuenta con procedimientos e instructivos para el tratamiento de los equipos críticos	Mal uso y tratamiento de los equipos críticos		3	4	22	**RT**
						No se cuenta con equipos o repuestos para equipos de alta disponibilidad	Fallas técnicas en los equipos críticos		2	5	20	**RT**
						No existe un plan de renovación de partes o equipos críticos	Caída del equipo por obsolescencia		2	3	16	**RT**
						Mala configuración por inexperiencia del personal responsable	Caída de los equipos servidores por fallas en la configuración		2	4	18	**RT**
						No se cuenta con mecanismos de seguridad perimetral, específicamente de control de accesos físicos	Manipulación no autorizada del equipo crítico		2	5	20	**RT**

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No se programa el mantenimiento de los equipos anualmente Los servidores no están ubicados en una sala aislada con temperatura controlada	Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos		3	4	22	**RT**
						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	15	**TT**
						No se han definido áreas seguras No existe o debilidades en los controles de acceso físico a las áreas seguras	Pérdida o hurto de recursos de tratamiento de datos		2	5	20	**RT**

Tabla N° 27. Análisis y evaluación de riesgos de TI del Área de Producción – Activos de Información

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Procedimientos y reglamentos de actividades de producción	2	1	3	6	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los procedimientos y reglamentos de actividades de producción están documentados, pero no aprobados. El activo de información es entregado a los empleados, cuando firman su contrato. No existe acuerdos de confidencialidad. No existe un procedimiento formal de gestión de cambios	2	3	12	TT
						Poca difusión de las normativas internas y procedimientos	Incumplimiento de las actividades, funciones y responsabilidades		2	3	12	TT
						No existe procedimientos para la generación de copias de respaldo del activo de información	Indisponibilidad del activo de información por eventos sociales o naturales		1	3	9	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	Modificación parcial o completa no autorizada del contenido del activo de información		2	2	10	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
2	Planes de desarrollo en el Área de Producción y Soporte (Actividades, tareas, asignación de trabajo)	3	2	1	6	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los procedimientos y reglamentos de actividades de producción están documentados, pero no aprobados. El activo de información es entregado a los empleados, cuando firman su contrato. No existe acuerdos de confidencialidad. No existe un procedimiento formal de gestión de cambios	2	2	10	TT
						Desconocimiento de los planes por parte de los usuarios y empleados	Incumplimiento de las actividades, funciones y responsabilidades		1	2	8	TT
						No existe procedimientos para la generación de copias de respaldo del activo de información	Indisponibilidad del activo de información por eventos sociales o naturales		1	2	8	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	Modificación parcial o completa no autorizada del contenido del activo de información		2	2	10	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
3	Plan de mantenimiento preventivo	2	3	1	6	Mala gestión de cambios en los planes No existe difusión ni seguimiento del cumplimiento de los planes	Incumplimiento de actividades, plazos y responsabilidades	La planificación del mantenimiento de equipos se realiza de manera anual Se lleva un registro del cumplimiento de las actividades de mantenimiento	3	3	15	TT
						Presupuesto insuficiente para mantenimiento preventivos Planificación de actividades de mantenimiento incoherentes por falta de coordinación entre áreas	Mala planificación de las actividades de mantenimiento preventivo		3	3	15	TT
						No existen controles de verificación del cumplimiento de las actividades de los planes de mantenimiento	Incumplimiento o ejecución inoportuna de las actividades de mantenimiento preventivo		4	4	22	RT
4	Registros de incidentes y problemas	2	3	3	8	Poca concienciación de los usuarios en materia de seguridad de la información	Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna	Se realizan capacitaciones programadas de concienciación en materia de seguridad Se lleva un registro de incidentes de TI en una hoja de cálculo, pero no existe un procedimiento formal	4	5	26	NT
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un registro de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de gestión de incidentes y problemas	Cambios intencionales o no autorizados en el contenido del activo de información		4	4	22	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						Falta de seguimiento del cumplimiento del procedimiento de gestión de incidentes y problemas	Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna		4	3	18	RT
5	Hojas de requerimientos y cambios aprobadas	2	2	3	7	Requerimientos de cambios no autorizadas Procedimiento de atención de requerimientos de cambios no formalizado, aprobado, documentado y difundido	Atención de los requerimientos de cambios en las aplicaciones y sistemas en producción incorrectas	Se tiene un formato establecido para el registro de las peticiones de cambio, las cuales se anexan en el expediente de los proyectos Las peticiones de cambio son aprobadas por el Líder de cada proyecto	2	4	15	TT
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de atención de requerimientos de cambios en los aplicativos y sistemas en producción No existe un registro de control de cambios	Cambios intencionales o no autorizados en el contenido del activo de información		3	4	19	RT
						Poca experiencia de los analistas Falta o deficiencias en el control de autorización de cambios	Mal registro de los requerimientos de cambio de las aplicaciones y sistemas en producción		4	4	23	RT
6	Registro de usuarios	3	2	2	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad	Extracción o divulgación no autorizada de la información sensible	Se asigna un usuario y clave de acceso a la red y base de datos a los usuarios, la cual es administrada desde un servidor de dominio	2	5	17	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible						
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un registro de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de gestión de usuarios	Cambios intencionales o no autorizados en el contenido del activo de información		2	5	17	**RT**
7	Perfiles de usuario	3	2	2	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los perfiles de usuario son asignados por el Jefe de producción, a petición de los líderes de los proyectos. Los perfiles de usuario están asociados a la función que cumple el empleado o usuario en la empresa	2	5	17	**RT**
						No existe un procedimiento formal, aprobado, documentado y difundido de control de cambios No existe un procedimiento formal, aprobado, documentado y difundido de gestión de perfiles de usuario y asignación de privilegios	Cambios intencionales o no autorizados en el contenido del activo de información		2	4	15	**TT**

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No existe un registro de control de cambios						
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios Falta o deficiencias en los controles de acceso	Creación de perfiles de usuario o generación de privilegios de acceso a los recursos de información no autorizada		2	5	17	**RT**
8	Manuales de usuario	1	1	2	4	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se generan manuales de usuario cuando se realizan cambios sustantivos en las aplicaciones y sistemas	3	3	13	**TT**
						Poco conocimiento de los procesos del negocio Procedimientos de cambios en los sistemas y aplicaciones no contemplan capacitación de usuarios o no son oportunas	Incorrecto uso o poco entendimiento de los manuales de usuario		2	3	10	**TT**

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
9	Estructura de base de datos	2	2	2	6	No se cuenta con un procedimiento ni registros de control de cambios en las estructuras de datos	Errores o inconsistencias en los cambios realizados sobre las estructuras de base de datos	Existe un registro de cambios de código, estructuras de datos y carga de datos, en formato Excel. El encargado de registrar los cambios es el analista programador que realiza el cambio.	2	5	16	RT
						No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible		3	5	21	RT
						No existe procedimientos para la gestión de cambios No se registran los cambios en las estructuras de de datos	Inconsistencia en los datos		3	4	18	RT
10	Bitacora de accesos	2	2	3	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se lleva un registro bitácora de los accesos a la base de datos, aplicaciones y sistemas desde que el usuario se loguea con su usuario. El acceso a la bitácora está permitido solo al Jefe de producción	2	4	15	TT
						Falta o deficiencias en el control de acceso a las bitácoras de seguimiento o auditoría	Acceso y uso no autorizado al contenido de las bitácoras de seguimiento		2	4	15	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		2	4	15	TT
11	Informes de las pruebas de testeo y certificación	3	2	1	6	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Las pruebas y testeos antes de puesta en producción lo realizan el área de producción con la participación del Jefe de Desarrollo. Los resultados de las pruebas y testeos se documentan y anexan en el expediente de cada proyecto No existen procedimientos de seguridad para protegerlos	2	3	13	TT
						Procedimiento mal diseñado o poco entendido - testeo y pruebas	Errores en el proceso con generación de datos o resultados incorrectos		2	4	15	TT
						Documentación y registros desactualizados o no disponibles - testeo y pruebas de cambios	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información		3	4	19	RT
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		2	3	13	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos	Extravío o hurto del activo de información		3	3	16	RT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	3	13	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
12	Configuración de equipos	3	2	3	8	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Los equipos terminales en el área de producción, tienen las mismas configuraciones de sistemas operativos Las configuraciones de los equipos terminales la realizan los responsables de soporte técnico	2	3	13	TT
						Procedimiento mal diseñado o poco entendido - configuración de equipos	Errores en el proceso con generación de datos o resultados incorrectos		3	4	19	RT
						Documentación y registros desactualizados o no disponibles - configuración de equipos	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información		3	4	19	RT
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		3	3	16	RT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos	Extravío o hurto del activo de información		2	4	15	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	4	15	TT
13	Inventario de HW y SW	1	2	3	6	Documentación y registros desactualizados o no disponibles - gestión de inventarios de HW y	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	Se cuenta con un inventario de hardware y software, pero no está actualizado	2	3	13	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						SW						
						Procedimiento mal diseñado o poco entendido - gestión de inventarios	Errores en el proceso con generación de datos o resultados incorrectos		2	3	13	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	3	13	TT
14	Información de respaldos y copias de seguridad	2	2	3	7	No se ha implementado acuerdos de confidencialidad con el personal Poca concienciación en de los empleados materia de seguridad de la información Incumplimiento o deficiencias en los controles de acceso a la información sensible	Extracción o divulgación no autorizada de la información sensible	Se generan copias de seguridad de la base de datos de todas las aplicaciones y sistemas. Una copia se almacena en un disco duro externo que es administrado por el Jefe de Producción, con una frecuencia mensual Se generan respaldos de las aplicaciones y sistemas	2	3	13	TT
						Procedimiento mal diseñado o poco entendido - generación de copias de respaldo	Errores en el proceso con generación de datos o resultados incorrectos		3	5	22	RT
						Documentación y registros desactualizados o no disponibles - generación de copias de respaldos	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información		3	5	22	RT
						Inadecuada gestión de los perfiles de usuario y de los privilegios de acceso	Accesos y uso al activo de información de manera no autorizados		2	3	13	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de gestión de accesos	Extravío o hurto del activo de información		2	5	17	RT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	4	15	TT
15	Documentación del personal (HV)	1	2	2	5	Documentación y registros desactualizados o no disponibles - gestión de legajos	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	La documentación de las hojas de vida de los trabajadores y sus contratos las gestiona el administrador de la empresa.	3	2	11	TT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de accesos No se registran bitácoras de seguimiento o auditoría	Modificación parcial o total de la información		2	4	13	TT

Tabla N° 28. Análisis y evaluación de riesgos de TI del Área de Producción – Activos de Software

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas de gestión (Drupal, Activity Directory, SO)	3	3	3	9	Inexistencia de procedimientos o instructivos de instalación de software	Errores en la instalación de software de gestión	Las terminales en el área de producción cuentan con las mismas versiones de sistemas operativos, software base y software de gestión Existen procedimientos establecidos para las instalaciones y configuraciones del software, pero está desactualizado	2	3	15	TT
						Herramientas con versiones desactualizadas	Baja performance de las herramientas de gestión		2	3	15	TT
						No existe procedimientos ni entorno especial para el cambio de versiones	Desconfiguración de las aplicaciones con impacto en los contenidos de los archivos		2	4	17	RT
						Inexistencia o deficiencias de los controles de instalación de software no permitido	Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información		2	4	17	RT
						Falta de documentación de procedimientos e instructivos de configuración o actualizaciones de aplicaciones	Errores en la configuración de las aplicaciones de gestión		2	3	15	TT
2	Software de ofimática	1	1	3	5	Soporte técnico ineficiente en la instalación de software	Errores en la instalación de software de ofimática	Las terminales en el área de producción cuentan con los mismos softwares de ofimática Existen procedimientos establecidos para las instalaciones y configuraciones del software, pero está desactualizado	2	2	9	TT
						Sistema antimalware obsoleto	Infección por malware		2	2	9	TT
						Soporte técnico inexistente o deficiente de los software base o de ofimática	Desconfiguración o baja de performance de los software base o de ofimática		2	2	9	TT
						Inexistencias de procedimientos o instructivos de instalación y configuración de software	Configuraciones de software que afectan otras aplicaciones o bajan su performance		2	2	9	TT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						Inexistencia o debilidades en los controles de acceso a los recursos de información	Sustracción o eliminación intencional o por error de drivers e instaladores		2	2	9	TT
						Puertas de conexión expuestas por uso de versiones de sistemas operativos de distintas versiones	Acceso a los recursos de información aprovechando debilidades del sistema operativo		2	2	9	TT
3	Motores de base de datos (Oracle, DB2, MySQL)	3	3	3	9	Inexistencia de procedimientos o instructivos de instalación de software	Errores en la instalación de motores de base de datos	Se generan copias de respaldo de la base de datos con una frecuencia semanal. El custodio de las copias en el Jefe de Producción El acceso a las bases de datos en producción, solo es permitido con el usuario del Jefe de Producción Los cambios, nuevas versiones de las aplicaciones y sistemas se prueban y revisan antes de la puesta en producción, documentándose los resultados	2	5	19	RT
						Sistema antimalware obsoleto	Infección por malware		1	5	14	TT
						No se genera una copia de la base de datos para pruebas, testeos y cambios de versiones de la base de datos	Desconfiguración de los motores de base de datos o modificaciones en las estructuras de la base de datos		2	5	19	RT
						Soporte técnico inexistente o deficiente de los motores de base de datos	Desconfiguración o baja de performance de los motores de base de datos		2	5	19	RT
						Inexistencia o debilidades de controles de acceso a la base de datos Privilegios de acceso a la base de datos mal configurados	Acceso a la base de datos de manera no autorizada		2	5	19	RT
						Herramientas con versiones desactualizadas	Baja performance de los motores de base de datos		2	3	15	TT
						No existe procedimientos ni entorno especial para el cambio de versiones	Desconfiguración de los motores de base de datos con impacto en las estructuras de datos		2	4	17	RT
						Inexistencia o deficiencias de los controles de instalación de	Instalación de aplicaciones no permitidas que afectan la performance		2	5	19	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						software no permitido	de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información					
						Licencias limitadas o vencidas de motores de base de datos	Problemas graves o errores en la instancia de conexión a la base de datos		2	5	19	RT
						Falta de documentación de procedimientos e instructivos de configuración o actualizaciones de aplicaciones	Errores en la configuración de los motores de base de datos		2	5	19	RT
4	Software de Virtualización	1	2	3	6	Poca capacidad de los equipos terminales para trabajar en entornos virtuales	Baja performance de la operación de los equipos	Se cuenta con software de virtualización actualizado	2	3	12	TT
5	Aplicaciones	2	3	3	8	Soporte técnico ineficiente en la instalación de software	Errores en la instalación de aplicaciones	Se tiene un procedimiento para atención de requerimientos de modificaciones de las aplicaciones en producción Se registran los cambios en el código, estructura de datos y carga de datos, en una bitácora en Excel. El acceso a los códigos fuentes solo es permitido al Jefe de Desarrollo	3	3	17	RT
						No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	Errores en los cambios de versiones de las aplicaciones o en el software base		3	3	17	RT
						No se genera documentación técnica y funcional de las nuevas aplicaciones o sistemas o de sus modificaciones	Errores en los cambios o dificultad para entender las estructuras de las aplicaciones o base de datos en el proceso de desarrollo		3	3	17	RT
						Falta de estandarización en el proceso de codificación y programación	Codificación o estructuras de datos no integrada o desorganizada		3	3	17	RT
						Inexistencia o debilidades en los controles de acceso a los códigos fuentes	Sustracción o eliminación intencional de los códigos fuente		3	5	23	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No existe procedimientos de continuidad para las aplicaciones y sistemas	Indisponibilidad de las aplicaciones por eventos no controlados		3	5	23	RT
						Inexistencia y deficiencias en los controles de instalación de software no permitido	Instalación de aplicaciones infectadas con malware		2	5	18	RT
						Inexistencia o debilidades de controles de acceso a las aplicaciones Privilegios de acceso a los aplicativos de seguridad mal configurados	Acceso no autorizado a los contenidos de las aplicaciones de seguridad		3	5	23	RT
						Software de desarrollo desactualizadas y sin soporte	Aplicaciones no integradas a los sistemas principales		4	3	20	RT
						No se realizan pruebas ni testeos de nuevas aplicaciones o cambios antes de la puesta en producción	Errores de integración o procesamiento de las aplicaciones		4	5	28	NT

Fuente: Desarrollo propio

Tabla N° 29. Análisis y evaluación de riesgos de TI del Área de Producción – Activos de Hardware

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	PCs/Laptops	3	3	3	9	No se cuenta con un plan de mantenimiento preventivo	Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.	Se ha definido la responsabilidad de la protección de los equipos a los usuarios asignados Se cuenta con un plan de renovación de equipos cada tres años Los equipos terminales están configurados desde un servidor de dominio para evitar instalaciones o desinstalaciones no autorizadas	2	3	15	TT
						Inexistencia o debilidades en los controles de acceso físico a los equipos	Manipulación no autorizada de los equipos terminales		3	2	15	TT
						No existe un plan de mantenimiento preventivo No se cuenta con instructivos para el uso adecuado de los equipos terminales	Indisponibilidad o caída de equipo terminal		3	2	15	TT
						No existe un plan de mantenimiento preventivo No se cuenta con un catálogo de proveedores especializados	Fallas técnicas en los equipos terminales		2	3	15	TT
						No se cuenta con un plan de renovación de equipos y repuestos	Obsolescencia del equipo		2	3	15	TT
						Sistema antimalware obsoleto	Baja performance o caída de los equipos terminales por infección de malware		2	3	15	TT
						Los equipos terminales no están configurados para prevenir la desinstalación de las aplicaciones o software de manera no autorizada	Desinstalación de aplicaciones de manera no autorizadas		3	3	18	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	14	TT
						No se aplica políticas de escritorio limpio y pantalla bloqueada	Revelación de información sensible		5	2	19	RT
						No se cuenta con un procedimiento formal, aprobado, documentado y conocido de gestión de perfiles usuario	Acceso al equipo con diferentes usuarios		5	3	24	RT
						Inexistencia de un procedimiento formal, aprobado, documentado de borrado de la información por baja de equipo	Sustracción o divulgación de información sensible		3	1	12	TT
						No se ha definido áreas seguras Inexistencia o debilidades en los controles de accesos físicos a las áreas seguras o equipos críticos No se cuenta con un procedimiento formal para la movilidad de los equipos fuera de las instalaciones de la empresa	Hurto o extravío de equipos terminal		5	3	24	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
2	Servidores (Aplicaciones, BD, Dominio, Antimalware, de pruebas)	2	3	3	8	No se cuenta con servidores alternos listos para puesta en producción No existe un plan de mantenimiento preventivo No se cuenta con un catálogo de proveedores especializados	Fallas técnicas en los equipos críticos, como servidores y switch	Los servidores se ubican en un área de acceso restringido. La llave la administra el Jefe de Producción Se cuenta con un plan de mantenimiento preventivo anual de los equipos de comunicaciones Se cuenta con sistemas UPS con capacidades y autonomías suficientes para mantener funcionando los servidores por 20 minutos	2	5	18	RT
						No se cuenta con un sistema de alertas de capacidad de disco	Saturación del espacio de almacenamiento secundario		3	5	23	RT
						No se cuenta con un sistema de continuidad alterno para el abastecimiento de energía Los UPS no tienen la autonomía y capacidad necesaria para bastecer de energía a los equipos críticos	Interrupción repentina del fluido eléctrico		2	5	18	RT
						Sistema antimalware obsoleto	Baja de performance o mal funcionamiento por infección de malware		3	5	23	RT
						Inexistencia o debilidades en los controles de acceso físico a los equipos	Manipulación no autorizada de los equipos críticos		3	4	20	RT
						No se cuenta con corta fuegos alternos listos para puesta en producción	Falta de capacidad o fallas técnicas del corta fuego		2	5	18	RT
						No se cuenta con un plan de renovación de equipos y repuestos	Obsolescencia del equipo		2	3	14	TT
						Errores en la configuración de los equipos críticos	Errores de procesamiento o mal funcionamiento		2	4	16	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No se han definido perfiles de usuario. No existen procedimientos para la asignación de privilegios de acceso según el perfil de usuario	Acceso no autorizado a los equipos críticos		2	5	18	RT
						No se cuenta con un plan de mantenimiento preventivo	Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.		3	4	20	RT
						No se cuenta con un plan de continuidad	Deterioro o indisponibilidad del equipo por eventos naturales o sociales		1	5	13	TT
						No se ha definido áreas seguras Inexistencia o debilidades en los controles de accesos físicos a las áreas seguras o equipos críticos	Hurto o extravío de equipos críticos		2	5	18	RT
3	Equipos de comunicación (switchs, routers)	2	3	3	8	No se cuenta con servidores alternos listos para puesta en producción No existe un plan de mantenimiento preventivo No se cuenta con un catálogo de proveedores especializados	Fallas técnicas en los equipos críticos, como servidores y switch	Los equipos de comunicaciones están protegidos por gabinetes. La llave la administra el Jefe de Producción Se han definido áreas seguras para los equipos de comunicaciones Se cuenta con un plan de mantenimiento preventivo anual de los equipos de comunicaciones	3	5	23	RT
						No se cuenta con un plan de renovación de equipos y repuestos	Obsolescencia del equipo		3	5	23	RT

N°	Activo afectado	Criterio de seguridad afectado				Vulnerabilidades	Amenazas	Control existente	Riesgo efectivo			
		Confidencialidad	Integridad	Disponibilidad	Valoración				Probabilidad	Impacto	Nivel de riesgo	Tolerancia
						No se cuenta con un sistema de continuidad alterno para el abastecimiento de energía Los UPS no tienen la autonomía y capacidad necesaria para bastecer de energía a los equipos críticos	Interrupción repentina del fluido eléctrico		3	5	23	**RT**
						No se ha definido áreas seguras Inexistencia o debilidades en los controles de accesos físicos a las áreas seguras o equipos críticos	Hurto o extravío de equipos críticos		3	5	23	**RT**
						No se cuenta con un plan de mantenimiento preventivo	Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.		3	4	20	**RT**
						Inexistencia o debilidades en los controles de acceso físico a los equipos	Manipulación no autorizada de los equipos críticos		2	5	18	**RT**

4.1.4. Fase 4: Tratamiento de los riesgos de TI

Luego de haber determinado el nivel de exposición al riesgo, se debe evaluar la estrategia y mecanismos de seguridad que la empresa ha implementado para la mitigación de los escenarios de riesgo que están fuera de los rangos de tolerancia.

En las tablas siguientes se muestran los resultados de esta evaluación del tratamiento de los riesgos no tolerables que se ha realizado.

Tabla N° 30. Tratamiento de riesgos de TI del Área de Desarrollo - Activos de Información

N°	Activo Afectado	Criticidad	Amenazas	Riesgo Efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Procedimientos y reglamentos de desarrollo	6	Sustracción no autorizada y divulgación de documentación sensible por el personal	5	4	26	NT	Implementar una política de confidencialidad Implementar un Compromiso de Confidencialidad Firmado	Reducir	3	4	19	RT
			Pérdida o sustracción de información	3	4	18	RT	Implementar un sistema de control de versiones	Reducir	2	3	13	TT
4	Hojas de requerimientos y cambios aprobadas	5	Procesamiento erróneo por parte del personal de Desarrollo	4	4	21	RT	Formalizar la metodología de Atención de requerimientos de cambio Capacitar / Concientizar a los usuarios	Reducir	2	3	11	TT
			Modificación parcial o completa de la información, de manera intencional o por error	4	4	21	RT	Implementar un sistema de control de versiones	Reducir	1	4	9	TT
5	Documentos técnicos de desarrollo (análisis, diseño)	7	Sustracción no autorizada y divulgación de documentación sensible por el personal	4	5	27	NT	Implementar una política de confidencialidad Implementar un Compromiso de Confidencialidad Firmado	Reducir	2	5	17	RT

N°	Activo Afectado	Criticidad	Amenazas	Riesgo Efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Procesamiento erróneo por parte del personal de Desarrollo	4	5	27	NT	Formalizar la metodología de Ingeniería de Software Capacitar / Concientizar a los usuarios	Reducir	2	3	13	TT
			Sustracción no autorizada de documentación sensible	3	4	19	RT	Implementar controles para protección de documentos	Reducir	2	4	15	TT
			Errores en la ejecución de las pruebas unitarias	4	5	27	NT	Estandarizar y difundir métodos de ejecución de pruebas unitarias	Reducir	2	3	13	TT
			Información no disponible, en desuso u obsoleta	3	3	16	RT	Revisiones periódicas del Jefe de Desarrollo	Reducir	2	3	13	TT
			Modificación parcial o completa de la información, de manera intencional o por error	3	4	19	RT	Implementar un sistema de control de versiones	Reducir	2	4	15	TT
6	Registros de Control de Cambios (scripts, BD, carga data)	9	Sustracción no autorizada y divulgación de documentación sensible por el personal	3	4	21	RT	Implementar una política de confidencialidad Implementar un Compromiso de Confidencialidad Firmado	Reducir	1	4	13	TT
			Procesamiento erróneo por parte del usuario	4	5	29	NT	Reforzar el compromiso de las gerencias con la ejecución de las pruebas	Reducir	2	4	17	RT
			Sustracción no autorizada de documentación sensible	2	4	17	RT	Implementar controles para protección de documentos	Reducir	1	4	13	TT
			Modificación parcial o completa de la información, de manera intencional o por error	3	3	18	RT	Implementar un sistema de control de versiones	Reducir	2	2	13	TT
7	Manuales de usuario	4	Sustracción no autorizada y divulgación de documentación sensible por el personal	5	3	19	RT	Implementar una política de confidencialidad Implementar un Compromiso de Confidencialidad Firmado	Reducir	3	3	13	TT
			Información no disponible, en desuso u obsoleta	4	3	16	RT	Revisiones periódicas del Jefe de Desarrollo	Reducir	3	3	13	TT

N°	Activo Afectado	Criticidad	Amenazas	Riesgo Efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Sustracción no autorizada de documentación sensible	5	3	19	RT	Implementar controles para protección de documentos	Reducir	2	3	10	TT
8	Informes de las pruebas de testeo y certificación	9	Sustracción no autorizada y divulgación de documentación sensible por el personal	3	4	21	RT	Implementar una política de confidencialidad Implementar un Compromiso de Confidencialidad Firmado	Reducir	1	3	12	TT
			Procesamiento erróneo por parte del usuario	4	5	29	NT	Formalizar la metodología de Ingeniería de Software Capacitar / Concientizar a los usuarios	Reducir	2	3	15	TT
			Información no disponible, en desuso u obsoleta	2	4	17	RT	Revisiones periódicas del Jefe de Desarrollo	Reducir	2	3	15	TT
			Sustracción no autorizada de documentación sensible	3	4	21	RT	Implementar controles para protección de documentos	Reducir	1	2	11	TT
			Modificación parcial o completa de la información, de manera intencional o por error	3	3	18	RT	Implementar un sistema de control de reportes	Reducir	2	2	13	TT
9	Documentos de versiones de software	9	Sustracción no autorizada y divulgación de documentación sensible por el personal	3	4	21	RT	Implementar una política de confidencialidad Implementar un Compromiso de Confidencialidad Firmado	Reducir	1	3	12	TT
			Información no disponible, en desuso u obsoleta	4	3	21	RT	Revisiones periódicas del Jefe de Desarrollo	Reducir	2	3	15	TT
			Sustracción no autorizada de documentación sensible	3	4	21	RT	Implementar controles para protección de documentos	Reducir	1	2	11	TT

Tabla N° 31. Análisis y evaluación de riesgos de TI del Área de Desarrollo - Activos de Software

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas y entornos de desarrollo	7	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones	2	5	17	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	3	11	TT
4	Motores de base de datos	9	Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	2	5	19	RT	Implementar manuales, videos, tutoriales para los softwares	Reducir	1	5	14	TT
			Indisponibilidad o inoperatividad de los sistemas por caída de los motores de base de datos o de los servidores que los administran	2	5	19	RT	Implementar un ambiente para las pruebas de cambios de versiones	Reducir	1	5	14	TT
			Deficiencias o caídas de los sistemas o aplicaciones por falta de mantenimiento de los motores de BD	2	5	19	RT	Implementar monitoreos de performance de las BD	Reducir	1	3	12	TT
			Posibilidad de uso o modificación de los datos de los sistemas y aplicaciones de manera no autorizada	2	5	19	RT	Configurar accesos en base perfiles de usuarios	Reducir	1	5	14	TT
			Puesta en producción de versiones no autorizadas o no probadas o en desuso	2	4	17	RT	Planificación del cambio de versiones	Reducir	2	3	15	TT
			Instalación de aplicativos no autorizados o no licenciados	2	5	19	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	2	4	17	RT
			Software de desarrollo con versiones obsoletas por falta de continuidad de versiones	2	5	19	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	5	14	TT
			Indisponibilidad, limitaciones o deficiencias en los motores de BD	2	5	19	RT	Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras Administración de Licencias	Reducir	1	5	14	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas y entornos de desarrollo	7	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones	2	5	17	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	3	11	TT
			Pérdida o eliminación de archivos de la BD	2	5	19	RT	Implementar manuales, videos, tutoriales para los softwares	Reducir	1	3	12	TT
7	Aplicativos	8	Procedimientos de instalación de software con errores	3	3	17	RT	Implementar instructivos de instalación	Reducir	1	3	11	TT
			Cambio de la versión del software base no controlada con repercusión en los sistemas	3	3	17	RT	Planificación del cambio de versiones	Reducir	1	3	11	TT
			Poco entendimiento de la funcionalidad de los sistemas por parte de los desarrolladores	3	3	17	RT	Elaborar documentación técnica de los desarrollos	Reducir	2	3	14	TT
			Malas prácticas en el desarrollo de software	3	3	17	RT	Difundir los estándares de programación	Reducir	2	2	12	TT
			Sustracción parcial /total de los archivos de código fuente de los sistemas o aplicaciones	3	5	23	RT	Separar los ambientes de contingencia, calidad y desarrollo	Reducir	2	5	18	RT
			No continuidad de los proyectos de desarrollo de software o de la atención de requerimientos de cambio	3	5	23	RT	Separar los ambientes de contingencia, calidad y desarrollo	Reducir	2	4	16	RT
			Infección por malware	2	5	18	RT	Auditoría de código fuente	Reducir	1	5	13	TT
			Accesos, uso o manipulación de aplicativos de manera no autorizada	3	5	23	RT	Desarrollar sistema de control de accesos por aplicativo Mejorar el proceso de reserva de fuentes	Reducir	1	5	13	TT
			Errores en el procesamiento de datos y baja performance de funcionamiento del activo por incorrecta instalación o mala configuración	4	3	20	RT	Planificar la migración de aplicativos a java	Reducir	3	3	17	RT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas y entornos de desarrollo	7	Software de desarrollo con versiones obsoletas por falta de continuidad de versiones	2	5	17	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	3	11	TT
			Aplicaciones y sistemas puestos en producción sin pruebas y testeos	4	5	28	NT	Separar ambientes de certificación Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación	Reducir	2	3	14	TT

Tabla N° 32. Análisis y evaluación de riesgos de TI del Área de Desarrollo - Activos de Hardware

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	PCs/Laptops	8	Instalación de aplicaciones no autorizadas	3	3	17	RT	Elaborar política de protección de equipo Habilitar restricciones en el dominio para prohibir desinstalación de programas Habilitar el protector de pantalla automático Habilitar restricciones de eliminación de iconos de escritorio Capacitación en seguridad de la información	Reducir	2	3	14	TT
			Revelación de información sensible	5	2	18	RT	Habilitar el protector de pantalla automático Capacitación en seguridad de la información	Reducir	2	2	12	TT
			Acceso no autorizado a los equipos terminales	5	3	23	RT	Eliminar usuarios genéricos Generar cuentas de usuarios en base a perfiles de usuario	Reducir	1	2	10	TT
			Pérdida o hurto de recursos de tratamiento de datos	5	3	23	RT	Implementar documentos para el retiro de equipos fuera de las instalaciones (políticas, formatos, procedimientos) Implementar controles físicos de seguridad (cables de seguridad para laptops) Implementar controles para prevenir el acceso físico del personal a lugares restringidos	Reducir	2	3	14	TT
2	Servidores	8	Fallas técnicas en los equipos críticos	2	5	18	RT	Implementar programa de mantenimiento preventivo de equipos Implementar mecanismos de control a los contratos de mantenimiento con terceros Implementar contingencia de servidores Independizar UPS para protección exclusiva de los equipos de C. Cómputo Seguimiento a las garantías Mantener relaciones comerciales con proveedores estratégicos	Reducir	1	3	11	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Indisponibilidad de la infraestructura de almacenamiento secundario	3	5	23	RT	Implementar alertas sobre espacio en disco Implementar solución automatizada para monitoreo de servidores	Reducir	1	3	11	TT
			Indisponibilidad del equipo crítico por caída del fluido eléctrico	2	5	18	RT	Independizar UPS para protección exclusiva de los equipos de C. Cómputo	Reducir	1	3	11	TT
			Caída parcial o total del equipo por efecto de malware	3	5	23	RT	Implementar informes mensuales sobre estado del antivirus Habilitar archivo físico para informes mensuales visados	Reducir	1	5	13	TT
			Mal uso y tratamiento de los equipos críticos	3	4	20	RT	Capacitación a operadores Actualización del MOF (detallando responsabilidades) Elaborar instructivos técnicos sobre la función de los servidores	Reducir	1	4	12	TT
			Fallas técnicas en los equipos críticos	2	5	18	RT	Implementar HA en firewall	Reducir	1	5	13	TT
			Caída de los equipos servidores por fallas en la configuración	2	4	16	RT	Implementar procedimientos de cambios de configuración	Reducir	1	4	12	TT
			Manipulación no autorizada del equipo crítico	2	5	18	RT	Implementar control de claves a los servidores Implementar control dual de clave maestra Renovar el sistema de control de accesos de producción Cambiar la puerta de Data Center por una puerta de metal Implementar procedimientos de cambios de configuración	Reducir	1	4	12	TT
			Baja de performance en el funcionamiento o caídas el recurso de tratamiento de datos	3	4	20	RT	Implementar programa de mantenimiento preventivo de equipos Implementar detectores para el control de temperatura Implementar aire acondicionado de precisión Implementar deshumedesedor	Reducir	1	4	12	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Pérdida o hurto de recursos de tratamiento de datos	2	5	18	RT	Implementar mecanismos para controlar el acceso físico al Centro de Cómputo Implementar controles físicos de seguridad	Reducir	1	5	13	TT

Tabla N° 33. Tratamiento de riesgos de TI del Área de Producción y Soporte - Activos de Información

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
3	Plan de mantenimiento preventivo	6	Incumplimiento o ejecución inoportuna de las actividades de mantenimiento preventivo	4	4	22	RT	Planificación anual de las actividades de mantenimiento preventivo Revisión periódica del cumplimiento del plan de mantenimiento preventivo	Reducir	2	2	10	TT
4	Registros de incidentes y problemas	8	Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna	4	5	28	NT	Clasificación y priorización de los incidentes de TI Desarrollo de actividades de concientización sobre seguridad de la información Evaluaciones del cumplimiento del procedimiento de gestión de incidentes de TI en base a la trazabilidad de la atención de los incidentes de TI	Reducir	1	3	11	TT
			Cambios intencionales o no autorizados en el contenido del activo de información	4	4	24	RT	Evaluaciones periódicas del cumplimiento del procedimiento de gestión de incidentes de TI en base a la trazabilidad de la atención de incidentes de TI	Reducir	1	3	11	TT
			Incumplimiento de la generación de registros de incidentes y problemas, o no es oportuna	4	3	20	RT	Incorporar actividades de mejora continua del procedimiento de gestión de incidentes en base a los registros de atención de incidentes de TI	Reducir	1	3	11	TT
5	Hojas de requerimientos y cambios aprobadas	7	Cambios intencionales o no autorizados en el contenido del activo de información	3	4	19	RT	Evaluaciones periódicas del cumplimiento del procedimiento de atención de requerimientos de cambios de los sistemas en producción	Reducir	2	3	13	TT
			Mal registro de los requerimientos de cambio de las aplicaciones y sistemas en producción	4	4	23	RT	Trazabilidad periódica de los cambios realizados en el procedimiento de atención de requerimientos de cambios de los sistemas en producción	Reducir	2	2	11	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
6	Registro de usuarios	7	Extracción o divulgación no autorizada de la información sensible	2	5	17	RT	Implementar compromiso de confidencialidad de información	Reducir	1	5	12	TT
			Cambios intencionales o no autorizados en el contenido del activo de información	2	5	17	RT	Evaluaciones periódicas del cumplimiento del procedimiento de gestión de cuentas de usuarios	Reducir	2	3	13	TT
7	Perfiles de usuario	7	Extracción o divulgación no autorizada de la información sensible	2	5	17	RT	Implementar compromiso de confidencialidad de información	Reducir	1	5	12	TT
			Creación de perfiles de usuario o generación de privilegios de acceso a los recursos de información no autorizada	2	5	17	RT	Evaluaciones periódicas del cumplimiento del procedimiento de gestión de cuentas de usuarios	Reducir	1	3	10	TT
9	Estructura de base de datos	6	Errores o inconsistencias en los cambios realizados sobre las estructuras de base de datos	2	5	16	RT	Generación de respaldos periódicos de la BD con procedimientos de restore Trazabilidad periódica a los cambios en la BD	Reducir	1	4	10	TT
			Extracción o divulgación no autorizada de la información sensible	3	5	21	RT	Implementar compromiso de confidencialidad de información	Reducir	1	5	11	TT
			Inconsistencia en los datos	3	4	18	RT	Implementación de un procedimiento de certificación de módulos antes de la puesta en producción	Reducir	2	2	10	TT
11	Informes de las pruebas de testeo y certificación	6	Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	3	4	18	RT	Implementación de un procedimiento de certificación de módulos antes de la puesta en producción	Reducir	1	2	8	TT
			Extravío o hurto del activo de información	3	4	18	RT	Implementar compromiso de confidencialidad de información Implementar controles para protección de documentos	Reducir	1	4	10	TT
12	Configuración de equipos	8	Errores en el proceso con generación de datos o resultados incorrectos	3	4	20	RT	Implementar un sistema de control de versiones	Reducir	1	2	10	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	3	4	20	RT	Revisiones periódicas de los cambios en las configuraciones de equipos	Reducir	1	2	10	TT
			Accesos y uso al activo de información de manera no autorizados	3	3	17	RT	Definir y configurar el control de accesos por roles	Reducir	2	2	12	TT
			Extravío o hurto del activo de información	2	4	16	RT	Implementar compromiso de confidencialidad de información Implementar controles para protección de documentos	Reducir	1	4	12	TT
			Modificación parcial o total de la información	2	4	16	RT	Implementar un sistema de control de versiones	Reducir	1	3	11	TT
14	Información de respaldos y copias de seguridad	7	Errores en el proceso con generación de datos o resultados incorrectos	3	5	22	RT	Implementar un proceso de generación de copias de seguridad con restore	Reducir	1	2	9	TT
			Descontrol o desorganización de la información en el proceso: duplicidad, inexistencia o errores en la información	3	5	22	RT	Revisiones periódicas de las copias de seguridad de la información en base a procesos de restore	Reducir	1	2	9	TT
			Extravío o hurto del activo de información	2	5	17	RT	Implementar compromiso de confidencialidad de información Implementar controles para protección de documentos	Reducir	1	4	11	TT

Tabla N° 34. Tratamiento de riesgos de TI del Área de Producción y Soporte - Activos de Software

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
1	Herramientas de gestión	9	Desconfiguración de las aplicaciones con impacto en los contenidos de los archivos	2	4	17	RT	Planificación del cambio de versiones	Reducir	1	4	13	TT
			Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información	2	4	17	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	4	13	TT
3	Motores de base de datos (Oracle, DB2, MySQL)	9	Errores en la instalación de motores de base de datos	2	5	19	RT	Implementar manuales, videos, tutoriales para los softwares Implementar un ambiente para las pruebas de cambios de versiones	Reducir	1	3	12	TT
			Desconfiguración de los motores de base de datos o modificaciones en las estructuras de la base de datos	2	5	19	RT	Implementar monitoreos de performance de las BD	Reducir	1	5	14	TT
			Desconfiguración o baja de performance de los motores de base de datos	2	5	19	RT	Planificación de las actividades de mantenimiento preventivo Capacitación al personal de soporte técnico	Reducir	1	3	12	TT
			Acceso a la base de datos de manera no autorizada	2	5	19	RT	Configurar accesos en base perfiles de usuarios	Reducir	1	5	14	TT
			Desconfiguración de los motores de base de datos con impacto en las estructura de datos	2	4	17	RT	Planificación del cambio de versiones	Reducir	1	4	13	TT
			Instalación de aplicaciones no permitidas que afectan la performance de las aplicaciones y sistemas o generan escenarios de riesgo a la seguridad de la información	2	5	19	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	4	13	TT
			Problemas graves o errores en la instancia de conexión a la base de datos	2	5	19	RT	Implementar controles y revisiones mensuales para las renovaciones de licencias	Reducir	1	4	13	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Errores en la configuración de los motores de base de datos	2	5	19	RT	Implementar manuales, videos, tutoriales para los softwares	Reducir	1	5	14	TT
5	Aplicaciones	8	Soporte técnico ineficiente en la instalación de software	3	3	17	RT	Implementar instructivos de instalación	Reducir	1	4	12	TT
			No se cuenta con un procedimiento formal, aprobado, documentado y difundido de control de cambios	3	3	17	RT	Planificación del cambio de versiones	Reducir	1	2	10	TT
			No se genera documentación técnica y funcional de las nuevas aplicaciones o sistemas o de sus modificaciones	3	3	17	RT	Elaborar documentación técnica de los desarrollos	Reducir	1	1	9	TT
			Falta de estandarización en el proceso de codificación y programación	3	3	17	RT	Difundir los estándares de programación	Reducir	1	2	10	TT
			Inexistencia o debilidades en los controles de acceso a los códigos fuentes	3	5	23	RT	Separar los ambientes de contingencia, calidad y desarrollo	Reducir	1	3	11	TT
			No existe procedimientos de continuidad para las aplicaciones y sistemas	3	5	23	RT	Separar los ambientes de contingencia, calidad y desarrollo	Reducir	1	3	11	TT
			Inexistencia y deficiencias en los controles de instalación de software no permitido	2	5	18	RT	Auditoría de código fuente	Reducir	1	5	13	TT
			Inexistencia o debilidades de controles de acceso a las aplicaciones Privilegios de acceso a los aplicativos de seguridad mal configurados	3	5	23	RT	Desarrollar sistema de control de accesos por aplicativo Mejorar el proceso de reserva de fuentes	Reducir	1	3	11	TT
			Software de desarrollo desactualizadas y sin soporte	4	3	20	RT	Planificar la migración de aplicativos a java	Reducir	2	3	14	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			No se realizan pruebas ni testeos de nuevas aplicaciones o cambios antes de la puesta en producción	4	5	28	NT	Separar ambientes de certificación Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación	Reducir	1	3	11	TT

Tabla N° 35. Tratamiento de riesgos de TI del Área de Producción y Soporte - Activos de Hardware

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
	PCs/Laptops	9	Desistalación de aplicacionesde manera no autorizadas	3	3	18	RT	Elaborar política de protección de equipo Habilitar restricciones en el dominio para prohibir desinstalación de programas Habilitar el protector de pantalla automático Habilitar restricciones de eliminación de iconos de escritorio Capacitación en seguridad de la información	Reducir	2	2	13	TT
			Revelación de información sensible	5	2	19	RT	Habilitar el protector de pantalla automático Capacitación en seguridad de la información	Reducir	2	2	13	TT
			Acceso al equipo con diferentes usuarios	5	3	24	RT	Eliminar usuarios genéricos Generar cuentas de usuarios en base a perfiles de usuario	Reducir	2	2	13	TT
			Hurto o extravío de equipos terminal	5	3	24	RT	Implementar documentos para el retiro de equipos fuera de las instalaciones (políticas, formatos, procedimientos) Implementar controles físicos de seguridad (cables de seguridad para laptops) Implementar controles para prevenir el acceso físico del personal a lugares restringidos	Reducir	2	3	15	TT
2	Servidores (Aplicaciones, BD, Dominio, Antimalware, de pruebas)	8	Fallas técnicas en los equipos críticos, como servidores y switch	2	5	18	RT	Implementar programa de mantenimiento preventivo de equipos Implementar mecanismos de control a los contratos de mantenimiento con terceros Implementar contingencia de servidores Independizar UPS para protección exclusiva de los equipos de C. Cómputo Seguimiento a las garantías Mantener relaciones comerciales con proveedores estratégicos	Reducir	1	4	12	TT
			Saturación del espacio de almacenamiento secundario	3	5	23	RT	Implementar alertas sobre espacio en disco Implementar solución automatizada para monitoreo de servidores	Reducir	1	4	12	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
			Interrupción repentina del fluido eléctrico	2	5	18	RT	Independizar UPS para protección exclusiva de los equipos de Cómputo	Reducir	1	3	11	TT
			Baja de performance o mal funcionamiento por infección de malware	3	5	23	RT	Implementar informes mensuales sobre estado del antivirus Habilitar archivo físico para informes mensuales visados	Reducir	1	3	11	TT
			Manipulación no autorizada de los equipos críticos	3	4	20	RT	Capacitación a operadores Actualización del MOF (detallando responsabilidades) Elaborar instructivos técnicos sobre la función de los servidores	Reducir	1	2	10	TT
			Falta de capacidad o fallas técnicas del corta fuego	2	5	18	RT	Implementar HA en firewall	Reducir	1	5	13	TT
			Errores de procesamiento o mal funcionamiento	2	4	16	RT	Implementar procedimientos de cambios de configuración	Reducir	1	4	12	TT
			Acceso no autorizado a los equipos críticos	2	5	18	RT	Implementar control de claves a los servidores Implementar control dual de clave maestra Renovar el sistema de control de accesos de producción Cambiar la puerta de Data Center por una puerta de metal Implementar procedimientos de cambios de configuración	Reducir	1	4	12	TT
			Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.	3	4	20	RT	Implementar programa de mantenimiento preventivo de equipos Implementar detectores para el control de temperatura Implementar aire acondicionado de precisión Implementar deshumedesedor	Reducir	1	3	11	TT
			Hurto o extravío de equipos críticos	2	5	18	RT	Implementar mecanismos para controlar el acceso físico al Centro de Cómputo Implementar controles físicos de seguridad	Reducir	1	4	12	TT

N°	Activo afectado	Valoración	Amenazas	Riesgo efectivo				Mecanismos de protección propuestos / Controles	Tipo de control	Riesgo Residual			
				Probabilidad	Impacto	Nivel de riesgo	Tolerancia			Probabilidad	Impacto	Nivel de riesgo	Tolerancia
3	Equipos de comunicación (switchs, routers)	8	Fallas técnicas en los equipos críticos, como servidores y switch	3	5	23	RT	Implementar programa de mantenimiento preventivo de equipos Implementar mecanismos de control a los contratos de mantenimiento con terceros Seguimiento a las garantías Mantener relaciones comerciales con proveedores estratégicos	Reducir	1	4	12	TT
			Obsolescencia del equipo	3	5	23	RT	Renovación tecnológica	Reducir	2	4	16	RT
			Interrupción repentina del fluido eléctrico	3	5	23	RT	Incluir los equipos en el "proyecto de implementación UPS" para el área de producción	Reducir	1	4	12	TT
			Hurto o extravío de equipos críticos	3	5	23	RT	Implementar gabinetes con seguridad (todos los ambientes)	Reducir	2	5	18	RT
			Degradación de los equipos por efectos naturales e industriales, como: polvo, suciedad, sol, humedad, etc.	3	4	20	RT	Elaborar plan de mantenimiento preventivo	Reducir	1	4	12	TT
			Manipulación no autorizada de los equipos críticos	2	5	18	RT	Definir rol de responsables	Reducir	1	4	12	TT

4.1.5. Plan de tratamiento de los riesgos de TI

A continuación, se detallan las actividades desarrolladas como mecanismos de protección o controles.

Tabla N° 36. Plan de tratamiento de riesgos de TI

N°	Mecanismo de protección	Actividades
1	Actualizar los estándares de programación	- Revisión de los estándares de programación para aplicativos - Redefinición de estándares de programación para aplicativos - Publicación de los estándares de programación para aplicativos - Inducción/Difusión al personal de desarrollo, sobre los estándares programación para aplicativos
2	Auditoría de código fuente	- Contrato de especialista en auditoria de códigos fuente - Elaboración del Plan de auditoria anual - Ejecución de la primera auditoría - Ejecución de las Acciones Correctivas / Preventivas
3	Concientizar al personal sobre la Seguridad de Información	- Elaborar plan de concientización en seguridad de información - Elaborar material de concientización / difusión - Ejecutar primera concientización en Seguridad de Información
4	Configurar accesos a carpetas por perfiles a la documentación Implementar controles para protección de documentos	- Definir alternativas de estructura de almacenamiento (SharePoint / carpetas) - Ejecución de alternativa seleccionada - Configuración de permisos por roles
5	Configurar accesos por perfiles a la Base de Datos (MySQL)	- Elaborar inventario de usuarios vs Base de Datos - Asignar accesos a usuarios
6	Contrato de confidencialidad con los proveedores	- Definición con área legal tipos de documentos para establecer confidencialidad con proveedores - Elaboración de Documentos definidos - Aprobación de documentos
7	Definir canales de comunicación eficiente con proveedores de servicios en línea y en lotes	- Definir el canal formal de comunicación entre Agroindustrial Pomalca SAA y sus proveedores de servicios tipo IaaS para reportar incidencias en producción.
8	Desarrollar sistema de control de accesos por aplicativo	- Evacuación y adquisición de software especializado para el control de accesos
9	Elaborar documentación técnica de los desarrollos	- Elaborar matriz para control de entrega de documentos de los proyectos
10	Dimensionar licencias según las demandas presentes y futuras Administración de Licencias Implementar controles y revisiones anuales para las renovaciones de licencias Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras	- Elaborar lineamientos para la gestión de licencias - Definir criterios de dimensionamiento de licencias - Ejecutar primera revisión del inventario de licencias - Realizar dimensionamiento anual de licencias
12	Elaborar y difundir MOFs Mantener actualizado la información la documentación	- Elaborar/Actualizar MOF de personal de desarrollo - Difundir MOF a todo el personal de desarrollo
13	Estandarizar y difundir métodos de ejecución de pruebas unitarias	- Capacitar a los desarrolladores en técnicas para la elaboración de pruebas unitarias
14	Formalizar la metodología de Atención de requerimientos Capacitar / Concientizar a los usuarios	- Elaborar procedimientos y formatos para la metodología de Atención de Requerimientos - Aprobar procedimientos y formatos - Difusión y Capacitación a personal de desarrollo y usuarios finales
15	Formalizar la metodología de Ingeniería de Software	- Elaborar procedimientos y formatos para la metodología de Ingeniería de Software - Aprobar procedimientos y formatos - Difusión y Capacitación a personal de desarrollo y usuarios finales
16	Implementar compromiso de confidencialidad Implementar una política de confidencialidad	- Definición con área legal tipos de documentos para establecer confidencialidad de personal interno - Aprobación de documentos
17	Implementar instructivos de instalación	- Elaborar instructivos de instalación

18	Implementar manuales, videos, tutoriales para los softwares	- Identificar necesidad de manuales, videos, tutoriales para los softwares utilizados - Implementar manuales, videos, tutoriales para los softwares
19	Implementar procedimientos e instructivos para configurar ambientes de prueba	- Elaborar procedimientos e instructivos para configuración de ambientes de prueba (en línea y batch) - Revisar y aprobar procedimientos
20	Implementar un laboratorio para las pruebas de cambios de versiones	- Elaborar procedimientos / formatos para implementar laboratorio de pruebas - Revisar y Aprobar procedimientos
21	Implementar un sistema de control de versiones Planificación del cambio de versiones	- Definir herramienta para control de versiones - Evaluar herramienta especializada - Implementar herramienta especializada
22	Separar los ambientes de contingencia, calidad y desarrollo	- Separar los ambientes de contingencia, control de calidad, producción y desarrollo
23	Mejorar el proceso de reserva y desarrollo de fuentes para aplicativos Java.	- Revisar estructura de los proyectos - Ejecutar mejoras a los proyectos
24	Revisiones periódicas de nuevas actualizaciones	- Elaborar lineamientos de nuevas actualizaciones - Ejecutar primera revisión de nuevas versiones de los aplicativos
25	Revisiones trimestrales de la documentación de proyectos del Jefe de Desarrollo	- Elaborar lineamientos para las revisiones de la documentación - Ejecutar primera revisión de cumplimiento de documentación de proyectos
26	Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación	- Definir herramienta de control de cambios - Evaluar herramienta especializada - Implementar herramienta especializada
27	Alertas, seguimiento, reportes, etc. sobre el servicio de Base de Datos	- Elaborar inventario de servicios críticos del servidor - Identificar alertas a configurar por cada servicio - Configurar alertas de problema en el servicio - Definir reportes periódicos de performance del servidor - Configurar y programar reportes periódicos de la performance del servidor - Configura reportes periódicos de seguimiento de espacio disponible en el disco duro
28	Definir y configurar el control de accesos por roles (documentos, base de datos)	- Definir roles en base a responsabilidades - Definir accesos por rol - Asignar y configurar accesos - Validar los accesos
29	Definir y configurar el control de accesos por roles para la documentación de proyectos Implementar inventario de documentos y control de cambios	- Definir alternativas de estructura de almacenamiento (SharePoint / carpetas) - Ejecución de alternativa seleccionada - Configuración de permisos por roles - Configuración de control de cambios
30	Definir y configurar el control de accesos por roles para las bases de datos	- Elaborar inventario de usuarios que acceden actualmente a la BD
31	Definir y configurar el control de accesos por roles para manipulación de bases Implementar controles de acceso a las plataformas y los códigos fuente Implementar inventario de documentación del código fuente	- Elaborar inventario de usuarios que acceden actualmente a la BD - Identificar roles a configurar - Identificar accesos por rol - Configurar roles y accesos de base de datos - Asignar roles por usuario - Validar asignación de roles y accesos - Elaborar documento de roles y accesos - Capacitar a Producción en la asignación de roles y actualización de documento
32	Elaborar y difundir MOFs (incluir Seguridad de Información) Establecer y difundir procedimientos y políticas Mantener actualizado la información la documentación	- Revisar Análisis de Puestos elaborado - Actualizar y validar Análisis de Puestos - Enviar a RRHH el Análisis de Puestos para su revisión, aceptación y publicación
33	Implementar ambientes de desarrollo diferente al de producción Implementar ambientes de desarrollo	- Elaborar documento de especificaciones de servidor de desarrollo - Implementar servidor de desarrollo - Configurar servidor - Importar datos - Asignar accesos a usuarios - Validar implementación
34	Revisiones periódicas de nuevas actualizaciones de software	- Elaborar plan de revisiones periódicas de actualización de software
35	Implementar controles de	- Elaborar inventario de procesos de carga

	procesamientos de información	- Elaborar inventario de controles de procesos aimplementar - Implementar controles - Elaborar reportes periódicos de ejecución de procesos
36	Implementar controles de validación de información procesada	- Elaborar inventario de tablas - Identificar métodos de validación por cada tabla procesada - Implementar reportes y controles de validación de información
37	Actualización de manuales de configuración	- Elaborar manuales de configuración - Elaborar instructivos de configuración de respaldo y restauración para servidores
38	Implementa programa de capacitación y sensibilización al personal en seguridad de información	- Elaborar presentación de capacitación en Seguridad de Información - Elaborar boletines de Seguridad de Información - Ejecutar Capacitación en Seguridad de Información
39	Capacitación al equipo de administración en cuidado de equipos	- Elaborar un plan de capacitación en equipos de cómputo - Capacitar al Equipo de mantenimiento en cuidado de equipos de cómputo (impresoras, laptop, PC's, otros)
40	Capacitación en uso de equipos de cómputo	- Elaborar un plan de capacitación en equipos de cómputo - Capacitar a los usuarios en cuidado de equipos de cómputo (impresoras, laptop, PC's, otros)
41	Coordinaciones previas a los trabajos de mantenimiento	- Elaborar lineamientos para los trabajos de mantenimiento a las PC's, Laptops, Impresoras, Otros
42	Elaborar documentación técnica sobre función de los servidores	- Elaborar instructivos técnicos para la manipulación de servidores
43	Contar con un stock mínimo de repuestos	- Evaluar stock mínimo de Routers, Switch y Patch Panel - Adquisición de stock de Routers, Switch y Patch Panel - Inventariar equipos de comunicación
44	Contar con un stock mínimo de repuestos y laptop	- Evaluar stock mínimo repuestos de PC's y laptops - Adquisición de stock de repuestos de PC's y laptops - Inventariar de repuestos de PC's y laptops
45	Implementar programa de mantenimiento preventivo de equipos	- Seleccionar equipos para el mantenimiento preventivo interno - Elaborar procedimiento para el Mantenimiento preventivo de equipos - Elaborar programa de mantenimiento preventivo
46	Corregir las instalaciones eléctricas	- Detectar y reportar conexiones eléctricas inadecuadas - Corregir instalaciones eléctricas inadecuadas
47	Seguimiento a las garantías	- Elaborar lineamientos para el seguimiento y control de garantías
48	Mantener relaciones comerciales con proveedores estratégicos	- Elaborar de lista de proveedores, diferenciando los estratégicos
49	Control diario del estado del antivirus y antispam	- Elaborar lineamientos para el control y seguimiento diario del estado del antivirus y antispam - Elaborar bitácora de control de antivirus y antispam
50	Elaborar instructivos, políticas y procedimientos de operación y mantenimiento	- Elaborar instructivos, políticas y procedimiento para la operación y mantenimiento - Elaborar instructivos, políticas y procedimiento para la operación y mantenimiento de la Central Telefónica - Elaborar instructivos, políticas y procedimiento para la operación y mantenimiento de Firewall - Elaborar instructivos para la operación y mantenimiento de antivirus y antispam - Elaborar instructivos para la operación y mantenimiento del directorio activo - Elaborar instructivos para la operación y mantenimiento del servidor de archivo - Elaborar instructivos para la operación y mantenimiento de Servidores
51	Elaborar política de protección de equipos (PC's, laptops e Impresoras	- Elaborar la política para la protección de PC's, laptops, impresoras, otros
52	Habilitar restricciones en el dominio para prohibir desinstalación de programas	- Habilitar restricciones en el dominio para prohibir desinstalación de programas
53	Habilitar el protector de pantalla automático	- Habilitar el protector de pantalla automático
54	Eliminar usuarios genéricos	- Identificar usuarios genéricos en todas las Sedes - Eliminar usuarios genéricos / Reasignar
55	Establecer un inventario actualizado de equipos (vida útil)	- Definir vida útil de las PC's, laptops, servidores, UPS, otros - Elaborar inventario actualizado de todos los equipos (incluir vida útil por equipo)
56	Elaborar plan de renovación de equipos	- Elaborar plan de renovación de equipos (PC's, laptops, UPS)
57	Implementar controles para prevenir el acceso físico del personal a lugares	- Elaborar Check List de controles para prevenir acceso físico de personal a lugares restringidos

	restringidos	- Implementar controles para para prevenir acceso físico de personal a lugares restringidos - Elaborar lineamientos para ingreso a lugares restringidos
58	Implementar extintores de Gas Halotron	- Adquirir extintores de gases de Halotron y polvo químico - Implementar extintores especiales
59	Implementar aire acondicionado de precisión	- Evaluación de tipos de aire acondicionado de precisión - Presentación y sustentación a Gerencia TI - Adquirir aire acondicionado de precisión - Implementación de aire acondicionado de precisión seleccionado
60	Implementar deshumedecedor	- Evaluación de tipos de deshumedecedor - Presentación y sustentación a Gerencia TI - Adquirir deshumedecedor
61	Independizar UPS para protección exclusiva de los equipos de C. Cómputo	- Cotizar trabajo de circuito eléctrico independiente - Ejecutar trabajo circuito eléctrico - Elaborar plan de pruebas de UPS - Realizar pruebas de independización

Fuente: Desarrollo propio

CONCLUSIONES

1. El implementar mecanismos para que la información de una organización cumpla con los requisitos de seguridad, como son su confidencialidad, integridad y disponibilidad, requiere el conocimiento de la empresa. Por ello, para lograr este objetivo, se tuvo que describir y mapear los procesos típicos en las empresas del sector agroindustrial azucarero, tomando como referencia, la empresa Agroindustrial Pomalca SAA, con la finalidad de determinar el alcance de un SGSI que proteja los activos de TI que están relacionados con los procesos. Los resultados nos indican que los activos de TI que se deberán proteger en una empresa del sector agroindustrial azucarero son los que dan soporte a los procesos de producción y comercialización, que son el core del negocio.

2. Los estándares de seguridad de la información nos indican que son varios dominios los que deben ser considerados en un SGSI. Sin embargo, se debe analizar cuáles de los dominios serán considerados en el alcance del SGSI en base a las características propias de los procesos en la empresa, su capacidad instalada, el equipamiento con el que cuenta y el tipo de activos de información que deben de protegerse. Para ello, se realizó un análisis de aplicabilidad de los controles de seguridad, en base a la identificación de los activos de información y el equipamiento de TI que se utilizan en los procesos seleccionados en el alcance del SGSI y los objetivos de control del estándar ISO/IEC 27002. El análisis nos dio como resultado que los activos de información que tienen mayor prioridad de protección son los que están relacionados con los dominios de seguridad de: Continuidad del negocio, Desarrollo de sistema de información, Control de accesos, gestión de recursos humanos y Gestión de activos.

3. Lograr los objetivos de un SGSI depende mucho de los resultados del análisis de riesgos de TI que se realice. Es importante contar con un marco metodológico que identifique y evalúe los escenarios de riesgo que pueden afectar los criterios de seguridad de los activos de TI. Tomando como base la metodología Magerit y el enfoque de la norma ISO/IEC 27005 se elaboró un marco metodológico para la gestión de riesgos, en la cual se priorizó los activos de TI a proteger, se definió una forma de identificar las amenazas y vulnerabilidades para cada activo, se valoró el impacto y la probabilidad de ocurrencia de los escenarios de riesgo y finalmente se estimó los niveles de exposición al riesgo.

4. Ningún sistema o modelo de gestión de riesgos cumpliría su función si no permite evaluar los controles o mecanismos de protección que se propongan para la mitigación de riesgos en rangos no tolerables. Para ello, se realizó una simulación del procedimiento de tratamiento de los riesgos, a través de la inclusión de actividades de evaluación de la efectividad de controles. Esto sirvió para identificar controles necesarios y la planificación de las actividades para su implementación. En este caso se propusieron 61 mecanismos de control.

Recomendaciones

1. Las limitaciones que se tuvieron para la recopilación de la información en diferentes empresas del sector agroindustrial azucarero, nos permite proponer la realización de otras investigaciones en las que se aplique el modelo de gestión de riesgos de TI propuesto, para probar y contrastar los resultados obtenidos en nuestra investigación.

2. Se recomienda automatizar el marco metodológico propuesto para poder hacer frente a cualquier cambio que se pueda dar en la empresa, en relación a los componentes de la gestión de riesgos que hemos considerado en el modelo.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre Mollehuanca, D. A. (2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S:A. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Aguirre, D., & Palacios, J. (2014). *Evaluación técnica de seguridades del data center del municipio de Quito según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.* Ecuador: Universidad de las fuerzas armadas ESPE, Sede SANGOLQUI.

Alexander, A. (2011). Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca. CENTRUM - Centro de Negocios, Pontificia Universidad Católica del Perú.

BSI Group México . (s/a). Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013. *ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición*.

Carrasco, C. A. (2016). *Impacto del riesgo en el gobierno de las tecnologias de Información y comunicación en la gestión empresarial industrial del sigo XXI.* Lima-Perú.

Condori Alejo, H. I. (2016). Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. *tesis postgrado*. Lima: Universidad Inca Garcilaso de la Vega.

Enriquez, P. (2013). Implementación de los controles asignados al dominio "Gestión De Activos", bajo los lineamientos establecidos por la norma ISO/IEC 27001 anexo a, para las empresas Municipales de Cali, Emcali E.I.C.E-ESP. *Tesis*. Cali, Colombia.

Espinoza Aguinaga, H. R. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Espinoza, A. H. (2017). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *Tesis PreGrado*. Lima: Pontificia Universidad Católica del Peru.

Giuratal, P. (2008). *Application Strategy and Design for a Profitable SaaS.* Recuperado el 13 de enero de 2018, de http://www.ebizq.net/hot_topics/web20/features/9365.html.

Hernández Pinto, M. G. (2006). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. *tesis pregrado*. Guayaquil - Ecuador: Escuela Superior Politécnica del Litoral.

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, P. (24 de 05 de 2010). *Metodología de la Investigación.* Obtenido de https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf

Huamán, F. (2014). Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del Estado Peruano. *Tesis*. Lima, Perú.

Huamán, F. (2014). Diseño de Procedimientos de Auditoría de Cumplimiento de la Norma NTP-ISO/IEC 17799:2007 como parte del Proceso de Implantación de la Norma Técnica NTP-ISO/IEC 27001:2008 en Instituciones del Estado Peruano. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

INDECOPI. (2014). *Norma Técnica Peruana "NTP-ISO/ IEC 27001:2014. Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requisitos. Segunda edición. Lima,Perú.*

Inteco. (s/a). Implantación de un SGSI en la empresa. *SGSI*, 22.

ISO 27000.es. (2005). *ISO 27000*. Recuperado el 15 de 03 de 2016, de ISO 27000: www.iso27000.es

ISO 27001. (2005). *Norma Técnica Peruana. Adaptado en el año 2008.*

ISO/IEC 27001. (2013). *Tecnologia de la información - Tecnicas de seguridad - Sistemas de Gestion de seguridad de la información - Requerimientos.*

ISO/IEC 27002. (2013). *Information technology - Security techniques - Code of practice for information security management.* EEUU.

ISOTools Excellence. (17 de 01 de 2014). *http://www.pmg-ssi.com*. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

ISOTools Excellence. (18 de 08 de 2015). *La norma ISO 27001:2013 ¿Cuál es su estructura? [Entrada en Blog]*. Obtenido de https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

López, A. (2011). Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara. *Tesis*. Venezuela.

Magerit - Libro 1. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciónes Públicas.

Magerit. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciónes Públicas.

MAGERIT. (18 de 09 de 2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Montesino Perurena, R., Baluja Garcia, W., & Porven Rubier, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista de Ingenieria Electrónica Automática y Comunicaciones*.

NTP ISO/IEC 17799. (2007). *EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.* Lima.

NTP-ISO/IEC 27001. (2014). *EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.* Lima.

NTP-ISO/IEC 27005. (2009). *EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información.* Lima, Perú.

NTP-ISO/IEC 27005. (2009). *EDI. Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información.* Primera Edicion 2009-09-30.

Ozier, W. (2004). *Risk Analysis and Assessment" Information Security Management Handbook. 5th edition.* USA: Auerbach Publications.

Palacios, J., & Aguirre, D. (2014). Evaluación técnica de seguridades de la data center del municipio de Quito según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005. *Tesis*. Ecuador.

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals.* USA: Auerbach Publications.

Reina García, E., & Morales Ramírez , J. R. (2014). Modelamiento de procesos basados en el grupo de normas internacionales ISO/IEC 27000 para gestionar el riesgo y seleccionar controles en la implementación del sistema de gestión de seguridad de la información. *tesis pregrado*. Universidad tecnológica de Pereira Facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación.

Robles , R., & Rodriguez de Roa, Á. (2016). La gestión de la seguridad en la empresa. *Comite de Entidades de Certificación de la AEC*, 14-18.

Talavera Álvarez, V. R. (2015). *Diseño de un Sistema de Gestión De Seguridad de la Información para una entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013.* Lima-Perú: Pontificia Universidad Católica del Perú.

Talavera, V. (2015). Diseño de un Sistema de Gestión De Seguridad de la Información para una entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013. *Tesis*. Lima, Perú.

ANEXO N° 1

TABLAS DE REFERENCIA PARA LA VALORACIÓN DE LA CRITICIDAD DE LOS ACTIVOS DE TI

Para la valoración de los activos se tomarán en cuenta las siguientes dimensiones de seguridad:

Tabla N° 37. Descripción de las dimensiones de seguridad de la información que se tomarán en cuenta en la valoración de la criticidad de los activos de TI

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Fuente: (Magerit, 2012)

Tabla N° 38. Definición de escala de valoración de la criticidad de los activos de TI

[pi] Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7 – 8	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5 – 6	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3 – 4	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1 – 2	pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9 - 10	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7 - 8	probablemente cause un incumplimiento grave de una ley o regulación
5 - 6	probablemente sea causa de incumplimiento de una ley o regulación
3 – 4	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1 – 2	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9 - 10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7 - 8	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5 - 6	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

3 – 4	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1 – 2	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales económicos	
9 - 10	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7 - 8	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
5 - 6	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3 – 4	de bajo interés para la competencia de bajo valor comercial
1 – 2	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
[da] de interrupción del servicio	
9 - 10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7 - 8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5 - 6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3 – 4	Probablemente cause la interrupción de actividades propias de la Organización
1 – 2	Pudiera causar la interrupción de actividades propias de la Organización
[po] de orden público	
9 - 10	alteración seria del orden público
7 - 8	probablemente cause manifestaciones, o presiones significativas
3 - 6	causa de protestas puntuales
1 – 2	pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7 – 8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5 – 6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3 – 4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1 – 2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] administración y gestión	
9 - 10	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7 - 8	probablemente impediría la operación efectiva de la Organización
5 - 6	probablemente impediría la operación efectiva de más de una parte de la Organización
3 – 4	probablemente impediría la operación efectiva de una parte de la Organización

1 – 2	pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1 - 2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[pd] persecución de delitos	
6 - 10	Impida la investigación de delitos graves o facilite su comisión
1 – 5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9 –10	RTO < 4 horas
7 – 8	4 horas < RTO < 1 día
4 – 6	1 día < RTO < 5 días
1 – 3	5 días < RTO

Fuente: (Magerit, 2012)

ANEXO N° 2

CATÁLOGO DE AMENAZAS POR ACTIVO Y DIMENSIÓN DE SEGURIDAD DE LA INFORMACIÓN

Tabla N° 39. Catálogo de amenazas por activo y dimensión se seguridad de la información

[N]	Desastres naturales			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[N.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[N.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[N.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I]	**De origen industrial**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[I.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.*]	Desastres	Desastres debidos a la actividad humana: explosiones,	[D] disponibilidad	[HW] equipos informáticos (hardware)

	industriales	derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas. Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.		[Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.3]	Contaminación mecánica	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.4]	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.5]	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	[D] disponibilidad	[SW] aplicaciones (software) [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.6]	Corte del suministro eléctrico	Cese de la alimentación de potencia	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información (electrónicos) [AUX] equipamiento auxiliar
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.8]	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	[D] disponibilidad	[COM] redes de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante,	[D] disponibilidad	[AUX] equipamiento auxiliar
[I.10]	Degradación de los	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	Media] soportes de información

	soportes de almacenamiento de la información			
[I.11]	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación	[C] confidencialidad	[HW] equipos informáticos (hardware) [Media] media [AUX] equipamiento auxiliar [L] instalaciones
[E]	**Errores y fallos no intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[E.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información
[E.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información
[E.3]	Errores de monitorización *(log)*	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad (trazabilidad)	[D.log] registros de actividad
[E.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad	[D.conf] datos de configuración
[E.7]	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.	[D] disponibilidad	[P] personal

		Acciones descoordinadas, errores por omisión, etc.		
[E.8]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	SW] aplicaciones (software)
[E.9]	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	[C] confidencialidad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[E.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[E.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	
[E.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[E.18]	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[D] disponibilidad	D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[E.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones

				[P] personal (revelación)
[E.20]	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[I] integridad [D] disponibilidad [C] confidencialidad	[SW] aplicaciones (software)
[E.21]	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	[I] integridad [D] disponibilidad	[SW] aplicaciones (software)
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes electrónicos [AUX] equipamiento auxiliar
[E.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	[S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[E.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[E.28]	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	[P] personal interno
[A]	**Ataques intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[A.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	[D.log] registros de actividad
[A.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [A] disponibilidad	[D.log] registros de actividad
[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios.	[C] confidencialidad [A] autenticidad [I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios

		Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.		[SW] aplicaciones (software) [COM] redes de comunicaciones
[A.6]	Abuso de privilegios de acceso	Cada usuario utiliza un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, puede ocasionar problemas.	[C] confidencialidad [I] integridad [D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[A.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	[SW] aplicaciones (software)
[A.9]	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.10]	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Conánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datosafectados.	[I] integridad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.	[C] confidencialidad	[COM] redes de comunicaciones

		A veces se denomina “monitorización de tráfico”.		
[A.13]	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	[I] integridad (trazabilidad)	S] servicios [D.log] registros de actividad
[A.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	[COM] redes de comunicaciones
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [Media] soportes de información [L] instalaciones
[A.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[A.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	[SW] aplicaciones (software)
[A.22]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	[HW] equipos [Media] soportes de información [AUX] equipamiento auxiliar
[A.24]	Denegación de	La carencia de recursos suficientes provoca la caída del sistema	[D] disponibilidad	[S] servicios

	servicio	cuando la carga de trabajo es desmesurada (saturación del equipo informático)		[HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[A.25]	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[A.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[A.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	[L] instalaciones
[A.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	[P] personal interno
[A.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	[P] personal interno
[A.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	[P] personal interno

Fuente: Elaboración propia, adecuado de (Magerit, 2012)

ANEXO N° 3

CUESTIONARIO PARA LA RECOPILACIÓN DE LA INFORMACIÓN PARA LA EVALUACIÓN DE LAS BRECHAS DE SEGURIDAD DE LA INFORMACIÓN

Tabla N° 40. Cuestionario para la evaluación de brechas de seguridad de la información

PREGUNTAS	SI	NO	COMENTARIOS
1. ¿Se lleva un registro detallado de los activos de información de la Unidad (inventario)?			
2. ¿El inventario de activos informáticos se encuentra actualizado?			
3. ¿Hay asignación de responsabilidades a los funcionarios sobre la custodia de los activos informáticos?			
4. ¿Existe un inventario de las configuraciones de los equipos (incluyendo componentes y software instalado)?			
5. ¿Se lleva control de licencias de software y sus costos de licenciamiento (en caso necesario)?			
6. ¿Se han identificado los activos o servicios más críticos para el cumplimiento de los objetivos del Área?			
7. ¿Se tiene un procedimiento para identificar amenazas?			
8. ¿se identifican los activos afectados por amenazas?			
9. ¿Cuenta con una escala de valoración de amenazas?			
10. ¿Se calcula la probabilidad de ocurrencia de las amenazas?			
11. ¿La oficina cuenta con un manual de políticas con respecto a amenazas?			
12. ¿Se encuentran documentados las políticas y procedimientos respecto a amenazas?			
13. ¿Se lleva un registro de las amenazas ocurridas?			
14. ¿Se tiene un procedimiento para identificar vulnerabilidades?			
15. ¿se identifican los activos afectados por vulnerabilidades?			
16. ¿Cuenta con una escala de valoración de vulnerabilidades?			
17. ¿La oficina cuenta con un manual de políticas con respecto a vulnerabilidades?			
18. ¿Se encuentran documentados las políticas y procedimientos respecto a vulnerabilidades?			
19. ¿Se lleva un registro de las vulnerabilidades detectadas?			
20. ¿Existe algún mecanismo que determine la magnitud del impacto?			
21. ¿Se cuenta con una escala de			

valorización de impactos?			
22. ¿Se han identificado los riesgos de TI asociados a la gestión y operación de la plataforma informática del Área?			
23. ¿Se han identificado los riesgos asociados a los recursos más críticos?			
24. ¿Se estiman los niveles necesarios de exposición al riesgo?			
25. ¿Se clasifican los riesgos según su criticidad?			
26. ¿Se han establecido controles para mitigar los riesgos de los recursos de información más críticos?			
27. ¿Se tienen definidas las estrategias de cómo implementar los controles?			
28. ¿Cuentan con procedimientos para identificar controles?			
29. ¿El Área cuenta con un manual de políticas, procedimientos y normativa relacionada a la seguridad de información?			
30. ¿El Área cuenta con un manual de políticas, procedimientos y normativa relacionada a la gestión de riesgos?			
31. ¿Se ha establecido un mecanismo para la atención y registro de incidentes?			
32. ¿Se utilizan claves seguras de acceso?			
33. ¿Se llevan a cabo políticas en lo referente a gestión de cuentas de usuario?			
34. ¿Se eliminan los derechos de acceso a funcionarios inactivos o que han dejado de laborar para la Unidad?			
35. ¿Se revisan periódicamente los registros de acceso a los sistemas?			
36. ¿La carga de los extintores de incendio se encuentra vigente?			
37. ¿Se conoce el mecanismo de operación de los diversos tipos de extintores de incendio?			
38. ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal del Área o por motivo de reparación?			
39. ¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?			
40. ¿Se ha establecido una política de respaldos periódicos de la información en la Unidad?			
41. ¿La oficina cuenta con el personal y cantidad adecuada para la realización de las funciones?			
42. ¿El área se encuentra en un ambiente adecuado para la realización de sus funciones?			
43. ¿Se tienen identificados los servicios requeridos por la función de TI?			

44. ¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados?			
45. ¿Se lleva el control de la vida útil de los activos de información?			
46. ¿Se mantiene un registro auxiliar de los activos informáticos en desuso?			
47. ¿Se lleva control de los componentes recuperables de los activos en desuso (discos duros, memoria, tarjetas de video, etc)?			
48. ¿Se sigue algún procedimiento para borrar la información de los discos duros u otras unidades de almacenamiento, antes de su desecho?			
49. ¿Se mantiene un control de la salida de activos por parte de terceros?			

Fuente: Elaboración propia

ANEXO N° 4

RESULTADOS DEL ANÁLISIS DE RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMATICA

En el siguiente formato contiene el resumen del análisis y evaluación de los posibles riesgos relacionados con Tecnología de la Información que afectan directamente los activos tecnológicos.

I. SERVIDORES Y CONCENTRADORES CENTRALES

Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Servidores y concentradores centrales y de borde	Acceso no autorizado		
	Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje		
	Destrucción o fallo de un componente crítico del equipo (microprocesador, memoria, fuente de poder, otros)		
	Errores de configuración		
	Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento racks, otros)		
	Límite de vida útil – Máquinas obsoletas (antigüedad del equipo, repotenciamiento de componentes)		
	Mantenimiento		
	Robo		
	Afectación por virus		

II. BASE DE DATOS

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Base de Datos	Copia no autorizada de o a un medio de datos externos		
	Errores de software (motor y contenedor de base de datos)		
	Falta de espacio de almacenamiento		
	Pérdida o falla de backups		
	Pérdida de confidencialidad en datos privados y de sistema		
	Directorios compartidos		
	Sabotaje		
	Afectación de virus		

III. SOFTWARE DE OFIMÁTICA (SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS)

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Software de BackOffice y sistemas operativos instalados en servidores y terminales	Aplicaciones sin licencias		
	Error de configuración		
	Mala Administración de control de accesos		
	Pérdida de datos		
	Afectación de virus		

IV. BACKUP (SISTEMA DE RESPALDO DE INFORMACIÓN)

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Backup de información	Procedimientos inexistentes o mal diseñados para generación de respaldo de la BD, aplicaciones y documentación		
	Acceso no autorizado a las copias de respaldo		
	Resguardo seguro de las copias de respaldo de la BD, aplicaciones y documentación		
	Falta de pruebas de recuperación (Restore) y puesta en producción de las copias de resplado		
	Mal etiquetado de las copias de respaldo		

V. CABLEADO Y CONCENTRADORES

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Cableado y concentradores	Conexión de cables inadmisible (modificación de conexiones y mal etiquetado)		
	Daño o destrucción, de cables o equipamiento, inadvertido (mala ubicación, por limpieza, impedimento de libre tránsito, otros)		
	Factores ambientales		
	Accesos no autorizados.		
	Longitud de los cables de red excedidos a las normas		

VI. RED DE COMPUTADORAS

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Red de computadoras	Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)		
	Configuración inadecuada de componentes de red		
	Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros)		
	Mal uso de servicios de red (mal uso del netmeeting, transmisión de datos, otros)		

VII. USUARIOS

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Usuarios	Acceso no autorizado a datos		
	Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida		
	Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)		
	Destrucción negligente de datos por parte de los usuarios		
	Documentación deficiente (manual de usuario)		
	Entrada sin autorización a ambientes		
	Entrenamiento de usuarios inadecuado		
	Falta de controles y log de las transacciones realizadas por los usuarios.		
	No cumplimiento con las medidas de seguridad del sistema		

VIII. DOCUMENTACIÓN DE LOS SISTEMAS EN PRODUCCIÓN

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Documentación de programas, hardware, procedimientos administrativos locales, manuales, etc.	Acceso no autorizado a datos de documentación		
	Borrado, modificación o revelación desautorizada de información		
	Copia no autorizada de un medio de documentación del sistema		
	Descripción de archivos y programas inadecuado		
	Documentación insuficiente o faltante, en relación a seguridad de la información		
	Mantenimiento y actualización inadecuado o ausente de la documentación		

IX. SISTEMAS O APLICACIONES INFORMÁTICAS EN PRODUCCIÓN

Nombre del Activo	Factor de Riesgo	¿Se protege?	¿Cómo? / Por qué?
Sistemas y aplicaciones informáticas en producción	Modificaciones inoportunas y no documentadas		
	Funcionalidad del sistema (no atiende todos los requerimientos de los usuarios y áreas)		
	Acceso a los programas fuentes no controlado		
	Validación en los procesos de captura y registro de transacciones		

Bach. JHOELY MAILIS TAPIA CARRILLO

Bach. JOSUE LUIS VIDAL CASTILLO

Dr. Ing. ERNESTO KARLO CELI ARÉVALO

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

"Año de la universalización de la salud".

CONSTANCIA DE APROBACION DE ORIGINALIDAD DE TESIS

Según Res. N° 659-2020-R

Yo, **ERNESTO KARLO CELI ARÉVALO**, asesor de tesis de los bachilleres:

JHOELY MAIUS TAPIA CARRILLO

JOSUE LUIS VIDAL CASTILLO

TITULADA:

La seguridad de la información y su relación con la gestión de los riesgos de negocio en las empresas agroindustriales azucareras

Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de 13% verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Se expide la presente según lo dispuesto en la Resolución Nº 659-2020-R, de fecha 08 de setiembre de 2020, que aprueba la Directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la Universidad Nacional Pedro Ruiz Gallo.

Lambayeque, 11 de mayo del 2021

Atentamente,

Dr. Ing. Ernesto Karlo Celi Arévalo
DNI. 18068078

Se adjunta:
Recibo digital de Turnitin
Revisión de informe en Turnitin

Informe final de tesis

INFORME DE ORIGINALIDAD

13%	12%	2%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	procesoelaboraciondeazucar.blogspot.com Fuente de Internet	1%
2	Submitted to Universidad Nacional Pedro Ruiz Gallo Trabajo del estudiante	1%
3	grupobonanza.blogspot.com Fuente de Internet	1%
4	www.producearequipa.gob.pe Fuente de Internet	<1%
5	anfacal.org Fuente de Internet	<1%
6	inba.info Fuente de Internet	<1%
7	repositorio.unab.cl Fuente de Internet	<1%
8	oa.upm.es Fuente de Internet	<1%

93	www.javanicaragua.org Fuente de Internet	<1 %
94	www.webyempresas.com Fuente de Internet	<1 %
95	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		

Dr. Ernesto Celi Arévalo

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Jhoely Tapia & Josue Vidal
Título del ejercicio:	Informes final tesis
Título de la entrega:	Informe final de tesis
Nombre del archivo:	DesarrolloTesis.docx
Tamaño del archivo:	3.44M
Total páginas:	178
Total de palabras:	47,111
Total de caracteres:	254,921
Fecha de entrega:	11-may-2021 07:57a.m. (UTC-0500)
Identificador de la entre...	1583548014

Universidad Nacional Pedro Ruiz Gallo

Dr. Ernesto Celi