ANÁLISIS DE RIESGOS SEGÚN LA NORMA ISO 27001:2013 PARA LAS AULAS VIRTUALES DE LA UNIVERSIDAD SANTO TOMÁS MODALIDAD PRESENCIAL

VIVIAN ANDREA GARCIA BALAGUERA
JHON JARBY ORTIZ GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
2017

ANÁLISIS DE RIESGOS SEGÚN LA NORMA ISO 27001:2013 PARA LAS AULAS VIRTUALES DE LA UNIVERSIDAD SANTO TOMÁS MODALIDAD PRESENCIAL

VIVIAN ANDREA GARCIA BALAGUERA
JHON JARBY ORTIZ GONZALEZ

Ing. SALOMÓN GONZÁLEZ GARCÍA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C 3 de abril de 2017

DEDICATORIA

Dedicamos esta tesis a Dios quien hace todo posible; a nuestra hijita Vivian que con sus 4 años nos ha comprendido y nos ha dado el tiempo para poder culminar este proyecto.

A nuestras familias que con su apoyo nos animaron a continuar con este proceso

AGRADECIMIENTOS

Al personal del departamento de TIC dela universidad quien presto todo apoyo para el desarrollo de este trabajo

TABLA DE CONTENIDO

Pág.

INDICE DE TABLAS

TABLA DE FIGURAS

Pág.

TABLA DE GRAFICAS

LISTA DE ANEXOS

TÍTULO ANÁLISIS DE RIESGOS SEGÚN LA NORMA ISO 27001 PARA LAS AULAS VIRTUALES DE LA UNIVERSIDAD SANTO TOMAS MODALIDAD PRESENCIAL

INTRODUCCIÓN

El presente trabajo consistió en realizar un análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial, el uso de estas por la comunidad educativa, es una política institucional obligatoria para los docentes de Tiempo Completo (TC) y Medio Tiempo (MT), al volverse una política el uso de las Aulas virtuales, el uso de éstas aumenta por parte de docentes y estudiantes y la posibilidad de un ataque informáticos se convierte en un peligro eminente.

El evaluar la seguridad y el control de información de las aulas virtuales es muy importante, puesto que en esta se registran notas y trabajos de los estudiantes, y material de producción intelectual de los docentes, la perdida de en esta información, generaría problemas instituciones, que le generarían perdida económicas a la universidad; la verificación de que si cumplen y aplican los controles, políticas de acuerdo a la norma ISO 27001: 2013, contribuye a la estabilidad académica en la instrucción.

1.PLANTEAMIENTO DEL PROBLEMA

La universidad Santo Tomás en la actualidad, ha incorporado el uso de las aulas virtuales en la modalidad presencial, como una política institucional obligatoria para los docentes de Tiempo Completo (TC) y Medio Tiempo (MT), estas son administradas por la oficina de educación virtual. El problema radica que al volverse una política el uso de las Aulas virtuales, el uso de éstas aumenta por parte de docentes y estudiantes y la posibilidad de un ataque informáticos se convierte en un peligro eminente.

Surge la necesita evaluar la seguridad y el control de información de las aulas virtuales cumple y aplican los controles, políticas de acuerdo a la norma ISO 27001: 2013, puesto que en esta se registran notas y trabajos de los estudiantes, y material de producción intelectual de los docentes por tanto se debe verificar si se mantiene, con el fin de tener la certificación de su SGSI(Sistema de Gestión de Seguridad de la información) que demuestre que la información de las aulas virtuales se rige tres principios básicos que dictamina el estándar internacional los cuales son: la confidencialidad, integridad, disponibilidad, demostrando que se aplican las mejores prácticas, en cuanto al manejo de información de las Aulas virtuales generando tranquilidad Institucional, tanto a los docentes y estudiantes al usar estas.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis de riesgos según la norma ISO 2700: 2013 ayudará a la Seguridad en las Aulas Virtuales de la Universidad Santo Tomás?

2. JUSTIFICACIÓN DEL PROYECTO

La seguridad de la información, según ISO 27001: 2013, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. el realizar un Diagnóstico del SGSI en las aulas Virtuales de la Universidad Santo Tomás, es de importante puesto que en estas, se guarda información de docentes como cuestionarios, material didáctico de la autoría de éste, registro de notas de estudiantes y trabajos propuesto por el y los estudiantes en la plataforma desarrollan trabajos, y lo suben a esta; si esta plataforma fuera víctima de un ataqué informático ocasionaría un problema académico en el semestre que generaría caos académico en la universidad entre docentes y estudiantes.

Por tanto el propósito del diagnóstico del sistema de gestión de la seguridad de la información es, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la Universidad de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías y de esta forma garantizar la preservación de su confidencialidad, integridad y disponibilidad de la información que se encuentra en las Aulas virtuales, y así evitar y prevenir problemas por perdidas, copiado o cambio de información.

Con este trabajo se benefició a los estudiantes y docentes de la universidad Santo Tomás, porque se genera confianza en el uso de los sistemas de información.

3. OBJETIVOS

3.1 GENERAL

Determinar los riesgos de Seguridad Mediante la aplicación de una auditoría según la norma ISO 27001 en las Aulas Virtuales De La Universidad Santo Tomás.

3.2 OBJETIVOS ESPECÍFICOS

- Elaborar un plan de Auditoría según la norma ISO 27001.
- Realizar un diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás en relación con la norma ISO 27001.
- Elaborar el informe final de los resultados para establecer el plan de mejoramiento de la seguridad según los requerimientos de la norma ISO 27001 para mejorar el desempeño de la organización.

4.MARCO DE REFRENCIA

4.1 MARCO TEÓRICO

4.1.1 Antecedentes

Al buscar antecedentes en el contexto mundial y nacional sobre análisis de riesgo según la norma ISO 27001 de aulas virtuales modalidad presencial, no se encontraron investigaciones específicas en la temática, pero se encontró 5 trabajos de investigación sobre evaluación de evaluación de riesgos a continuación se relacionan:

La primera consistió en evaluar la técnica de seguridad del data center del municipio de Quito según las normas ISO/IEC 27001: 2005 SGSIE ISO IEC 27002: 2005[1], la investigación documental – descriptiva realizó la evaluación técnica informática para determinar el cumplimiento de las normas y estándares internacionales que establecen un GAP de la gestión de seguridad de la información, según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 270021005. Para esto la recolección de la información se emplearon técnicas de investigación de campo de fuentes primarias, como son la observancia y entrevista; y secundarias como son documentos y libros dicha información se analizó y evaluó, para determinar el cumplimiento o no de los lineamientos según las norma ISO/IEC 27002:2005; este trabajo de investigación se realizó con el fin de identificar vulnerabilidades de seguridad en el de todos los elementos que se encuentran en Data Center y recomendar se establezcan políticas de seguridad de la información y se implemente controles para el manejo de riesgos, monitoreo y revisión del desempeño y efectividad del Data Center, considerando el mejoramiento continuo de la seguridad.

La segunda Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa[2] esta investigación se aborda el tema relacionado con la seguridad informática, haciendo énfasis en el análisis de la norma ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission)27001 y su puesta en práctica en una empresa. En primer lugar se realizó un estudio de la seguridad informática. Después se realizó una caracterización general de las normas ISO/IEC 27000, profundizando en la ISO/IEC

[1] D. Aguirre and j. Palacio, Evaluación Técnica De Seguridades Del Data Center Del Municipio De Quito Según Las Normas Iso/Iec 27001:2005 Sgsie Iso/Iec 27002:2005, Quito: Universidad De Fuerzas Armadas Espe Maestría De Evaluación Y Auditoria De Sistemas Tecnológicos, 2014.

[2] C. Sandoval, Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una, Guayaquil: Universidad Católica Santiago de Guayaquil Maestría en Telecomunicaciones, 2014.

27001 que abarca lo concerniente a las técnicas de seguridad, los Sistemas de Gestión de Seguridad de la Información y los requerimientos a tener en cuenta. Por último, se implementa el Plan de Seguridad Informática de la empresa, con los análisis de riesgos, basado en el estándar mencionado. Este trabajo se desarrolló teniendo en cuenta la necesidad de que la seguridad en la empresa cumpla cabalmente con los parámetros internacionales establecidos, contribuyendo así al mejoramiento de la misma y al propósito de obtener su certificación.

La tercera Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca (IUCMC)[3] investigación aplicada que consistió en implementar la metodología MAGERIT para el análisis de riesgo con el fin de garantizar la seguridad de los activos de información y el normal funcionamiento interno de la IUCMC. Con el fin de conocer de manera global el estado actual de la seguridad informática dentro de la IUCMC. Los controles y políticas de seguridad de la información resultado de este análisis de riesgos pueden ser tomados como soporte para la implementación del SGSI; encaminado a: Reducir el ambiente de riesgo vigente. La IUCMC actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de las directivas (alta gerencia) y de todo el personal es posible contrarresta.

La cuarta Modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408 COMMON CRITERIA[4]. en la investigación se realizó un análisis de riesgo a un conjunto de sistemas software seleccionados de acuerdo a los requerimientos de ley en Colombia, con el fin de determinar qué tan distantes están del cumplimiento del estándar ISO/IEC 15304 y sus falencias generales en seguridad. El resultado no fue bueno, y refleja la falta de documentación y detalle en las funciones de seguridad del software que se desarrolla en las empresas seleccionadas y la no prevención de incidentes de seguridad ante las amenazas reales de un ambiente de producción.

Finalmente la investigación del Diseño de una Política de Gestión de Riesgos de la Información para La Dependencia de Admisiones Registro y Control de Universidad

[3] J. Perafán and M. Caicedo, Análisis de Riesgos de la Seguridad de la Información para la Institución, Popayán: Universidad Nacional Abierta y a Distancia Especialización en Seguridad Informática, 2014.

[4] A. Chamorro, MODELO PARA LA EVALUACION EN SEGURIDAD INFORMÁTICA A PRODUCTOS SOFTWARE, BASADO EN EL ESTÁNDAR ISO/IEC 15408 COMMON CRITERIA, Cali: Universidad ICESI Maestría en Gestión de Informática y Telecomunicaciones, 2012.

Francisco de Paula Santander Ocaña[5] esta propone una política de gestión de riesgos de la información para la oficina de admisiones registro y control de la universidad francisco de paula Santander Ocaña; se sustenta en el marco de trabajo de ISO/IEC 31000/ 2009 y en la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT. El trabajo está enfocado en la gestión de riesgos de la información, y se involucran conceptos relacionados con seguridad de la información que consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

4.1. 2. La seguridad Informática y la Seguridad de La Información

La Seguridad Informática (IT Security) es la distinción táctica y operacional de la Seguridad, es decir, Es la forma como se detallan las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos[6].

Es decir, es la disciplina que nos habla de los riesgos, amenazas de los esquemas normativos para minimizar los riesgos en el manejo de los activos, es decir esta se encarga de proporcionar evaluar los riesgos y las amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo normativa o buenas practicas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad en el manejo de la información (activos)[7].

Esta se encarga de llevar a cabo las soluciones técnicas de protección de la información (los activos), mientras que, la Seguridad de la Información (Information Security) se encarga de proporcionar evaluar el riesgo y las amenazas, trazar el plan de acción y adecuación para minimizar los riesgos.

---

[5] Y. Osorio and Y. Pérez, Diseño de una Política de Gestión de Riesgos de la Información, Ocaña: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA Especialización en Auditoria de Sistemas., 2012.

[6] CANO,j. "La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes," ISACA Journal Online, vol. 5, 2011

[7] Ibid.,p.85

Los atributos de seguridad de la información son:

Confidencialidad: La información se revela únicamente si así está estipulado, a personas, procesos o entidades autorizadas y en el momento autorizado.

Integridad: La información es precisa, coherente y completa desde su creación hasta su destrucción.

Disponibilidad: La información es accedida por las personas o sistemas autorizados en el momento y en el medio que se requiere.

Figura 1 Los atributos de seguridad de la información son

Fuente Autores

4.1.3 Sistema de Gestión de Seguridad Informática y de la Información

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System[8].

Un Sistema de gestión de la seguridad de la información (SGS)[9] se puede definir como, un sistema que se encarga de proveer los mecanismos y herramientas, basados en la norma ISO 27001, para la preservación de la información, con

[8] WWW.ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, Madrid, 2012.
[9] ICONTEC, Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, Bogotá, 2009.

respecto a su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización, cuyo objetivo es conocer en una institución, a lo que puede estar expuesta la información, establece como se deben gestionar los riesgos , necesarios para lograr los objetivos de la organización

La norma internacional UNE/ISO 27001, establece las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). Esta norma establece un enfoque por procesos basado en el ciclo Deming, que plantea la gestión de la seguridad como un proceso de mejora continua, a partir de la repetición cíclica de cuatro fases como lo son planificar, hacer, verificar y actuar.[10].

Dentro de las especificaciones de la norma se establece un esquema documental del SGSI, que debe mantenerse actualizado, disponible y enmarcado en un índice, especialmente si la empresa desea superar un proceso de certificación, tal como lo describe un proceso de implantación de un SGSI[11]

4.1.4 Auditoria de la gestión de seguridad de la Información

Existen múltiples definiciones en términos generales sobre auditoria, por lo que se escogieron las definiciones consideradas como más generales y completas:

Para AMERICAN ACCOUNTING ASSOCIATION[12] citado por [13] "La Auditoría es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso".

Para Poter[14] citado por[15], la Auditoría es el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de

[10] WWW.ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, Madrid, 2012.
[11] M. AVILA ARZUZA, Implantación de un SGSI, Barcelona: Universitat Oberta de Catalunya, 2012.
[12] AMERICAN ACCOUNTING ASSOCIATION, Auditing Concepts Committee. Reports of the Committee on Basis Concepts, vol. 47, 1972.
[13] G. Mejía and A. Cuéllar, "Teoría General de la Auditoría y Revisoría Fiscal," 2003. [Online]. Available: http://fccea.unicauca.edu.co/old/tgarf/. [Accessed Marzo 2016].
[14] T. Poter and W. Burton, Auditoría un enfoque conceptual, México: Limusa, 1993.
[15] G. Mejía and A. Cuéllar, "Teoría General de la Auditoría y Revisoría Fiscal," 2003. [Online]. Available: http://fccea.unicauca.edu.co/old/tgarf/. [Accessed Marzo 2016

establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario.

Mejía [16] la define como “El proceso que consiste en el examen crítico, sistemático y representativo del sistema de información de una empresa o parte de ella, realizado con independencia y utilizando técnicas determinadas, con el propósito de emitir una opinión profesional sobre la misma, que permitan la adecuada toma de decisiones y brindar recomendaciones que mejoren el sistema examinado.”

Para fines de la gestión de seguridad de la información, se puede definir una auditoría como un proceso independiente, documentado y, sistemático mediante uso de técnicas y herramientas, cuyo objetivo principal es la emisión de un diagnóstico sobre un sistema de información, que permita tomar decisiones y brindar recomendaciones de mejora sobre el mismo.

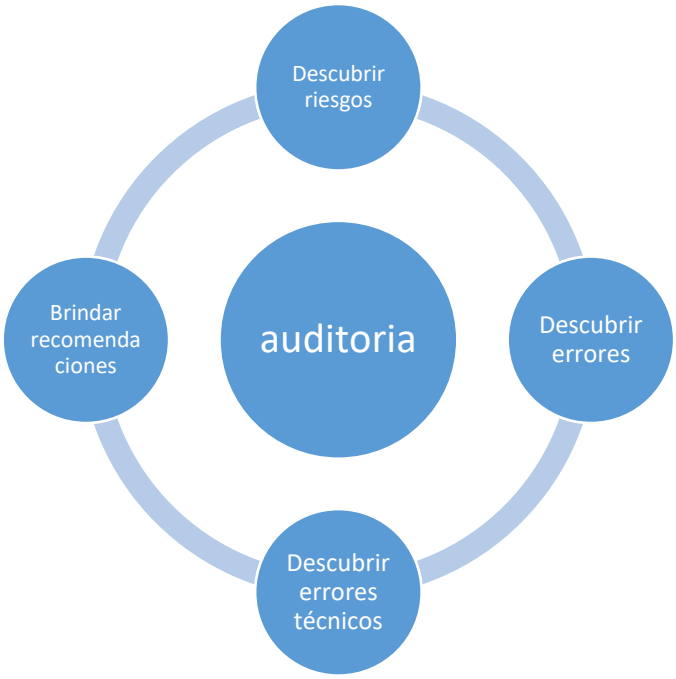
Se puede establecer como los objetivos que persigue la auditoria[17]

- Descubrir riesgos y amenazas de la información
- Descubrir errores de principio
- Descubrir errores técnicos
- Brindar recomendaciones que mejoren el sistema examinado

Figura 2 Objetivos que persigue la auditoria

[16] Ibid.,p.34

[17] G. Mejía and A. Cuéllar, "Teoría General de la Auditoría y Revisoría Fiscal," 2003. [Online]. Available: http://fccea.unicauca.edu.co/old/tgarf/. [Accessed Marzo 2016].



Fuente Autores

4.1.5 Análisis de Riesgos de la Información

Para nadie es un secreto que desde hace varias décadas la información se ha convertido en el Activo con más valor de una organización, pasando por el ciclo continuo de ser insumo de alto valor, convirtiéndose en producto del desarrollo de las actividades, o viceversa, siendo esta fundamental para el cumplimiento de los objetivos y subsistencia de las organizaciones.

Gracias al avance vertiginoso de la tecnología, con el objeto de brindar eficiencia y agilizar la administración y los procesos, se incorporan sistemas automatizados de procesamiento de información. Las organizaciones se ven expuestas a una serie de peligros, que se han incrementado por las nuevas amenazas surgidas por uso de las tecnologías de la información y las comunicaciones[18].

Es por esto que es de gran importancia contar con métodos para determinar, analizar, valorar y clasificar los riesgos, para poder implementar mecanismos que permitan controlarlos y minimizarlos.

La gestión de riesgos es una actividad para salvaguardar los activos de información de una organización. Es un proceso que debe ser constante, para minimizar los

[18] Universidad Nacional de Luján, "seguridad informática," [Online]. Available: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf. [Accessed Marzo 2016].

costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, aplicando medidas de protección sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables para la misma.[19]

El proceso de gestión de riesgos involucra cuatro actividades cíclicas:

• La identificación de activos y los riesgos a los que están expuestos

• El análisis de los riesgos identificados para cada activo

• La selección e implantación de controles que reduzcan los riesgos.

• El seguimiento, medición y mejora de las medidas implementadas.

Figura 3 El proceso de gestión de riesgos involucra cuatro actividades cíclicas

Fuente Autores

4.2 MARCO CONCEPTUAL

- **Activo: (inglés: Asset).** En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la

[19] Ibid.,p.5

misma que tenga valor para la organización. Según ISO/IEC 13335-1:2004[20] Cualquier cosa que tiene valor para la organización.

- **Amenaza**: Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema u organización Según ISO/IEC 27002:2005[21]
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas Según ISO/IEC 27002:2005[22]
- **Impacto**: cambio adverso a los objetivos del negocio esperados Según ISO/IEC 27005:2008[23]
- **Riesgo de Seguridad de la Información:** ISO/IEC 27005:2008[24] El potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a la organización.
- **Control**: Segú la ISO/IEC 27002:2005 es el medio para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
- **Riesgo aceptable**: Riesgo en un nivel con el cual la organización se siente cómoda ISO/IEC 27001:2005 [25]
- **Riesgo residual**: Riesgo remanente después del tratamiento del riesgo ISO/IEC 27001:2005[17]
- **ISO: Organización Internacional de Normalización**, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.[17]

---

[20] ISO, ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management, 2004.
[21] ISO, ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management, 2005.
[22] Ibid.,p.2
[23] ISO, ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management, 2008.
[24] ISO, ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management, 2008.
[25] ISO, ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements, 2005.

4.3 MARCO LEGAL

Ley 527 de 1999: Por medio de esta ley se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación[26].

Ley 1581 de 2012: La ley de protección de datos personales, complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.[27]

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones[28].

Ley 1273 de 2009: se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos, añade dos nuevos capítulos al Código Penal: Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver, esta Ley está relacionada a la ISO27000[29].

Ley 1341 Del 30 De Julio De 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones[30].

---

[26] E. C. d. Colombia, "alcaldiabogot," 1999. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276. [Accessed 2016].

[27] EL CONGRESO DE COLOMBIA, "alcaldiabogotá," 2012. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Accessed 2016].

[28] El CONGRESO DE LA REPUBlICA, "Superintndencia de Industria y Comercio," 2008. [Online]. Available: http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf. [Accessed 2016].

[29] EL CONGRESO DE COLOMBIA, "Alcaldia Bogotá," 2009. [Online]. Available: http://www.alcaldiabogota.gov.222co/sisjur/normas/Norma1.jsp?i=34492. [Accessed 2016].

[30] EL CONGRESO DE COLOMBIA, "Alcaldia Bogotá," 2009. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913. [Accessed 2016].

5. MARCO METODOLÓGICO

5.1 METODOLOGÍA DE INVESTIGACIÓN

Para la realización de este proyecto, se realizó una Investigación Aplicada según Sampieri[31] la investigación aplicada recibe el nombre de "investigación práctica o empírica", que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad. Está orientada a orientados a resolver problemas de la vida cotidiana o a controlar situaciones prácticas.

Al aplicar este tipo de investigación se busca resolver el problema de identificar y mitigar los riesgos informáticos que se pueden presentar o que se están presentando en las aulas virtuales de la USTA, tratando y de dar una solución a la problemática identificada.

5.2 METODOLOGÍA DE DESARROLLO

Los pasos que se implementaron para desarrollar el trabajo propuesto

Análisis fuentes teóricas:

se consultarán diversas fuentes con relación al análisis de riesgos en la seguridad informática y se decidió la norma ISO 27001 para análisis de riesgos

Definición de los objetivos del proyecto y delimitación del alcance de acuerdo al problema planteado:

Se elaboró el plan de auditoria que se presenta en el anexo 1 y el 14 de octubre de 2016 se implementó con el fin de hacer el diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás en relación con la norma ISO 27001.

[31] R. Sampieri, C. Fernandez and P. Baptista, Metodología de la invetigación, Mexico: Mc Graw Hill, 2015.

Diagnóstico de la situación actual

En esta etapa se desarrollarán las siguientes actividades:

- Levantamiento de información e identificación de los activos de información que componen el proceso alcance del sistema SGSI, a través de la aplicación de metodologías que contemplen entrevistas y formatos.

Análisis de Activos

Los Activos de Información, es la base principal de la entidad y con el fin de facilitar el manejo y mantenimiento del inventario los activos se clasifican en la tabla1 la siguiente forma:

Tabla 1 Análisis de las aulas Virtuales activos

COD	TIPO DE ACTIVO	ACTIVOS	DESCRIPCIÓN
D100	[D] Datos / Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.	El plantel educativo Santo Tomás maneja cualquier tipo de datos en diferentes formatos, que son distribuidos a todo el personal, pero con algunas restricciones.
SI100	[SI] Sistema de Información	aplicaciones PHP	Moodle
SI200	[SI] Sistema de Información	Correo electrónico	Servicio corporativo Gmail
SI300	[SW] Software / Aplicativos	Servidores WEB	Apache
SW100	[SW] Software / Aplicativos	Motor de Base de Datos	Mysql.
SW200	[SW] Software / Aplicativos	Antivirus y anti espías	Software para evitar programas que alteren el correcto funcionamiento de las pc's y servidores, y que prohíban el ingreso de códigos que puedan espiar las actividades de un equipo de la organización
SW300	[SW] Software / Aplicativos	Cortafuegos	Hardware y software que permite la administración de permisos de usuarios a través de las redes de la organización

Tabla 1. (continuación)

COD	TIPO DE ACTIVO	ACTIVOS	DESCRIPCIÓN
HW100	[HW] Hardware / Equipos informáticos	Estaciones de trabajo	Pc's asignados a Docentes, estudiantes, directivos, Operadores de centro de cómputo, Ingenieros Administradores de redes e Infraestructura.
HW200	[HW] Hardware / Equipos informáticos	Servidores de alto desempeño tipo Blade	arquitectura de alta disponibilidad a nivel de hardware y soportados por un chasis que brinda aprovechamiento del recurso
HW300	[HW] Hardware / Equipos informáticos	Unidades LUM presentadas desde datastore o sistema de almacenamiento DELL EQL.	almacenamiento de alta densidad y velocidades de consulta, permiten una atención ágil del servicio, estos servidores están interconectados con redes internas dedicadas de alta velocidad que garantizan la trasmisión de información.
M100	[M] Soportes de información	Respaldos en cinta	Respaldos de información de las bases de datos
COM100	[COM] Redes de comunicaciones	recursos de conectividad interna	Que permite extender el servicio a redes públicas, dichas conexiones superan los 140 Mbps dedicados hacia Internet y 100 Mbps dedicados a cada una de las sedes.
COM200	[COM] Redes de comunicaciones	recursos de conectividad externa	Únicamente la colectividad fuera de las instalaciones de la sede principal es contratada con un ISP, es decir conexiones de datos MPLS y servicios de Internet.
P100	[P] Personal	Personal los ingenieros competentes para la gestión de los recursos de TI.	Personal humano que labora en la institución y desempeñan funciones que están implicadas dentro del entorno
P200	[P] Personal	Administrativo de las aulas virtuales	Personal humano que labora en la institución y desempeñan funciones administrativas
P200	[P] Personal	Docentes	Personal humano que labora en la institución y desempeñan funciones docentes
P200	[P] Personal	Estudiantes	Estudiantes de la institución
L100	[L] Instalaciones	Instalaciones Servidores	Lugares donde se hospedan los sistemas de información y comunicaciones.
L100	[L] Instalaciones	Instalaciones Estaciones de trabajo	Lugares donde se hospedan los sistemas de información y comunicaciones.
L100	[L] Instalaciones	Instalaciones Copias de seguridad	Lugares donde se hospedan los sistemas de información y comunicaciones.
S100	[S] Servicios	Gestión aulas virtuales	Función que satisface una necesidad de los usuarios de las aulas virtuales como la gestión de cursos y usuarios
S200	[S] Servicios	Capacitación	Función que satisface una necesidad de los usuarios de las aulas virtuales como la gestión de cursos y usuarios

Tabla 1. (continuación)

COD	TIPO DE ACTIVO	ACTIVOS	DESCRIPCIÓN
S300	[S] Servicios	Asesoría	Asesoría a estudiantes y docentes

Fuente autores

Posteriormente en la tabla 2, se presenta revisión y análisis de las políticas de seguridad del departamento de TIC de la universidad santo Tomás.

A continuación, se describe la información y documentación solicitada a la unidad de informática y telemática y suministrada por ellos:

Tabla 2 Estado actual de revisión y análisis de las políticas de seguridad del departamento de TIC de la universidad Santo Tomás.

(Convenciones: C - Cumple; NC - No Cumple; NA - No Aplica; EP-En Proceso)

DOCUMENTO	DESCRIPCION	C	NC	NA	EN
Políticas de seguridad	Documento donde se plantea toda la normativa que deben seguir los funcionarios de la Unidad. El documento debe considerar aspectos generales y específicos sobre acceso a la información, responsabilidad y manejo de activos de información, procedimientos a seguir cuando se presente un incidente de seguridad. Nota: El Departamento de TIC un documento de políticas de seguridad y controles. Pero está en construcción porque no tiene aprobación oficial				x
Manual de funciones y competencias laborales	La unidad facilitó el manual en el que se detallan las funciones esenciales de cada funcionario, desde el director hasta el último empleado y los resultados o criterios de desempeño esperados para cada cargo, pero está en construcción				x
Procesos y procedimientos	La unidad proporcionó una serie de documentos que contienen diagramas de flujo, los cuales describen las actividades y su secuencia requerida en la realización de los procedimientos de la unidad. Además, incluyen objetivo, alcance y responsables que intervienen en el procedimiento.	x			
	Publicación de información en la página web institucional.	x			

Tabla 2. (continuación)

DOCUMENTO	DESCRIPCION	C	NC	NA	EN
	Distribución de espacios físicos Aula de Informática.	x			
	Plan de mantenimiento preventivo de equipo de cómputo, ofimática y telecomunicaciones.	x			
	Servicio de mantenimiento correctivo y preventivo de hardware y software.	x			
	Desarrollo de cursos de lenguaje y herramientas informáticas	x			
	Administración Bases de Datos.	x			
	Cableado estructurado	x			
Inventario de activos	Cada administrador de la unidad suministró un inventario de su área de responsabilidad, en el que se recopilan los principales activos del área por medio de los cuales es posible la prestación de los servicios.	x			
Portafolio de servicios	No se cuenta con la página web del departamento de TIC, esta está en construcción.	x			
Registro de problemas e incidentes	Información detallada acerca de un incidente, junto con su historial desde su registro hasta su resolución. Nota: El departamento de TIC cuenta con documentos de registros de incidencias y problemas. Se proporcionó un conjunto de formatos que administran los empleados de la unidad dependiendo de sus funciones y responsabilidades. Los principales formatos son los siguientes:	x			
	Registro de capacitación Portal Web.	x			
	Información publicada en el Portal Web.	x			
	Formato para mantenimiento de equipos.	x			
	Préstamo de quipos.	x			

Tabla 2. (continuación)

DOCUMENTO	DESCRIPCION	C	NC	NA	EN
	Redes y telecomunicaciones.	x			
	Mantenimiento preventivo dependencias.	x			
	Hoja de vida equipo.	x			
	Servicios RENATA.	x			
	Mantenimiento preventivo.	x			
	Hoja de vida de equipos de redes y telecomunicaciones.	x			
	Hoja de vida de mantenimiento de equipos de cómputo	x			

Fuente Autores

En la Tabla 3 se hace el análisis GAP, para determinar el nivel de implementación de la norma ISO 27001 y en la tabla 4 se presentan los resultados.

Tabla 3 Análisis GAP

Convenciones:
D: El control se documentó e implementó
MD :El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.
RD:El control no cumple las normas y debe ser rediseñado para cumplir con las normas
PNP:El proceso no está en su lugar / no implementado.
(Control requeridos ni documentado ni implementado)
NA (Not Applicable) El control no es aplicable para la empresa ni para el negocio**.**

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
4	**Sistema de Gestión de Seguridad de la Información**	
4,1	**Requisitos generales**	
4,1	La organización debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado	**MD**
4,2	**Establecimiento y gestión del SGSI**	
4.2.1	**Establecer el SGSI**	
4.2.1 (a)	Definir el alcance y los límites del SGSI	**MD**
4.2.1 (b)	Definir una política SGSI	**MD**
4.2.1 (c)	Definir el enfoque de evaluación de riesgos	**MD**
4.2.1 (d)	Identificar los riesgos	**MD**
4.2.1 (e)	Analizar y evaluar los riesgos	**MD**

Tabla 3. (continuación)

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
4.2.1 (f)	Identificar y evaluar las opciones para el tratamiento de los riesgos	**MD**
4.2.1 (g)	Seleccionar los objetivos de control y controles para el tratamiento de los riesgos	**MD**
4.2.1 (h)	Obtener la aprobación de la gestión de los riesgos residuales propuestos	**MD**
4.2.1 (i)	Obtener la autorización de la gerencia para implementar y operar el SGSI	**D**
4.2.1 (j)	Preparar una Declaración de aplicabilidad	**D**
4.2.2	**Implementar el SGSI**	
4.2.2 (a)	Formular un plan de tratamiento de riesgos	**MD**
4.2.2 (b)	Implementar el plan de tratamiento de riesgos con el fin de alcanzar los objetivos de control identificados	**MD**
4.2.2 (c)	Implementar controles seleccionados en 4.2.1g para cumplir los objetivos de control	**MD**
4.2.2 (d)	Definir la forma de medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo estas medidas se van a utilizar para evaluar la efectividad de los controles para producir resultados comparables y reproducibles (ver 4.2.3c)	**MD**
4.2.2 (e)	Implementar programas de capacitación y sensibilización (véase 5.2.2)	**MD**
4.2.2 (f)	Gestione la operación del SGSI	**MD**
4.2.2 (g)	Administrar los recursos para el SGSI (ver 5.2)	**MD**
4.2.2 (h)	Implementar procedimientos y otros controles capaces de permitir una rápida detección de eventos de seguridad y respuesta a incidentes de seguridad (véase 4.2.3a)	**MD**
4.2.3	**Supervisar y revisar el SGSI**	
4.2.3 (a)	Ejecutar el seguimiento y revisar los procedimientos y otros controles	**MD**
4.2.3 (b)	Llevar a cabo revisiones periódicas de la eficacia del SGSI	**MD**
4.2.3 (c)	Medir la efectividad de los controles para verificar que se han cumplido los requisitos de seguridad.	**MD**
4.2.3 (d)	Revisar las evaluaciones de riesgo a intervalos planificados y revisar los riesgos residuales y los niveles aceptables de riesgos identificados	**MD**
4.2.3 (e)	Realizar auditorías de ISMS internas a intervalos planificados (ver 6)	**MD**
4.2.3 (f)	Realizar Auditorías Internas de ISMS una planificados Intervalos (ver 6)	**MD**
4.2.3 (g)	Actualización de seguridad planea tomar en cuenta los resultados del seguimiento y la revisión de las actividades	**MD**
4.2.3 (h)	Grabar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI (ver 4.3.3)	**MD**
4.2.4	**Mantener y mejorar el SGSI**	

Tabla 3. (continuación)

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
4.2.4 (a)	Implementar las mejoras identificadas en el SGSI.	**MD**
4.2.4 (b)	Tomar las acciones correctivas y preventivas apropiadas de conformidad con 8.2 y 8.3	**MD**
4.2.4 (c)	Comunicar las acciones y mejoras a todas las partes interesadas	**MD**
4.2.4 (d)	Asegúrese de que las mejoras a alcanzar sus objetivos previstos	**MD**
4,3	**Requisitos de documentación**	
4.3.1	**Documentación SGSI Generales**	
4.3.1 (a)	Declaraciones documentadas de la política del SGSI (ver 4.2.1b) y objetivos	**MD**
4.3.1 (b)	Alcance del SGSI (ver 4.2.1a)	**MD**
4.3.1 (c)	Procedimientos y controles en apoyo del SGSI	**MD**
4.3.1 (d)	Descripción de la metodología de evaluación de riesgos (ver 4.2.1c)	**MD**
4.3.1 (e)	Informe de evaluación de riesgos (ver 4.2.1c a 4.2.1g)	**MD**
4.3.1 (f)	Plan de tratamiento del riesgo (ver 4.2.2b)	**MD**
4.3.1 (g)	Procedimientos necesitados por la organización para asegurarse de la eficaz planificación, operación y control de sus procesos de seguridad de la información y describir la forma de medir la efectividad de los controles (ver 4.2.3c)	**MD**
4.3.1 (h)	Los registros requeridos por esta Norma Internacional (véase 4.3.3)	**MD**
4.3.1 (i)	Declaración de aplicabilidad	**MD**
4.3.2	**Control de los documentos**	
4.3.2	Los documentos requeridos por el SGSI serán protegidos y controlados. Debe establecerse un procedimiento documentado para definir las acciones de gestión necesarias para:	**D**
4.3.2 (a)	Aprobar documentos adecuación antes de su emisión	**D**
4.3.2 (b)	Documentos que sean necesarios Revisar y actualizar y re-aprobar los documentos	**D**
4.3.2 (c)	Asegurarse de que se identifican los cambios y el estado de revisión actual de los documentos	**D**
4.3.2 (d)	Asegúrese de que las versiones pertinentes de los documentos aplicables están disponibles en los puntos de uso	**MD**
4.3.2 (e)	Asegúrese de que los documentos permanecen legibles y fácilmente identificables	**MD**
4.3.2 (f)	Asegúrese de que los documentos se encuentran a disposición de quienes los necesitan, y de conformidad con los procedimientos aplicables a su clasificación son transferidos, almacenados y finalmente eliminados	**MD**
4.3.2 (g)	Asegurarse de que se identifican los documentos de origen externo	**MD**
4.3.2 (h)	Asegúrese de que se controla la distribución de documentos	**MD**
4.3.2 (i)	Prevenir el uso no intencionado de documentos obsoletos	**MD**

Tabla 3. (continuación)

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
4.3.2 (j)	Aplicar una identificación adecuada en los documentos si se mantengan por cualquier razón	**MD**
4.3.3	**Control de los registros**	
4.3.3	Los registros deben establecerse y mantenerse para proporcionar evidencia de la conformidad con los requisitos y el funcionamiento eficaz del SGSI …	**MD**
4.3.3	Los registros deben ser protegidos y controlados.	**MD**
4.3.3	Los Registros Deben ser Controlados.	**MD**
4.3.3	Los registros deben permanecer legibles, fácilmente identificables y recuperables.	**MD**
4.3.3	Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros deben ser documentados e implementados.	**MD**
4.3.3	Deberá llevarse un registro de los resultados del proceso, como se indica en 4.2 y de todas las apariciones de los incidentes de seguridad significativos relacionados con el SGSI.	**MD**
5	**Responsabilidad de la dirección**	
5,1	**Compromiso de la dirección**	
5,1	Dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI por:	**MD**
5.1 (a)	El establecimiento de una política de SGSI	**MD**
5.1 (b)	Asegurarse de que se establecen los objetivos y planes del SGSI	**MD**
5.1 (c)	Establecer las funciones y responsabilidades de seguridad de la información	**MD**
5.1 (d)	Comunicar a la organización la importancia de satisfacer los objetivos de seguridad de la información y que se ajuste a la política de seguridad de la información, las atribuciones que la ley y la necesidad de mejora continua	**MD**
5.1 (e)	Proporcionar recursos suficientes para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI (ver 5.2.1)	**MD**
5.1 (f)	Decidir los criterios de aceptación de riesgos y los niveles aceptables de riesgo	**MD**
5.1 (g)	Asegurar que las auditorías internas del SGSI se llevan a cabo (ver 6)	**MD**
5.1 (h)	La realización de revisiones por la dirección de los SGSI (ver 7)	**MD**
5,2	**Gestión de recursos**	
5.2.1	**Provisión de recursos**	
5.2.1	La organización debe determinar y proporcionar los recursos necesarios para:	**MD**
5.2.1 (a)	Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI	**MD**

Tabla 3. (continuación)

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
5.2.1 (b)	Asegurar que los procedimientos de seguridad de información apoyan los requerimientos de negocio	**MD**
5.2.1 (c)	Identificar y abordar los requisitos legales y reglamentarios y las obligaciones contractuales de seguridad	**MD**
5.2.1 (d)	Mantener la seguridad adecuada por la correcta aplicación de todos los controles implementados	**MD**
5.2.1 (e)	Llevar a cabo revisiones cuando sea necesario, y para reaccionar adecuadamente ante los resultados de estas revisiones	**MD**
5.2.1 (f)	Cuando sea necesario, mejorar la eficacia del SGSI	**MD**
5.2.2	**Formación, sensibilización y competencia**	
5.2.2	La organización debe asegurarse de que todo el personal que se asignan responsabilidades definidas en el SGSI son competentes para realizar las tareas requeridas por:	**MD**
5.2.2 (a)	La determinación de las competencias necesarias para el personal que realiza las labores que afectan el SGSI	**MD**
5.2.2 (b)	Proporcionar formación o tomar otras acciones (por ejemplo, que emplean a personal competente) para satisfacer estas necesidades	**MD**
5.2.2 (c)	Evaluación de la eficacia de las medidas adoptadas	**MD**
5.2.2 (d)	El mantenimiento de los registros de educación, formación, habilidades, experiencia y calificaciones (ver 4.3.3)	**MD**
5.2.2	La organización velará por que todo el personal pertinente, son conscientes de la relevancia e importancia de sus actividades de seguridad de la información y de cómo contribuyen al logro de los objetivos del SGSI.	**MD**
6	**Auditoría interna SGSI**	
6	La organización debe llevar a cabo auditorías de ISMS internas a intervalos planificados para determinar si los objetivos de control, controles, procesos y procedimientos de su SGSI:	**MD**
6 (a)	Cumplir con los requisitos de esta norma internacional y la legislación pertinente o las normas	**MD**
6 (b)	Cumplir con los requisitos de seguridad de información identificados	**MD**
6 (c)	Implantación y el mantenimiento eficaz	**MD**
6 (d)	Lleve a cabo como se esperaba.	**MD**
6	Se debe planificar un programa de auditorías	**MD**
6	La dirección responsable del área que está siendo auditada debe asegurarse de que se toman acciones sin demora injustificada para eliminar las no conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el informe de los resultados de la verificación (ver 8).	**MD**
7	**Revisión por la dirección del SGSI**	

Tabla 3. (continuación)

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
7,1	**General**	
7,1	La dirección revisará SGSI de la organización a intervalos planificados (por lo menos una vez al año) para asegurarse de su conveniencia, adecuación y eficacia	**MD**
7,2	**Revisiones de Entrada**	
7,2	La entrada a una revisión por la dirección debe incluir:	**MD**
7.2 (a)	Los resultados de las auditorías de SGSI y comentarios	**MD**
7.2 (b)	La retroalimentación de las partes interesadas	**MD**
7.2 (c)	Técnicas, productos o procedimientos, que podrían utilizarse en la organización para mejorar el rendimiento y la eficacia SGSI	**MD**
7.2 (d)	Estado de las acciones preventivas y correctivas	**MD**
7.2 (e)	Las vulnerabilidades o amenazas que no se abordan adecuadamente en la evaluación del riesgo conocido	**MD**
7.2 (f)	Los resultados de las mediciones de eficacia	**MD**
7.2 (g)	Las acciones de seguimiento de las revisiones por la dirección previas	**MD**
7.2 (h)	Todos los cambios que podrían afectar el SGSI	**MD**
7.2 (i)	Recomendaciones para la mejora	**MD**
7,3	**Revisiones de Salida**	
7,3	Las salidas de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con lo siguiente:	**D**
7.3 (a)	Mejora de la eficacia de los SGSI	**D**
7.3 (b)	Actualización de la evaluación de riesgos y plan de tratamiento de riesgos	**D**
7.3 (c)	Modificación de los procedimientos y controles de seguridad de la información que el efecto, si es necesario, para responder a eventos internos o externos que pueden impactar en el SGSI	**MD**
7.3 (d)	Las necesidades de recursos	**MD**
7.3 (e)	Mejora la forma en que se está midiendo la eficacia de los controles	**MD**
8	**Mejora del SGSI**	
8,1	**Mejora continua**	
8,1	La organización debe mejorar continuamente la eficacia del SGSI a través del uso de la política de seguridad de la información, los objetivos de seguridad de la información, resultados de las auditorías, el análisis de los sucesos supervisados, las acciones correctivas y preventivas y la revisión por la dirección (véase 7).	**MD**
8,2	**La acción correctiva**	
8,2	La organización debe tomar acciones para eliminar la causa de no conformidades con los requisitos del SGSI, a fin de prevenir la recurrencia. El procedimiento documentado para acciones correctivas debe definir los requisitos para:	**MD**
8.2 (a)	La identificación de las no conformidades	**MD**
8.2 (b)	Determinar las causas de las no conformidades	**MD**

Tabla 3. (continuación)

ISO 27001 clausulas	Requisito obligatorio para el SGSI	StatusCod
8.2 (c)	La evaluación de la necesidad de adoptar medidas para garantizar que las no conformidades no vuelvan a ocurrir	**MD**
8.2 (d)	La determinación y aplicación de las medidas correctoras necesarias	**MD**
8.2 (e)	Resultados de la grabación de acciones tomadas (véase 4.3.3)	**MD**
8.2 (f)	Revisión de las acciones correctivas tomadas	**MD**
8,3	**La acción preventiva**	
8,3	La organización debe determinar acciones para eliminar la causa de no conformidades potenciales con los requisitos del SGSI a fin de prevenir su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas a los efectos de los problemas potenciales. El procedimiento documentado para la acción preventiva deberá definir los requisitos para:	**MD**
8.3 (a)	La identificación de las no conformidades potenciales y sus causas	**MD**
8.3 (b)	La evaluación de la necesidad de actuar para prevenir la ocurrencia de no conformidades	**MD**
8.3 (c)	La determinación y aplicación de las medidas preventivas necesarias	**MD**
8.3 (d)	Resultados de la grabación de acciones tomadas (véase 4.3.3)	**MD**
8.3 (e)	Revisión de las acciones preventivas tomadas	**D**
8,3	La organización debe identificar los riesgos que lo precisen y determinar las necesidades de acción preventiva que se centran la atención en los riesgos cambiado significativamente	**MD**

Fuente: https://profesores.ing.unab.cl/~druete/website/webroot/archivos/cursos/ESC/

Resultados obtenidos

Tabla 4 Resultados del GAP

Cantidad	Códigos Status	Significado	Porcentaje de implementación %
10	**D**	El control se documentó e implementó	**8%**
108	**MD**	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	**92%**
	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	**0%**
	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	**0%**
	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	**0%**
117			

Fuente: https://profesores.ing.unab.cl/~druete/website/webroot/archivos/cursos/ESC/

Para la obtención de la tabla 1,2, y 3 se llevaron a cabo una serie de entrevistas libres con cada uno de siguientes funcionarios:

- Administrador de Sistemas
- Administrador Red de Datos e Internet
- Administrador Portal Web
- Administrador Área de Soporte y Servicios Tecnológicos: Mantenimiento preventivo
- Administrador Área de Soporte y Servicios Tecnológicos: Mantenimiento correctivo

Por medio de las cuales se preguntó acerca de la seguridad de la información relativo a gestión de activos, seguridad física, control de acceso (lógico), proceso de contratación del personal, cumplimiento y supervisión de las monitorias, licenciamiento software, funciones y características de los servidores, software y sistemas de información alojados en los servidores, copias de seguridad, etc. Además, se aclararon interrogantes que surgieron de la revisión de la información y documentación suministrada, ya que estaba incompleta o se requería de una aclaración por parte del administrador.

En conclusión

Políticas de seguridad de seguridad están en construcción, pero la universidad, las viene implementando.

Manual de funciones y competencias laborales, están en construcción, pero la universidad las viene implementando.

Procesos y procedimientos cuentan con estos y los tiene documentados.

Inventario de activos cuentan con este y hacen seguimiento al inventario

Portafolio de servicios cuentan con estos, pero están en construcción socializarlos a la comunidad educativa.

Registro de problemas e incidentes: cuentan con el seguimiento y toman medida para mitigarlos.

El 8% de los controles están documentados

El 92% de los controles, se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos, la empresa está en proceso de construcción y aprobación de los documentos.

Elaboración y presentación del informe definitivo: Se elaboró el trabajo de grado con el fin de sustentarlo, y paralelo a esto se desarrollará un informe que se presentará a la USTA.

Tabla 5 Declaración de aplicabilidad ISO 27001.
Leyenda (para la selección de controles y razón por la que se seleccionaron):
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas, RRA: resultado de la valoración de riesgos;
TSE: hasta cierto punto.

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**					
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información	80%				
	5.1.1	Políticas de seguridad de la información	80%			x	
	5.1.2	Revisión de las políticas de seguridad de la información	80%			x	
6 Organización de la Seguridad de la Información	6,1	Organización interna	49%				
	6.1.1	Roles y responsabilidad de seguridad de la información	90%	x	x		
	6.1.2	Segregación de deberes	100%		x	x	
	6.1.3	Contacto con autoridades	0%				
	6.1.4	Contacto con grupos de interés especial	0%				
	6.1.5	Seguridad de la información en la gestión de proyectos	80%			x	
	6,2	Dispositivos móviles y teletrabajo					
	6.2.1	Política de dispositivos móviles	70%				x
	6.2.2	Teletrabajo	0%				

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo	95%				
	7.1.1	Verificación de antecedentes	90%	x			
	7.1.2	Términos y condiciones del empleo	100%		x		
	7,2	Durante el empleo					
	7.2.1	Responsabilidades de la Alta Gerencia	100%		x		
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	100%		x		
	7.2.3	Proceso disciplinario	100%	x	x		
	7,3	Terminación y cambio de empleo					
	7.3.1	Termino de responsabilidades o cambio de empleo	80%	x	x		x
8 Gestión de Activos	8,1	Responsabilidad de los activos	88%				
	8.1.1	Inventario de activos	100%			x	x
	8.1.2	Propiedad de activos	100%			x	
	8.1.3	Uso aceptable de los activos	80%			x	
	8.1.4	Devolución de activos	90%			x	
	8,2	Clasificación de la información					
	8.2.1	Clasificación de la información	90%			x	x
	8.2.2	Etiquetado de la información	100%			x	x
	8.2.3	Manejo de activos	90%			x	x
	8,3	Manejo de medios					
	8.3.1	Gestión de medios removibles	70%			x	x

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
	8.3.2	Eliminación de medios	80%			x	x
	8.3.3	Transporte de medios físicos	80%			x	x
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso	84%				
	9.1.1	Política de control de acceso	90%			x	x
	9.1.2	Acceso a redes y servicios de red	90%			x	x
	9,2	Gestión de accesos de usuario					
	9.2.1	Registro y baja del usuario	90%			x	x
	9.2.2	Provisión de acceso a usuarios	90%			x	x
	9.2.3	Gestión de derechos de acceso privilegiados	90%			x	x
	9.2.4	Gestión de información de autenticación secreta de usuarios	90%			x	x
	9.2.5	Revisión de derechos de acceso de usuarios	80%			x	x
	9.2.6	Eliminación o ajuste de derechos de acceso	80%			x	x
	9,3	Responsabilidades del usuario					
	9.3.1	Uso de información de autenticación secreta	50%				x
	9,4	Control de acceso de sistemas y aplicaciones					
	9.4.1	Restricción de acceso a la información	90%			x	x
	9.4.2	Procedimientos de inicio de sesión seguro	80%			x	x
	9.4.3	Sistema de gestión de contraseñas	80%			x	x
	9.4.4	Uso de programas y utilidades privilegiadas	90%				x
	9.4.5	Control de acceso al código fuente del programa	90%				x

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
10 Criptografía	10,1	Controles criptográficos	80%				
	10.1.1	Política en el uso de controles criptográficos	80%				x
	10.1.2	Gestión de llaves	80%				x
11 Seguridad Física y del Entorno	11,1	Áreas seguras	83%				
	11.1.1	Perímetro de seguridad físico	90%			x	x
	11.1.2	Controles físicos de entrada	90%			x	x
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	90%			x	x
	11.1.4	Protección contra amenazas externas y del ambiente	80%			x	x
	11.1.5	Trabajo en áreas seguras	80%			x	x
	11.1.6	Áreas de entrega y carga	80%			x	x
	11,2	Equipo					
	11.2.1	Instalación y protección de equipo	100%			x	
	11.2.2	Servicios de soporte	90%			x	
	11.2.3	Seguridad en el cableado	60%			x	x
	11.2.4	Mantenimiento de equipos	90%			x	
	11.2.5	Retiro de activos	90%			x	x
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	80%			x	x
	11.2.7	Eliminación segura o reúso del equipo	70%			x	x
	11.2.8	Equipo de usuario desatendido	80%			x	x
	11.2.9	Política de escritorio limpio y pantalla limpia	80%			x	x

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades	74%				
	12.1.1	Documentación de procedimientos operacionales	70%			x	
	12.1.2	Gestión de cambios	60%			x	
	12.1.3	Gestión de la capacidad	70%			x	
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	80%			x	
	12,2	Protección de Software Malicioso					
	12.2.1	Controles contra software malicioso	80%			x	x
	12,3	Respaldo					
	12.3.1	Respaldo de información	90%			x	x
	12,4	Bitácoras y monitoreo					
	12.4.1	Bitácoras de eventos	70%				x
	12.4.2	Protección de información en bitácoras	80%			x	x
	12.4.3	Bitácoras de administrador y operador	70%			x	x
	12.4.4	Sincronización de relojes	80%			x	x
	12,5	Control de software operacional					
	12.5.1	Instalación de software en sistemas operacionales	70%			x	
	12,6	Gestión de vulnerabilidades técnicas					
	12.6.1	Gestión de vulnerabilidades técnicas	70%			x	
	12.6.2	Restricciones en la instalación de software	60%			x	
	12,7	Consideraciones de auditoria de sistemas de información					
	12.7.1	Controles de auditoría de sistemas de información	80%				

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red	80%				
	13.1.1	Controles de red	80%				x
	13.1.2	Seguridad en los servicios en red	90%				x
	13.1.3	Segregación en redes	90%				x
	13,2	Transferencia de información					
	13.2.1	Políticas y procedimientos para la transferencia de información	60%			x	
	13.2.2	Acuerdos en la transferencia de información	70%			x	
	13.2.3	Mensajería electrónica	80%			x	
	13.2.4	Acuerdos de confidencialidad o no-revelación	90%			x	
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de seguridad en sistemas de información	76%				
	14.1.1	Análisis y especificación de requerimientos de seguridad	90%				x
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	80%				x
	14.1.3	Protección de transacciones en servicios de aplicación	90%				x
	14,2	Seguridad en el proceso de desarrollo y soporte					
	14.2.1	Política de desarrollo seguro	80%				x
	14.2.2	Procedimientos de control de cambios del sistema	80%				x

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	80%				x
	14.2.4	Restricción de cambios en paquetes de software	70%				x
	14.2.5	Principios de seguridad en la ingeniería de sistemas	70%				x
	14.2.6	Entorno de desarrollo seguro	70%				x
	14.2.7	Desarrollo tercerizado	70%				x
	14.2.8	Pruebas de seguridad del sistema	70%				x
	14.2.9	Pruebas de aceptación del sistema	70%				x
	14,3	Datos de prueba					
	14.3.1	Protección de datos de prueba	70%				x
15 Relaciones con Proveedores	15,1	Seguridad de la información en relaciones con el proveedor	74%				
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	70%				x
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	70%				x
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	70%				x
	15,2	Gestión de entrega de servicios de proveedor					
	15.2.1	Monitoreo y revisión de servicios del proveedor	80%				x
	15.2.2	Gestión de cambios a los servicios del proveedor	80%				x

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
16 Gestión de Incidentes de Seguridad de la Información	16,1	Gestión de incidentes de seguridad de la información y mejoras	79%				
	16.1.1	Responsabilidades y procedimientos	80%			x	x
	16.1.2	Reporte de eventos de seguridad de la información	80%			x	x
	16.1.3	Reporte de debilidades de seguridad de la información	80%			x	x
	16.1.4	Valoración y decisión de eventos de seguridad de la información	80%			x	x
	16.1.5	Respuesta a incidentes de seguridad de la información	80%			x	x
	16.1.6	Aprendizaje de incidentes de seguridad de la información	70%			x	x
	16.1.7	Colección de evidencia	80%			x	x
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Continuidad de la seguridad de la información	75%				
	17.1.1	Planeación de la continuidad de la seguridad de la información	70%			x	x
	17.1.2	Implementación de la continuidad de la seguridad de la información	70%			x	x
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	80%			x	x
	17,2	Redundancias					
	17.2.1	Disponibilidad de facilidades de procesamiento de información	80%				

Tabla 5. (continuación)

Controles de Seguridad			Controles actuales	Controles seleccionados y razones de selección			
				LR	CO	BR/BP	RRA
18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales	85%				
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	100%	x		x	
	18.1.2	Derechos de propiedad intelectual (IPR)	100%	x		x	
	18.1.3	Protección de registros	80%	x		x	
	18.1.4	Privacidad y protección de información personal identificable (PIR)	80%	x		x	
	18.1.5	Regulación de controles criptográficos	80%	x		x	x
	18,2	Revisiones de seguridad de la información					
	18.2.1	Revisión independiente de seguridad de la información	70%			x	x
	18.2.2	Cumplimiento con políticas y estándares de seguridad	90%			x	x
	18.2.3	Revisión del cumplimiento técnico	80%			x	x

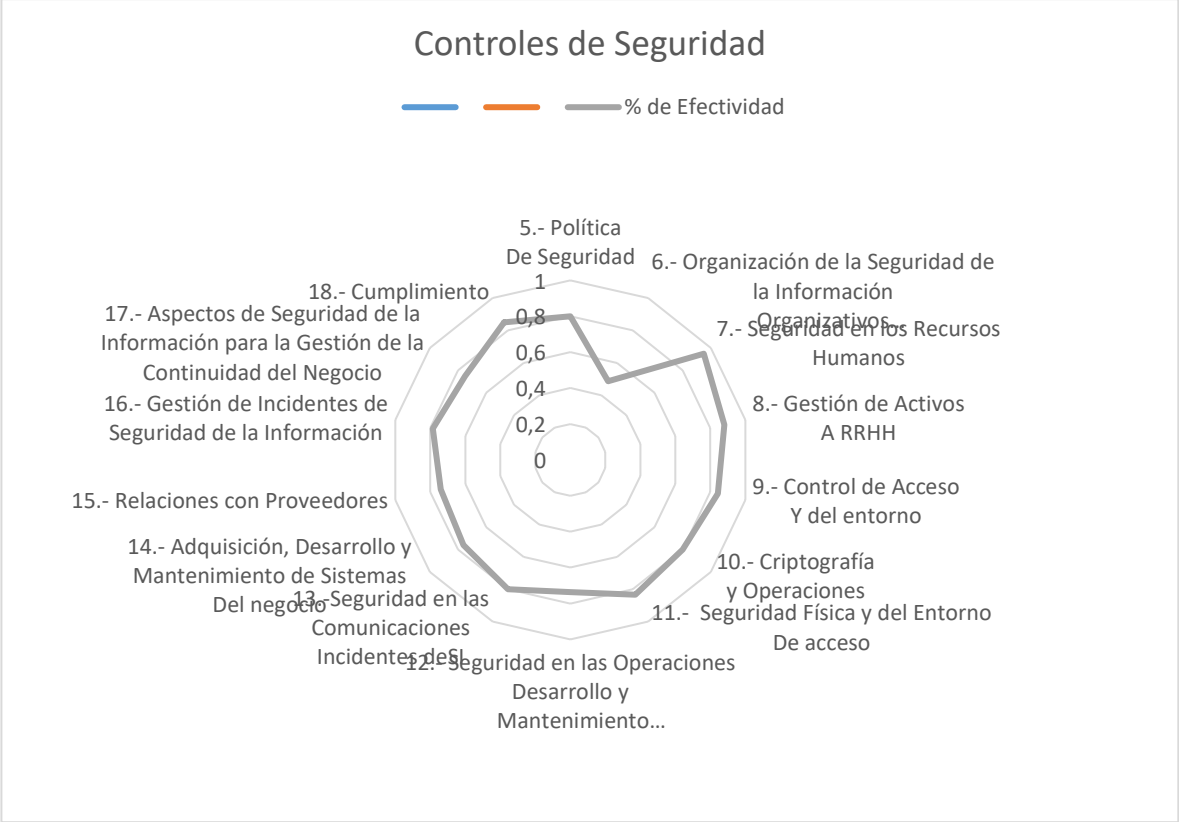
Fuente: Autores

Tabla 6 Análisis de porcentaje de efectividad: declaración de aplicabilidad ISO 27001

Dominio	% de Efectividad
5.- Política De Seguridad	80%
6.- Organización de la Seguridad de la Información Organizativos de la SI	49%
7.- Seguridad en los Recursos Humanos	95%
8.- Gestión de Activos A RRHH	88%
9.- Control de Acceso Y del entorno	84%
10.- Criptografía y Operaciones	80%
11.- Seguridad Física y del Entorno De acceso	83%
12.- Seguridad en las Operaciones Desarrollo y Mantenimiento De los SI	74%
13.-Seguridad en las Comunicaciones Incidentes de SI	80%
14.- Adquisición, Desarrollo y Mantenimiento de Sistemas Del negocio	76%
15.- Relaciones con Proveedores	74%
16.- Gestión de Incidentes de Seguridad de la Información	79%
17.- Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	75%
18.- Cumplimiento	85%

Fuente: www.ISO27001security.com

Gráfica 1 Grafica radar de la efectividad de acuerdo a la norma ISO



Fuente: autores

De los resultados obtenidos del análisis el ítem más bajo obtenido fue la Organización de la Seguridad de la Información Organizativos de la Sistema de información (SI), con un 49% esto se debe a que la organización está en proceso de documentar sus procesos.

El más alto con el 95% es Seguridad en los Recursos Humanos, que es un proceso que se viene trabajando e implementado hace varios años en la universidad, pero hace 2 se lleva el control total.

En cuanto los otro ítem se obtuvo la Política de Seguridad está en 80%, está en construcción y falta la aprobación total de esta, la Gestión de Activos A RRHH, 88%,estos están identificados, documentados, los Control de Acceso y del entorno 84% se viene implementados desde hace 2 años, Criptografía se obtuvo Operaciones 80% falta documenta alguno procesos e implementación en un 100%, la Seguridad Física y del Entorno de acceso es 83% se tiene controlados el 90% de los espacios pero falta documentar proceso y centro lar el 10% de los espacios, la Seguridad en las Operaciones, Desarrollo y Mantenimiento De los SI se obtuvo un 80%, se está realizando falta la evolución de que tan efectivo es la forma como

se realiza,-Seguridad en las Comunicaciones Incidentes de SI 80%, la adquisición, Desarrollo y Mantenimiento de Sistemas del negocio 76% se realiza adquisidores de nuevos equipos pero priman los temas monetarios en algunos casos que las necesidades, relaciones con Proveedores 74% se tiene varios proveedores, a relación es bueno pero debido a la documentación que se les solicita haces se pierden estos, la Gestión de Incidentes de Seguridad de la Información 79% se están documentando y se generan acciones para corregirlas, pero están en proceso de implementación, Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio 75% y Cumplimiento porque están en proceso de implementación 85%.

Tabla 7 Amenazas de activos

Amenaza/Activo	D100	SI100	SI200	SI300	SW100	SW200	SW300	HW100	HW200	HW300	M100	COM100	COM200	P1000	P2000	P2000	P2000	L1000	L2000	L3000	S1000	S2000	S3000
Fuego								SI	SI	SI	SI	SI	SI					SI	SI	SI			
Daños por agua								SI	SI	SI	SI	SI	SI					SI	SI	SI			
Desastres naturales								SI	SI	SI	SI	SI	SI					SI	SI	SI			
Fuga de información	SI	SI	SI	SI																			
Introducción de falsa información	SI	SI	SI	SI																			
Alteración de la información	SI	SI	SI	SI							SI										SI		
Corrupción de la información	SI	SI	SI	SI							SI										SI		
Destrucción de información	SI	SI	SI	SI							SI										SI		
Interceptación de información (escucha)	SI	SI	SI	SI																	SI		
Corte del suministro eléctrico		SI	SI	SI				SI	SI	SI											SI		
Condiciones inadecuadas de temperatura o humedad		SI	SI	SI				SI	SI	SI	SI										SI		
Fallo de servicios de comunicaciones		SI	SI	SI				SI	SI	SI		SI	SI								SI		
Interrupción de otros servicios y suministros esenciales		SI	SI	SI				SI	SI	SI													
Desastres industriales																							
Degradación de los soportes de almacenamiento de la información											SI										SI		
Difusión de software dañino	SI	SI	SI	SI							SI										SI		
Errores de mantenimiento / actualización de programas (software)	SI	SI	SI	SI	SI	SI	SI														SI		
Errores de mantenimiento / actualización de equipos (hardware)								SI	SI	SI	SI	SI	SI								SI		
Caída del sistema por sobrecarga	SI	SI	SI	SI				SI	SI	SI		SI	SI								SI		
Pérdida de equipos								SI	SI	SI								SI	SI	SI	SI		

Tabla 7. (continuación)

Amenaza/Activo	D100	SI100	SI200	SI300	SW100	SW200	SW300	HW100	HW200	HW300	M100	COM100	COM200	P1000	P2000	P2000	P2000	L1000	L2000	L3000	S1000	S2000	S3000
Indisponibilidad del personal																					SI		
Abuso de privilegios de acceso	SI	SI	SI	SI														SI	SI	SI	SI		
Acceso no autorizado	SI	SI	SI	SI														SI	SI	SI	SI		
Errores de los usuarios	SI	SI	SI	SI																	SI		
Errores del administrador	SI	SI	SI	SI																	SI		
Errores de configuración	SI	SI	SI	SI	SI	SI	SI				SI	SI	SI								SI		
Denegación de servicio		SI	SI	SI																	SI		
Robo								SI	SI	SI	SI												
Indisponibilidad del personal	SI	SI	SI	SI							SI			SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Extorsión																							
Ingeniería social	SI	SI	SI	SI																	SI		

Fuente autores

Se determinan los recursos afectados y se analiza la causa que origina cada uno de los riesgos encontrados, los recursos afectados son HW hardware, SW software, TH talento humano, y ORG.

Riesgo Es el calculado sobre un activo teniendo en cuenta[32]

• el impacto acumulado sobre un activo debido a una amenaza y

• la probabilidad de la amenaza

riesgo = impacto × Probabilidad

Criterios de aceptación del riesgo

Rango	Descripción
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable, es decir de alto impacto y debe proceder a su tratamiento.

De acuerdo a los dominios de la seguridad de la información, se tienen en Udigitalrm. [33]

Tabla 8 Dimensiones de la seguridad de la información

[A]	Autenticación	asegurar la identidad u origen de los datos.
[C]	Confidencialidad	asegurar que la información es sólo accesible para aquellos autorizados
[I]	Integridad	garantía de la exactitud y de que la información sea completa, así como los métodos de su procesamiento
[D]	Disponibilidad	asegurar que los usuarios autorizados tienen acceso cuando lo requieran en los tiempos adecuados
[T]	Trazabilidad	asegurar que en todo momento se podrá determinar quién hizo qué y en qué momento

Fuente Fundamentado en la metodología Margerit

Para hallar el valor final del Impacto del activo, se realizó la suma de los valores, ubicados en el rango de, de los distintos criterios, especificados en la tabla 8, y se dividido por 5, que

[32] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS , versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.Libro I - Método, Madrid, 2012

[33] UDIGITALRM. (2011). Guía de la seguridad de la Información para PYMES. Recuperado el diciembre de 2016, de https://ingtecnologia.files.wordpress.com/2011/06/gestion-de-la-seguridad-de-la-informacion.pdf

corresponde a los 5 dominios descritos, Bajo (1), Medio (2), Alto (3), de acuerdo la tabla de valoración que se utiliza para estimar el riesgo también.

Tabla 9 Estimación de Probabilidad

Valor	Descripción
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

Fuente Fundamentado en la metodología Margerit.

Tabla 10 Estimación de Impacto

Valor	Descripción
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente: Fundamentado en la metodología Margerit.

Tabla de Impacto

Impacto	Alto	3	6	9
	Medio	2	4	6
	Bajo	1	2	3
		Bajo	Medio	Alto
	Probabilidad			

Tabla 11 Estimación del Riesgo

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
[D] Datos / Información	D100	R1	Fuga de información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R2	Introducción de falsa información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R3	Alteración de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R4	Corrupción de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R5	Destrucción de información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R6	Interceptación de información (escucha)	Medio (2)	2	3	3	1	1	2	2	Medio (2)	4

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	D100	R7	Difusión de software dañino	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R8	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	D100	R9	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R10	Abuso de privilegios de acceso	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R11	Acceso no autorizado	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R12	Errores de los usuarios	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R13	Errores del administrador	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R14	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	D100	R15	Indisponibilidad del personal	Bajo (1)	1			1	2	1	1	Bajo (1)	1
	D100	R16	Ingeniería social	Medio (2)	2	2	2	2	2	2	2	Medio (2)	4
[SI] Sistema de Información	SI100	R17	Fuga de información	Alto (3)	3	3	3	3	3	3	3	Alto (3)	9
	SI100	R18	Introducción de falsa información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	SI100	R19	Alteración de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R20	Corrupción de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R21	Destrucción de información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R22	Interceptación de información (escucha)	Medio (2)	2	3	3	1	1	2	2	Medio (2)	4
	SI100	R23	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI100	R24	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI100	R25	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R26	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	3	3	1	1	2	2	Medio (2)	4
	SI100	R27	Difusión de software dañino	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R28	Errores de mantenimiento / actualización de	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
			programas (software)										
	SI100	R29	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R30	Abuso de privilegios de acceso	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R31	Acceso no autorizado	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R32	Errores de los usuarios	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R33	Errores del administrador	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R34	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R35	Denegación de servicio	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI100	R36	Indisponibilidad del personal	Bajo (1)	1	1	1	1	2		1	Bajo (1)	1
	SI100	R37	Ingeniería social	Medio (2)	2	2	2	2	2	2	2	Medio (2)	4
	SI200	R38	Fuga de información	Alto (3)	3	3	3	3	3	3	3	Alto (3)	9
	SI200	R39	Introducción de falsa información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	SI200	R40	Alteración de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R41	Corrupción de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R42	Destrucción de información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R43	Interceptación de información (escucha)	Medio (2)	2	3	3	1	1	2	2	Medio (2)	4
	SI200	R44	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI200	R45	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI200	R46	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R47	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	2	1	1	3	3	2	Medio (2)	4
	SI200	R48	Difusión de software dañino	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R49	Errores de mantenimiento / actualización de	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
			programas (software)										
	SI200	R50	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R51	Abuso de privilegios de acceso	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R52	Acceso no autorizado	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R53	Errores de los usuarios	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R54	Errores del administrador	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R55	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R56	Denegación de servicio	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI200	R57	Indisponibilidad del personal	Bajo (1)	1	3		1			1	Bajo (1)	1
	SI200	R58	Ingeniería social	Medio (2)	2	2	2	2	2	2	2	Medio (2)	4
[SW] Software / Aplicativos	SI300	R59	Fuga de información	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R60	Introducción de falsa información	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	SI300	R61	Alteración de la información	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R62	Corrupción de la información	Alto (3)	3	3	3	3	3	3	3	Alto (3)	9
	SI300	R63	Destrucción de información	Alto (3)	3	3	3	3	3	3	3	Alto (3)	9
	SI300	R64	Interceptación de información (escucha)	Medio (2)	2	3	3	1	1	2	2	Medio (2)	4
	SI300	R65	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R66	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R67	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	SI300	R68	Interrupción de otros servicios y suministros esenciales	Bajo (1)	1	2	1	1	3	3	2	Medio (2)	2
	SI300	R69	Difusión de software dañino	Alto (3)	3	3	3	3	3	3	3	Alto (3)	9
	SI300	R70	Errores de mantenimiento / actualización de	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
			programas (software)										
	SI300	R71	Caída del sistema por sobrecarga	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R72	Abuso de privilegios de acceso	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R73	Acceso no autorizado	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R74	Errores de los usuarios	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R75	Errores del administrador	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R76	Errores de configuración	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R77	Denegación de servicio	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SI300	R78	Indisponibilidad del personal	Bajo (1)	1	3		1			1	Bajo (1)	1
	SI300	R79	Ingeniería social	Medio (2)	2	2	2	2	2	2	2	Medio (2)	4
	SW100	R80	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	SW100	R81	Errores de configuración	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SW200	R82	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SW200	R83	Errores de configuración	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SW300	R84	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	SW300	R85	Errores de configuración	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
[HW] Hardware / Equipos informáticos	HW100	R86	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW100	R87	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW100	R88	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW100	R89	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW100	R90	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	HW100	R91	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW100	R92	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	2	1	1	3	3	2	Medio (2)	4
	HW100	R93	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW100	R94	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW100	R95	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW100	R96	Robo	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW200	R97	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW200	R98	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW200	R99	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW200	R100	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW200	R101	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	HW200	R102	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW200	R103	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	2	1	1	3	3	2	Medio (2)	4
	HW200	R104	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW200	R105	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW200	R106	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW200	R107	Robo	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW300	R108	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW300	R109	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW300	R110	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW300	R111	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW300	R112	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	HW300	R113	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW300	R114	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	2	1	1	3	3	2	Medio (2)	4
	HW300	R115	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW300	R116	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	HW300	R117	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	HW300	R118	Robo	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
[M] Soportes de información	M100	R119	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	M100	R120	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	M100	R121	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	M100	R122	Alteración de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	M100	R123	Corrupción de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	M100	R124	Destrucción de información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	M100	R125	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	M100	R126	Degradación de los soportes de almacenamiento de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	M100	R127	Difusión de software dañino	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	M100	R128	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	M100	R129	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	M100	R130	Robo	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	M100	R131	Indisponibilidad del personal	Bajo (1)	1	3		1			1	Bajo (1)	1
[COM] Redes de comunicaciones	COM100_	R132	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	COM100_	R133	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	COM100_	R134	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	COM100_	R135	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	COM100_	R136	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	COM100_	R137	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	COM100_	R138	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	COM200_	R139	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	COM200_	R140	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	COM200_	R141	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	COM200_	R142	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	COM200_	R143	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	COM200_	R144	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	COM200_	R145	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
[P] Personal	P100	R146	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	P200	R147	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1
	P300	R148	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1
	P300	R149	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1
[L] Instalaciones	L100	R150	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L100	R151	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L100	R152	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L100	R153	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L100	R154	Abuso de privilegios de acceso	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L100	R155	Acceso no autorizado	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L100	R156	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1
	L200	R157	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L200	R158	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L200	R159	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L200	R160	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	L200	R161	Abuso de privilegios de acceso	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L200	R162	Acceso no autorizado	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L200	R163	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1
	L300	R164	Fuego	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L300	R165	Daños por agua	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L300	R166	Desastres naturales	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L300	R167	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L300	R168	Abuso de privilegios de acceso	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L300	R169	Acceso no autorizado	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	L300	R170	Indisponibilidad del personal	Bajo (1)	1	1	1	1	1	1	1	Bajo (1)	1
[S] Servicios	S100	R171	Alteración de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R172	Corrupción de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R173	Destrucción de información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	S100	R174	Interceptación de información (escucha)	Medio (2)	2	3	3	1	1	2	2	Medio (2)	4
	S100	R175	Corte del suministro eléctrico	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	S100	R176	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	S100	R177	Fallo de servicios de comunicaciones	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R178	Degradación de los soportes de almacenamiento de la información	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R179	Difusión de software dañino	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R180	Errores de mantenimiento / actualización de programas (software)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R181	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6

Tabla 11. (Continuación)

Activo		Id Riesgo	Amenaza	Probabilidad		Impacto							Riesgo
						[A]	[C]	[I]	[D]	[T]	Total Cuantitativo	Total Cualitativo	
	S100	R182	Caída del sistema por sobrecarga	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R183	Pérdida de equipos	Bajo (1)	1	3	3	3	3	3	3	Alto (3)	3
	S100	R184	Indisponibilidad del personal	Bajo (1)	1	3		1			1	Bajo (1)	1
	S100	R185	Abuso de privilegios de acceso	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R186	Acceso no autorizado	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R187	Errores de los usuarios	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R188	Errores del administrador	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R189	Errores de configuración	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R190	Denegación de servicio	Medio (2)	2	3	3	3	3	3	3	Alto (3)	6
	S100	R191	Indisponibilidad del personal	Bajo (1)	1	3		1			1	Bajo (1)	1
	S100	R192	Ingeniería social	Medio (2)	2	2	2	2	2	2	2	Medio (2)	4
	S200	R193	Indisponibilidad del personal	Bajo (1)	1	3		1			1	Bajo (1)	1

Fuente los autores, Fundamentado en la metodología Margerit

Según la tabla de riesgos obtenemos el siguiente mapa de riesgos

Tabla 12 Mapa de riesgos

impacto	Alto	R8,R23,R24,R44,R45,R59,R60,R61,R65,R66,R70,R71,R72,R73,R74,R75,R76,R77,R80,R81,R82,R83,R84,R85,R86,R87,R88,R89,R90,R95,R96,R97,R98,R99,R100,R101,R106,R107,R108,R109,R110,R111,R112,R117,R118,R119,R120,R121,R125,R130,R132,R133,R134,R139,R140,R141,R150,R151,R152,R153,R154,R155,R157,R158,R159,R160,R161,R162,R164,R165,R166,R167,R168,R169,R175,R176,R183	R1,R2,R3,R4,R5,R7,R9,R10,R11,R12,R13,R14,R18,R19,R20,R21,R25,R27,R28,R29,R30,R31,R32,R33,R34,R35,R39,R40,R41,R42,R46,R48,R49,R50,R51,R52,R53,R54,R55,R56,R67,R91,R93,R94,R102,R104,R105,R113,R115,R116,R122,R123,R124,R126,R127,R128,R129,R135,R136,R137,R138,R142,R143,R144,R145,R171,R172,R173,R177,R178,R179,R180,R181,R182,R185,R186,R187,R188,R189,R190	R17,R38,R62,R63,R69
	Medio	R68	R6,R16,R22,R26,R37,R43,R47,R58,R64,R79,R92,R103,R114,R174,R192	R1,R2,R3,R4,R5,R7,R9,R10,R11,R12,R13,R14,R18,R19,R20,R21,R25,R27,R28,R29,R30,R31,R32,R33,R34,R35,R39,R40,R41,R42,R46,R48,R49,R50,R51,R52,R53,R54,R55,R56,R67,R91,R93,R94,R102,R104,R105,R113,R115,R116,R122,R123,R124,R126,R127,R128,R129,R135,R136,R137,R138,R142,R143,R144,R145,R171,R172,R173,R177,R178,R179,R180,R181,R182,R185,R186,R187,R188,R189,R190
	Bajo	R15,R36,R57,R78,R131,R146,R147,R148,R149,R156,R163,R170,R184,R191,R193	R68	R8,R23,R24,R44,R45,R59,R60,R61,R65,R66,R70,R71,R72,R73,R74,R75,R76,R77,R80,R81,R82,R83,R84,R85,R86,R87,R88,R89,R90,R95,R96,R97,R98,R99,R100,R101,R106,R107,R108,R109,R110,R111,R112,R117,R118,R119,R120,R121,R125,R130,R132,R133,R134,R139,R140,R141,R150,R151,R152,R153,R154,R155,R157,R158,R159,R160,R161,R162,R164,R165,R166,R167,R168,R169,R175,R176,R183
		Bajo	Medio	Alto
	Probabilidad			

Nota: Frente a los riesgos de Alta Probabilidad e impacto, se recomienda realizar acciones de forma simultánea con el objetivo inicial de reducir el riesgo, y de ser necesario compartir o transferir el riesgo mediante la contratación de expertos externos.

En cuanto a los riesgos de riesgo medio y bajo, es indispensable iniciar de forma escalonada, las acciones es decir iniciar con acciones para reducir el riesgo.

Tabla 13 Análisis de Riesgo

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R17	SI100	Fuga de información	Alto (3)	3	Alto (3)	3	9	**A.9.2.5 Revisión de derechos de acceso de usuarios** Deberían evitarse las situaciones que permitan que se produzcan fugas de información **A.8.3.1 Gestión de medios removibles** Se deberían establecer procedimientos para la gestión de los soportes extraíbles **A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación **A.8.2 Clasificación de la información** Deberían establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **A.12.1.1 Documentación de procedimientos operacionales** La documentación del sistema debería estar protegida contra accesos no autorizados.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R38	SI200	Fuga de información	Alto (3)	3	Alto (3)	3	9	A.9.2.5 Revisión de derechos de acceso de usuarios Deberían evitarse las situaciones que permitan que se produzcan fugas de información **A.8.3.1 Gestión de medios removibles** Se deberían establecer procedimientos para la gestión de los soportes extraíbles **A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación **A.8.2 Clasificación de la información** Deberían establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **A.12.1.1 Documentación de procedimientos operacionales** La documentación del sistema debería estar protegida contra accesos no autorizados.	* Reducir el riesgo
[SI] Sistema de Información	R62	SI300	Corrupción de la información	Alto (3)	3	Alto (3)	3	9	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R63	SI300	Destrucción de información	Alto (3)	3	Alto (3)	3	9	**A.8.2 Clasificación de la información de la organización**" Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo
[SI] Sistema de Información	R69	SI300	Difusión de software dañino	Alto (3)	3	Alto (3)	3	9	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.	* Reducir el riesgo
[D] Datos / Información	R1	D100	Fuga de información	Medio (2)	2	Alto (3)	3	6	**A.9.2.5 Revisión de derechos de acceso de usuarios** Deberían evitarse las situaciones que permitan que se produzcan fugas de información **A.8.3.1 Gestión de medios removibles** Se deberían establecer procedimientos para la gestión de los soportes extraíbles **A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación **A.8.2 Clasificación de la información** Deberían establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **A.12.1.1 Documentación de procedimientos operacionales** La documentación del sistema debería estar protegida contra accesos no autorizados.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[D] Datos / Información	R2	D100	Introducción de falsa información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[D] Datos / Información	R3	D100	Alteración de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[D] Datos / Información	R4	D100	Corrupción de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[D] Datos / Información	R5	D100	Destrucción de información	Medio (2)	2	Alto (3)	3	6	**A.8.2 Clasificación de la información de la organización"** Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[D] Datos / Información	R7	D100	Difusión de software dañino	Medio (2)	2	Alto (3)	3	6	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.	* Reducir el riesgo
[D] Datos / Información	R9	D100	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[D] Datos / Información	R10	D100	Abuso de privilegios de acceso	Medio (2)	2	Alto (3)	3	6	**A.9.2 Gestión de accesos de usuario** La asignación y el uso de privilegios deberían estar restringidos y controlados. **A.9.1 Requerimientos de negocio para el control de acceso** Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso. **A.9.2.5Revisión de los derechos de acceso de usuario** La Dirección debería revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[D] Datos / Información	R11	D100	Acceso no autorizado	Medio (2)	2	Alto (3)	3	6	A.9.2.5 Revisión de derechos de acceso de usuarios Se deberían utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos La identificación automática de los equipos se debería considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos Se debería controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración Los grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes. En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debería restringirse la capacidad de los usuarios para conectarse a la red, esto debería hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales **A. 13 Seguridad en las Comunicaciones** Se deberían implantar controles de encaminamiento (routing) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.	* Reducir el riesgo
[D] Datos / Información	R12	D100	Errores de los usuarios	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[D] Datos / Información	R13	D100	Errores del administrador	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[D] Datos / Información	R14	D100	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[SI] Sistema de Información	R18	SI100	Introducción de falsa información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R19	SI100	Alteración de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[SI] Sistema de Información	R20	SI100	Corrupción de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[SI] Sistema de Información	R21	SI100	Destrucción de información	Medio (2)	2	Alto (3)	3	6	**A.8.2 Clasificación de la información de la organización"** Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo
[SI] Sistema de Información	R25	SI100	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R27	SI100	Difusión de software dañino	Medio (2)	2	Alto (3)	3	6	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.	* Reducir el riesgo
[SI] Sistema de Información	R28	SI100	Errores de mantenimiento / actualización de programas (software)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[SI] Sistema de Información	R29	SI100	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[SI] Sistema de Información	R30	SI100	Abuso de privilegios de acceso	Medio (2)	2	Alto (3)	3	6	**A.9.2 Gestión de accesos de usuario** La asignación y el uso de privilegios deberían estar restringidos y controlados. **A.9.1 Requerimientos de negocio para el control de acceso** Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso. **A.9.2.5Revisión de los derechos de acceso de usuario** La Dirección debería revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R31	SI100	Acceso no autorizado	Medio (2)	2	Alto (3)	3	6	A.9.2.5 Revisión de derechos de acceso de usuarios Se deberían utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos La identificación automática de los equipos se debería considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos Se debería controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración Los grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes. En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debería restringirse la capacidad de los usuarios para conectarse a la red, esto debería hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales **A. 13 Seguridad en las Comunicaciones** Se deberían implantar controles de encaminamiento (routing) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.	* Reducir el riesgo
[SI] Sistema de Información	R32	SI100	Errores de los usuarios	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R33	SI100	Errores del administrador	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[SI] Sistema de Información	R34	SI100	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R35	SI100	Denegación de servicio	Medio (2)	2	Alto (3)	3	6	Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones A.9.2.5 Revisión de derechos de acceso de usuarios Debería establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. Debería desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio. **A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información	* Reducir el riesgo
[SI] Sistema de Información	R39	SI200	Introducción de falsa información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R40	SI200	Alteración de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[SI] Sistema de Información	R41	SI200	Corrupción de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[SI] Sistema de Información	R42	SI200	Destrucción de información	Medio (2)	2	Alto (3)	3	6	**A.8.2 Clasificación de la información de la organización"** Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo
[SI] Sistema de Información	R46	SI200	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R48	SI200	Difusión de software dañino	Medio (2)	2	Alto (3)	3	6	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.	* Reducir el riesgo
[SI] Sistema de Información	R49	SI200	Errores de mantenimiento / actualización de programas (software)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[SI] Sistema de Información	R50	SI200	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[SI] Sistema de Información	R51	SI200	Abuso de privilegios de acceso	Medio (2)	2	Alto (3)	3	6	**A.9.2 Gestión de accesos de usuario** La asignación y el uso de privilegios deberían estar restringidos y controlados. **A.9.1 Requerimientos de negocio para el control de acceso** Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso. **A.9.2.5Revisión de los derechos de acceso de usuario**	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
									La Dirección debería revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	
[SI] Sistema de Información	R52	SI200	Acceso no autorizado	Medio (2)	2	Alto (3)	3	6	A.9.2.5 Revisión de derechos de acceso de usuarios Se deberían utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos La identificación automática de los equipos se debería considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos Se debería controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración Los grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes. En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debería restringirse la capacidad de los usuarios para conectarse a la red, esto debería hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales **A. 13 Seguridad en las Comunicaciones** Se deberían implantar controles de encaminamiento (routing) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R53	SI200	Errores de los usuarios	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[SI] Sistema de Información	R54	SI200	Errores del administrador	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[SI] Sistema de Información	R55	SI200	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	Riesgo		Amenaza	Probabilidad		Impacto		Riesgo	controles	
[SI] Sistema de Información	R56	SI200	Denegación de servicio	Medio (2)	2	Alto (3)	3	6	Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones Debería establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. Debería desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio. **A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información	* Reducir el riesgo
[SI] Sistema de Información	R67	SI300	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	Riesgo		Amenaza	Probabilidad		Impacto		Riesgo	controles	
[HW] Hardware / Equipos informáticos	R91	HW100	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R93	HW100	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R94	HW100	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R102	HW200	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[HW] Hardware / Equipos informáticos	R104	HW200	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R105	HW200	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R113	HW300	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[HW] Hardware / Equipos informáticos	R115	HW300	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R116	HW300	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[M] Soportes de información	R122	M100	Alteración de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[M] Soportes de información	R123	M100	Corrupción de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[M] Soportes de información	R124	M100	Destrucción de información	Medio (2)	2	Alto (3)	3	6	**A.8.2 Clasificación de la información de la organización"** Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo
[M] Soportes de información	R126	M100	Degradación de los soportes de almacenamiento de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[M] Soportes de información	R127	M100	Difusión de software dañino	Medio (2)	2	Alto (3)	3	6	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.	* Reducir el riesgo
[M] Soportes de información	R128	M100	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[M] Soportes de información	R129	M100	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[COM] Redes de comunicaciones	R135	COM 100_	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo
[COM] Redes de comunicaciones	R136	COM 100_	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[COM] Redes de comunicaciones	R137	COM 100_	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[COM] Redes de comunicaciones	R138	COM 100_	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. **A.7.2.3 Proceso disciplinario** Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[COM] Redes de comunicaciones	R142	COM 200_	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 11.1.4 Protección contra amenazas externas y del ambiente** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo
[COM] Redes de comunicaciones	R143	COM 200_	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. A.7.2.3 Proceso disciplinario Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[COM] Redes de comunicaciones	R144	COM 200_	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[COM] Redes de comunicaciones	R145	COM 200_	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[S] Servicios	R171	S100	Alteración de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[S] Servicios	R172	S100	Corrupción de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[S] Servicios	R173	S100	Destrucción de información	Medio (2)	2	Alto (3)	3	6	**A.8.2 Clasificación de la información de la organización"** Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo
[S] Servicios	R177	S100	Fallo de servicios de comunicaciones	Medio (2)	2	Alto (3)	3	6	**A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[S] Servicios	R178	S100	Degradación de los soportes de almacenamiento de la información	Medio (2)	2	Alto (3)	3	6	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
[S] Servicios	R179	S100	Difusión de software dañino	Medio (2)	2	Alto (3)	3	6	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.	* Reducir el riesgo
[S] Servicios	R180	S100	Errores de mantenimiento / actualización de programas (software)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[S] Servicios	R181	S100	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[S] Servicios	R182	S100	Caída del sistema por sobrecarga	Medio (2)	2	Alto (3)	3	6	**A.12.1.3 Gestión de la capacidad** La utilización de los recursos se debería supervisar y ajustar, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	* Reducir el riesgo
[S] Servicios	R185	S100	Abuso de privilegios de acceso	Medio (2)	2	Alto (3)	3	6	**A.9.2 Gestión de accesos de usuario** La asignación y el uso de privilegios deberían estar restringidos y controlados. **A.9.1 Requerimientos de negocio para el control de acceso** Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso. **A.9.2.5Revisión de los derechos de acceso de usuario** La Dirección debería revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	Riesgo		Amenaza	Probabilidad		Impacto		Riesgo	controles	
[S] Servicios	R186	S100	Acceso no autorizado	Medio (2)	2	Alto (3)	3	6	A.9.2.5 Revisión de derechos de acceso de usuarios Se deberían utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos La identificación automática de los equipos se debería considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos Se debería controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración Los grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes. En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debería restringirse la capacidad de los usuarios para conectarse a la red, esto debería hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales **A. 13 Seguridad en las Comunicaciones** Se deberían implantar controles de encaminamiento (routing) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.	* Reducir el riesgo
[S] Servicios	R187	S100	Errores de los usuarios	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[S] Servicios	R188	S100	Errores del administrador	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo
[S] Servicios	R189	S100	Errores de configuración	Medio (2)	2	Alto (3)	3	6	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[S] Servicios	R190	S100	Denegación de servicio	Medio (2)	2	Alto (3)	3	6	Los fallos deberían ser registrados y analizados y se deberían tomar las correspondientes acciones Debería establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Debería desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio. **A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información	* Compartir o transferir el riesgo
[D] Datos / Información	R6	D100	Interceptación de información (escucha)	Medio (2)	2	Medio (2)	2	4	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación **A.13.2 Transferencia de información** Deberían establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros Durante el transporte fuera de los límites físicos de la organización,	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
									los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro	
[D] Datos / Información	R16	D100	Ingeniería social	Medio (2)	2	Medio (2)	2	4	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	* Reducir el riesgo
[SI] Sistema de Información	R22	SI100	Interceptación de información (escucha)	Medio (2)	2	Medio (2)	2	4	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación **A.13.2 Transferencia de información** Deberían establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R26	SI100	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	Medio (2)	2	4	**A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información Deberían desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos críticos de negocio.	* Compartir o transferir el riesgo
[SI] Sistema de Información	R37	SI100	Ingeniería social	Medio (2)	2	Medio (2)	2	4	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	* Reducir el riesgo
[SI] Sistema de Información	R43	SI200	Interceptación de información (escucha)	Medio (2)	2	Medio (2)	2	4	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación Deberían establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R47	SI200	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	Medio (2)	2	4	**A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información Deberían desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos críticos de negocio.	* Compartir o transferir el riesgo
[SI] Sistema de Información	R58	SI200	Ingeniería social	Medio (2)	2	Medio (2)	2	4	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	* Reducir el riesgo
[SI] Sistema de Información	R64	SI300	Interceptación de información (escucha)	Medio (2)	2	Medio (2)	2	4	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación Deberían establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[SI] Sistema de Información	R79	SI300	Ingeniería social	Medio (2)	2	Medio (2)	2	4	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R92	HW100	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	Medio (2)	2	4	**A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información Deberían desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos críticos de negocio.	* Reducir el riesgo
[HW] Hardware / Equipos informáticos	R103	HW200	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	Medio (2)	2	4	**A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información Deberían desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos críticos de negocio.	* Reducir el riesgo

Tabla 13. (Continuación)

ANÁLISIS DE RIESGOS										OPCIONES DE MANEJO
Activo	**Riesgo**		**Amenaza**	**Probabilidad**		**Impacto**		**Riesgo**	**controles**	
[HW] Hardware / Equipos informáticos	R114	HW300	Interrupción de otros servicios y suministros esenciales	Medio (2)	2	Medio (2)	2	4	**A. 17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio** Deberían identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información Deberían desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos críticos de negocio.	* Compartir o transferir el riesgo
[S] Servicios	R174	S100	Interceptación de información (escucha)	Medio (2)	2	Medio (2)	2	4	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación Deberían establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro	* Reducir el riesgo
[S] Servicios	R192	S100	Ingeniería social	Medio (2)	2	Medio (2)	2	4	**A.7.2.2 Conciencia, educación y entrenamiento de seguridad de la información** Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	* Reducir el riesgo

Fuente autores, Fundamentado en la metodología Margerit

6. DIVULGACIÓN

Se realizó mediante una reunión, con el departamento de TIC de la universidad Santo Tomás sede Bogotá, ver informe anexo 2, Informe De Auditoría.

Adicionalmente este documento se publicará en el repositorio de la Universidad Nacional Abierta y a distancia.

7. INFORME FINAL PARA EL MEJORAMIENTO DE LA SEGURIDAD.

INTRODUCCIÓN

El presente trabajo presenta el informe de los resultados encontrados en el análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial, puesto que el uso de estas por la comunidad educativa, es una política institucional obligatoria para los docentes de Tiempo Completo (TC) y Medio Tiempo (MT), al volverse una política el uso de las Aulas virtuales, el uso de éstas aumenta por parte de docentes y estudiantes y la posibilidad de un ataque informáticos se convierte en un peligro eminente.

El evaluar la seguridad y el control de información de las aulas virtuales es muy importante, puesto que en esta se registran notas y trabajos de los estudiantes, y material de producción intelectual de los docentes, la perdida de en esta información, generaría problemas instituciones, que le generarían perdida económicas a la universidad; la verificación de que si cumplen y aplican los controles, políticas de acuerdo a la norma ISO 27001: 2013, contribuye a la estabilidad académica en la instrucción.

OBJETIVO

Verificar los riesgos de Seguridad según la norma ISO 27001 en las Aulas Virtuales de la Universidad Santo Tomás.

Objetivos Específicos

- Realizar un diagnóstico de la situación actual de la seguridad de las aulas virtuales, Identificación y Análisis de Vulnerabilidades, en la universidad Santo Tomás en relación con la norma ISO 27001.
- Elaborar el informe final de los resultados para establecer el plan de mejoramiento de la seguridad según los requerimientos de la norma ISO 27001 para mejorar el desempeño de la organización.

ALCANCE

Estado los riesgos de Seguridad según la norma ISO 27001 en las Aulas Virtuales De La Universidad Santo Tomás sede Bogotá.

EXCLUSIONES: Se centró únicamente en Análisis de Riesgos según la ISO 27001 de las aulas virtuales de la USTA

CRITERIOS

norma ISO 27001

Técnicas y Procedimientos: Plan Auditoría Interna

EQUIPO AUDITOR
Líder Equipo Auditor: Vivian Andrea García
Auditor 1 Jhon Jarby Ortiz
Experto Técnico:
Responsable del Punto auditado: Calos Ángel Rocha

TIPO AUDITORIA: Interna

SITIO: sede Principal

HALLAZGOS

- **Resultados del GAP**

ayudarte a ver el nivel de implementación de la ISO 27001 en la organización, observa si está en un estado inicial o si te queda poco para alcanzar el nivel de implementación adecuado

Tabla 1

Cantidad	Códigos Status	Significado	Porcentaje de implementación %
10	**D**	El control se documentó e implementó	**8%**
108	**MD**	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	**92%**
	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	**0%**
	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	**0%**
	NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	**0%**
117			

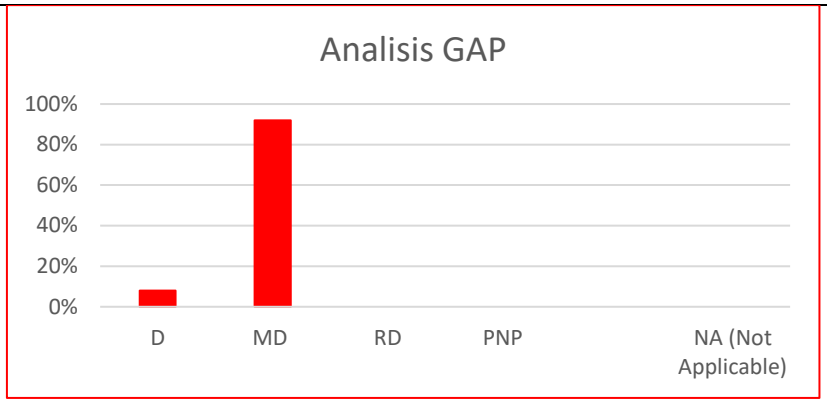
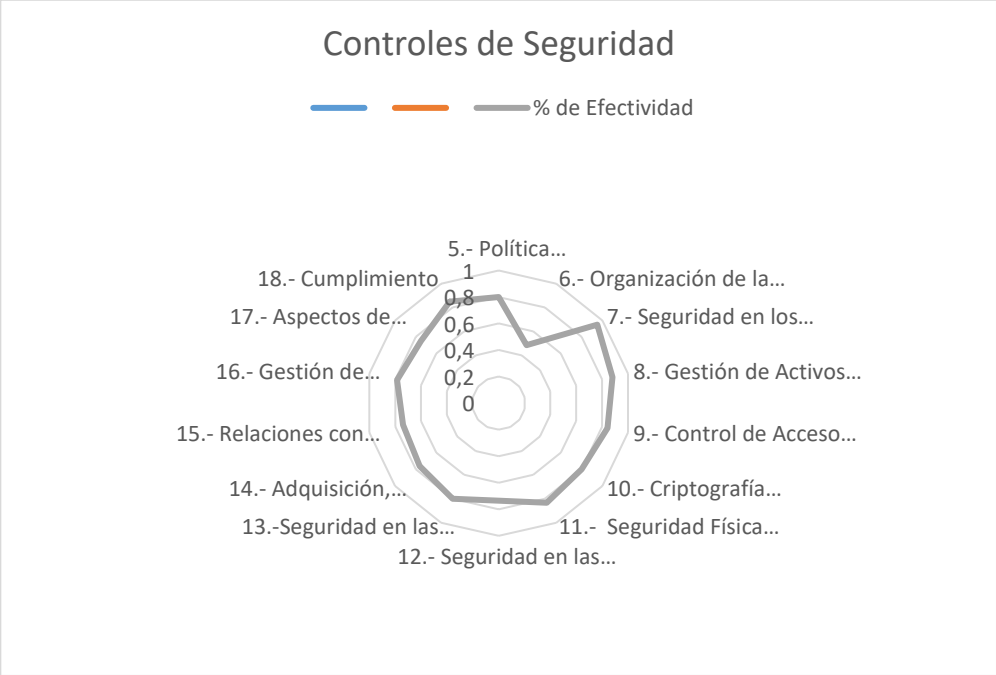


Tabla 2 Análisis de porcentaje de efectividad *Declaración de Aplicabilidad (*SoA *por las siglas en inglés de* Statement of Applicability

Dominio	% de Efectividad
5.- Política De Seguridad	80%
6.- Organización de la Seguridad de la Información Organizativos de la SI	49%
7.- Seguridad en os Recursos Humanos	95%
8.- Gestión de Activos A RRHH	88%
9.- Control de Acceso Y del entorno	84%
10.- Criptografía y Operaciones	80%
11.- Seguridad Física y del Entorno De acceso	83%
12.- Seguridad en las Operaciones Desarrollo y Mantenimiento De los SI	74%
13.-Seguridad en las Comunicaciones Incidentes de SI	80%
14.- Adquisición, Desarrollo y Mantenimiento de Sistemas Del negocio	76%
15.- Relaciones con Proveedores	74%
16.- Gestión de Incidentes de Seguridad de la Información	79%
17.- Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	75%
18.- Cumplimiento	85%

Gráfica 2 *Informe* Grafica radar de la efectividad de acuerdo a la norma ISO 27001



De los resultados obtenidos se Observa:

- En Análisis GAP nos muestra El 8% de los controles están documentados, El 92% de los controles, se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos, la empresa está en proceso de construcción y aprobación de los documentos.

- De acuerdo a el análisis, Declaración de Aplicabilidad (*SoA* por las siglas en inglés de *Statement of Applicability* se visualiza:

  el ítem más bajo obtenido Organización de la Seguridad de la Información Organizativos de la Sistema de información (SI), con un 49% esto se debe a que la organización está en proceso de documentar sus procesos.
  El más alto con el 95% es Seguridad en los Recursos Humanos, que es un proceso que se viene trabajando e implementado hace varios años en la universidad, pero hace 2 se lleva el control total.
  En cuanto los otro ítem se obtuvo la Política de Seguridad está en 80%, está en construcción y falta la aprobación total de esta, la Gestión de Activos A RRHH, 88%,estos están identificados, documentados, los Control de Acceso y del entorno 84% se viene implementados desde hace 2 años, Criptografía se obtuvo Operaciones 80% falta documenta alguno procesos e implementación en un 100%, la Seguridad Física y del Entorno de acceso es 83% se tiene controlados el 90% de los espacios pero falta documentar proceso y centro lar el 10% de los espacios, la Seguridad en las Operaciones, Desarrollo y Mantenimiento De los SI se obtuvo un 80%, se está realizando falta la evolución de que tan efectivo es la forma como se realiza,-Seguridad

en las Comunicaciones Incidentes de SI 80%, la adquisición, Desarrollo y Mantenimiento de Sistemas del negocio 76% se realiza adquisidores de nuevos equipos pero priman los temas monetarios en algunos casos que las necesidades, relaciones con Proveedores 74% se tiene varios proveedores, a relación es bueno pero debido a la documentación que se les solicita haces se pierden estos, la Gestión de Incidentes de Seguridad de la Información 79% se están documentando y se generan acciones para corregirlas, pero están en proceso de implementación, Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio 75% y Cumplimiento porque están en proceso de implementación 85%.

Mapa de Riesgos

Criterios de aceptación del riesgo

Rango Descripción

Riesgo <= 4 La organización considera el riesgo poco reseñable.

Riesgo > 4 La organización considera el riesgo reseñable, es decir de alto impacto y debe proceder a su tratamiento.

Tabla 3 de Impacto

Impacto	Alto	3	6	9
	Medio	2	4	6
	Bajo	1	2	3
		Bajo	Medio	Alto
	Probabilidad			

Tabla 4 Activos Afectados con Alto riesgo

COD	TIPO DE ACTIVO	ACTIVOS	DESCRIPCIÓN	Riesgo
SI100	[SI] Sistema de Información	aplicaciones PHP	Moodle	9
SI200	[SI] Sistema de Información	Correo electrónico	Servicio corporativo Gmail	9
SI300	[SW] Software / Aplicativos	Servidores WEB	Apache	9

Tabla 5 Análisis de riesgos altos

ANÁLISIS DE RIESGOS									OPCIONES DE MANEJO
Riesgo	Activos	Amenaza	Probabilidad		Impacto		Riesgo	controles	
R17 R38	SI100 SI200	Fuga de información	Alto (3)	3	Alto (3)	3	9	**A. 6 Organización de la Seguridad de la Información** Deberían evitarse las situaciones que permitan que se produzcan fugas de información **A.8.3.1 Gestión de medios removibles** Se deberían establecer procedimientos para la gestión de los soportes extraíbles **A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información** Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación **A.8.2 Clasificación de la información** Deberían establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **A.12.1.1 Documentación de procedimientos operacionales** La documentación del sistema debería estar protegida contra accesos no autorizados.	* Reducir el riesgo
R62	SI300	Corrupción de la información	Alto (3)	3	Alto (3)	3	9	**A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberían incorporar comprobaciones de validación en las aplicaciones. **A.17.2.1 Disponibilidad de facilidades de procesamiento de información** Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.	* Reducir el riesgo
R63	SI300	Destrucción de información	Alto (3)	3	Alto (3)	3	9	**A.8.2 Clasificación de la información de la organización"** Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.	* Reducir el riesgo
R69	SI300	Difusión de software dañino	Alto (3)	3	Alto (3)	3	9	**A.12.2.1 Controles contra software malicioso** Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían	* Reducir el riesgo

								implantar procedimientos adecuados de concienciación del usuario.	

Según la tabla de riesgos obtenemos el siguiente mapa de riesgos

Tabla 6 Mapa de riesgos

Impacto	Alto	R8 , R23 , R24 , R44 , R45 , R59 , R60 , R61 , R65 , R66 , R70 , R71 , R72 , R73 , R74 , R75 , R76 , R77 , R80 , R81 , R82 , R83 , R84 , R85 , R86 , R87 , R88 , R89 , R90 , R95 , R96 , R97 , R98 , R99 , R100 , R101 , R106 , R107 , R108 , R109 , R110 , R111 , R112 , R117 , R118 , R119 , R120 , R121 , R125 , R130 , R132 , R133 , R134 , R139 , R140 , R141 , R150 , R151 , R152 , R153 , R154 , R155 , R157 , R158 , R159 , R160 , R161 , R162 , R164 , R165 , R166 , R167 , R168 , R169 , R175 , R176 , R183	R1 , R2 , R3 , R4 , R5 , R7 , R9 , R10 , R11 , R12 , R13 , R14 , R18 , R19 , R20 , R21 , R25 , R27 , R28 , R29 , R30 , R31 , R32 , R33 , R34 , R35 , R39 , R40 , R41 , R42 , R46 , R48 , R49 , R50 , R51 , R52 , R53 , R54 , R55 , R56 , R67 , R91 , R93 , R94 , R102 , R104 , R105 , R113 , R115 , R116 , R122 , R123 , R124 , R126 , R127 , R128 , R129 , R135 , R136 , R137 , R138 , R142 , R143 , R144 , R145 , R171 , R172 , R173 , R177 , R178 , R179 , R180 , R181 , R182 , R185 , R186 , R187 , R188 , R189 , R190	R17 , R38 , R62 , R63 , R69
	Medio	R68	R6 , R16 , R22 , R26 , R37 , R43 , R47 , R58 , R64 , R79 , R92 , R103 , R114 , R174 , R192	R1 , R2 , R3 , R4 , R5 , R7 , R9 , R10 , R11 , R12 , R13 , R14 , R18 , R19 , R20 , R21 , R25 , R27 , R28 , R29 , R30 , R31 , R32 , R33 , R34 , R35 , R39 , R40 , R41 , R42 , R46 , R48 , R49 , R50 , R51 , R52 , R53 , R54 , R55 , R56 , R67 , R91 , R93 , R94 , R102 , R104 , R105 , R113 , R115 , R116 , R122 , R123 , R124 , R126 , R127 , R128 , R129 , R135 , R136 , R137 , R138 , R142 , R143 , R144 , R145 , R171 , R172 , R173 , R177 , R178 , R179 , R180 , R181 , R182 , R185 , R186 , R187 , R188 , R189 , R190
	Bajo	R15 , R36 , R57 , R78 , R131 , R146 , R147 , R148 , R149 , R156 , R163 , R170 , R184 , R191 , R193	R68	R8 , R23 , R24 , R44 , R45 , R59 , R60 , R61 , R65 , R66 , R70 , R71 , R72 , R73 , R74 , R75 , R76 , R77 , R80 , R81 , R82 , R83 , R84 , R85 , R86 , R87 , R88 , R89 , R90 , R95 , R96 , R97 , R98 , R99 , R100 , R101 , R106 , R107 , R108 , R109 , R110 , R111 , R112 , R117 , R118 , R119 , R120 , R121 , R125 , R130 , R132 , R133 , R134 , R139 , R140 , R141 , R150 , R151 , R152 , R153 , R154 , R155 , R157 , R158 , R159 , R160 , R161 , R162 , R164 , R165 , R166 , R167 , R168 , R169 , R175 , R176 , R183
		Bajo	Medio	Alto
	Probabilidad			

Conclusiones

- Políticas de seguridad de seguridad están en construcción, pero las viene implementando; el Manual de funciones y competencias laborales, están en construcción, pero se viene implementando.
- Procesos y procedimientos cuentan con estos y los tiene documentados.
- El Inventario de activos cuentan con este y hacen seguimiento al inventario desde hace 2 años.

- Portafolio de servicios cuentan con estos, pero están en construcción socializarlos a la comunidad educativa.
- Registro de problemas e incidentes: cuentan con el seguimiento y toman medida para mitigarlos.
- Los activos aplicaciones PHP, Correo electrónico, Servidores WEB, están en alto riesgo de Fuga de información, Corrupción de la información, Destrucción de información, Difusión de software dañino.

RECOMENDACIONES

- Realizar un Plan de Tratamiento del Riesgo, así como un plan de acción sobre cómo implementar los diversos controles definidos por la Declaración de Aplicabilidad.
- Desarrollar procedimientos de evaluación y tratamiento de riesgos
- se deberían evitarse las situaciones que permitan que se produzcan fugas de información
- Con respecto a los riesgos encontrados se sugiere:

- Establecer procedimientos para la gestión de los soportes extraíbles.
- Establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación
- Establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.

- La documentación del sistema deberá estar protegida contra accesos no autorizados.
- Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se debe incorporar comprobaciones de validación en las aplicaciones.
- realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.
- Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.
- implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario del sistema y sus conclusiones finales.

RESULTADO E IMPACTOS

Los activos aplicaciones PHP, Correo electrónico, Servidores WEB, están en alto riesgo de Fuga de información, Corrupción de la información, Destrucción de información, Difusión de software dañino.

En cuanto a los riesgos de riesgo medio y bajo, es indispensable iniciar de forma escalonada, las acciones es decir iniciar con acciones para reducir el riesgo, continuar con procesos para evitar el riesgo

Se recomienda que, aunque La organización use controles debe tomar medidas frente a los riesgos de riesgo medio, es indispensable iniciar de forma escalonada, con los siguientes controles del anexo 1 de la 2001:

A. 6 Organización de la Seguridad de la Información

A.8.3.1 Gestión de medios removibles

A.17.2.1 Disponibilidad de facilidades de procesamiento de información, A.13.2 Transferencia de información

A.8.2 Clasificación de la información

A.12.1.1 Documentación de procedimientos operacionales

A.17.2.1 Disponibilidad de facilidades de procesamiento de información

A.17.2.1 Disponibilidad de facilidades de procesamiento de información

A.8.2 Clasificación de la información

A.12.2.1 Controles contra software malicioso

Frente a los riesgos analizados, se recomienda realizar de forma simultanea de preferencia acciones como * Reducir el riesgo, y de ser necesario Compartir o transferir el riesgo mediante la contratación de expertos externos.

El impacto esperado es que la organización tome más conciencia sobre las amenazas y vulnerabilidades, aceptando las recomendaciones dadas y realice un plan de acción para mitigar los riesgos y el proceso de mejora continua.

CONCLUSIONES

Se Determinaron los riesgos de Seguridad Mediante la aplicación de una auditoría según la norma ISO 27001 en las Aulas Virtuales De La Universidad Santo Tomás, debidos a que la ISO 27001, una norma que define el sistema de gestión de seguridad de la información (SGSI). La implementación de esta, es el comienzo al camino de la certificación en ISO 27001 en la Universidad Santo Tomás.

El plan de auditoria que se elaboró y se implementó se hizo, con el fin de hacer el diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás en relación con la norma ISO 27001.

Al Realizar un diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás, en relación con la norma ISO 27001, se pudo establecer que más alto riesgo, se encontró en los activos aplicaciones php, correo electrónico, servidores web; los riegos detectados fueron fuga de información, corrupción de la información, destrucción de información, difusión de software dañino. Por tanto, la organización debe implementar los controles indicados para mitigar estos riesgos.

Al elaborar el informe final, según los requerimientos de la norma ISO 27001 para mejorar el desempeño de la organización, se encontró que, en la actualidad, la universidad Santo Tomás cuenta con un sistema de gestión de información con:

- Las políticas en construcción, pero estas se vienen implementando.
- El manual de funciones y competencias laborales en construcción, pero se viene implementando.
- Los procesos están definidos y los procedimientos están documentados.
- El inventario de activos y se realiza seguimiento al inventario desde hace 2 años.
- Su portafolio de servicios está definido, sin embargo, aún está en construcción ya falta socializarlos a la comunidad educativa.
- Realiza el registro de problemas e incidentes, con el seguimiento y medidas para mitigarlos.

RECOMENDACIONES

En base a la investigación realizada se sugiere las siguientes acciones para mitigar las amenazas y riesgos encontrados:

- Realizar un Plan de tratamiento del riesgo, así como un plan de acción sobre cómo implementar los diversos controles definidos por la Declaración de Aplicabilidad.

- Desarrollar procedimientos de evaluación y tratamiento de riesgos.

- Evitar las situaciones que permitan que se produzcan fugas de información.

Con respecto a los riesgos encontrados se sugiere:

- Establecer procedimientos para la gestión de los soportes extraíbles.

- Establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

- Establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.
- La documentación del sistema deberá estar protegida contra accesos no autorizados.

- Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se debe incorporar comprobaciones de validación en las aplicaciones.

- Realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.

- Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.

- Implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario del sistema y sus conclusiones finales.

BIBLIOGRAFÍA

AGUIRRE, Diego y PALACIO, Jhon. 2014. Evaluación Técnica De Seguridades Del Data Center Del Municipio De Quito Según Las Normas ISO/IEC 27001:2005 Sgsie Iso/Iec 27002:2005. Quito: Universidad De Fuerzas Armadas Espe Maestría De Evaluación Y Auditoria De Sistemas Tecnológicos, 2014.

AMERICAN ACCOUNTING ASSOCIATION. 1972. Auditing Concepts Committee. Reports of the Committee on Basis Concepts. 1972. Vol. 47.

AVILA ARZUZA, Maribel. 2012. Implantación de un SGSI. Barcelona: Universitat Oberta de Catalunya, 2012.

Chamorro, Alejandro. 2012. MODELO PARA LA EVALUACION EN SEGURIDAD INFORMÁTICA A PRODUCTOS SOFTWARE, BASADO EN EL ESTÁNDAR ISO/IEC 15408 COMMON CRITERIA. Cali: Universidad ICESI Maestría en Gestión de Informática y Telecomunicaciones, 2012.

Colombia, El Congreso de. 1999. alcaldiabogot. [Online]1999. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

EL CONGRESO DE COLOMBIA. 2009. Alcaldia Bogotá. [Online] 2009. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

—. 2009. Alcaldia Bogotá. [Online]2009. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913.

—. 2012. alcaldiabogotá. [Online]2012. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

El CONGRESO DE LA REPUBlICA. 2008. Superintndencia de Industria y Comercio. [Online] 2008. http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf.

ICONTEC. 2009. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana. Bogotá: s.n., 2009.

ISO. 2004. ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management. 2004.

—. 2005. ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements. 2005.

—. 2005. ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management. 2005.

—. 2008. ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management. 2008.

La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes. Cano, Jeimy J. 2011. 2011, ISACA Journal Online, Vol. 5.

MEJÍA, Guillermo and Cuéllar, Adolfo. 2003. Teoría General de la Auditoría y Revisoría Fiscal. [Online] 2003. http://fccea.unicauca.edu.co/old/tgarf/.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS , versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.Libro I - Método, Madrid, 2012.

OSORIO, Yenis and Pérez, Yesica. 2012. Diseño de una Política de Gestión de Riesgos de la Información. Ocaña: Universidad Francisco De Paula Santander Ocaña Especialización en Auditoria de Sistemas., 2012.

PERAFÁN, Jhon and Caicedo, Mildred. 2014. Análisis de Riesgos de la Seguridad de la Información para la Institución. Popayán: Universidad Nacional Abierta y a Distancia Especialización en Seguridad Informática, 2014.

POTER, Thomas y BURTON, William. 1993. Auditoría un enfoque conceptual. México: Limusa, 1993.

SAMPIERI, Roberto, Fernández, Carlos and Baptista, Pilar. 2015. Metodología de la invetigación. Mexico: Mc Graw Hill, 2015.

SANDOVAL, Cesar. 2014. Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una. Guayaquil: Universidad Católica Santiago de Guayaquil Maestría en Telecomunicaciones, 2014.

UNIVERSIDAD NACIONAL DE LUJÁN. seguridad informática. [Online] http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf.

UDIGITALRM. 2011. Guía de la seguridad de la Información para PYMES. Recuperado el Diciembre de 2016, de https://ingtecnologia.files.wordpress.com/2011/06/gestion-de-la-seguridad-de-la-informacion.pdf

WWW.ISO27000.ES. 2012. Sistema de Gestión de la Seguridad de la Información. Madrid: s.n., 2012.

ANEXOS

Anexo A Plan de auditoría

PLAN DE AUDITORIA
OBJETIVO: Verificar los riesgos de Seguridad según la norma ISO 27001 en las Aulas Virtuales de la Universidad Santo Tomás. • **Realizar un diagnóstico de la situación actual de la seguridad de las aulas virtuales, Identificación y Análisis de Vulnerabilidades, en la universidad Santo Tomás en relación con la norma ISO 27001.** • **Elaborar el informe final de los resultados para establecer el plan de mejoramiento de la seguridad según los requerimientos de la norma ISO 27001 para mejorar el desempeño de la organización.**
ALCANCE: Estado los riesgos de Seguridad según la norma ISO 27001 en las Aulas Virtuales De La Universidad Santo Tomás sede Bogotá.
CRITERIOS: norma ISO 27001
Técnicas y Procedimientos: Plan Auditoría Interna
EQUIPO AUDITOR: Líder Equipo Auditor: Vivian García Auditor 1 Jhon Ortiz **Experto Técnico:**
Responsable del Punto auditado: Calos Ángel Rocha
TIPO AUDITORIA: Interna
FECHA: 12 octubre de 2016 SITIO: sede Principal HORA: 8:00 am
Reunión de apertura: Departamento de TIC HORA: 8:00 am
Reunión de cierre: 14 de octubre de 2016 HORA: 6:00 pm
EXCLUSIONES: Se centrará únicamente en Análisis de Riesgos según la ISO 27001 de las aulas virtuales de la USTA

PROCESO Y/O ACTIVIDAD	REQUISITO POR AUDITAR NTC ISO 27001:2013	AUDITADOS CARGO Y NOMBRE	AUDITOR	FECHA	HORA	Lugar/Regional/Centro zonal
Etapa 1 “Planificación						
Etapa 2 diagnóstico de la situación actual de la seguridad de las aulas virtuales de acuerdo a la norma ISO 27001.						
Etapa 3 “Análisis de riesgos”						
Etapa 4 informe final de los resultados						

(1) La iniciación, terminación y horarios de la auditoría se adecuarán de acuerdo con el desplazamiento de auditores
OBSERVACIONES:
La información que se conocerá por la ejecución de esta Auditoría será tratada confidencialmente, por parte del equipo de auditores.
La duración de las entrevistas puede variar dependiendo de la organización de la documentación y los registros
Durante el desarrollo de la auditoría a los procesos de Aulas virtuales, se verificará en cada uno de ellos los respectivos Indicadores

Elaborado: _____Revisado: _____ Aprobado: _____

Anexo B RAE

Título de Documento.	ANÁLISIS DE RIESGOS SEGÚN LA NORMA ISO 27001 PARA LAS AULAS VIRTUALES DE LA UNIVERSIDAD SANTO TOMAS MODALIDAD PRESENCIAL
Autor	GARCÍA BALGUERA Vivian Andrea ORTIZ GONZÁLEZ Jhon Jarby
Palabras Claves	Análisis de Riesgo, ISO 27001
Descripción	El presente trabajo es una Investigación descriptiva, que consistió en determinar los riesgos de la seguridad de la información, en las aulas virtuales de la modalidad presencial, en la Universidad Santo Tomás, según la norma ISO 27001:2013, para esto se elaboró un plan de Auditoría fundamentado en la norma ISO 27001:2013, se realiza un diagnóstico de la situación actual de la seguridad de las aulas virtuales, según la norma mencionada, y finalmente de se elabora un informe final con los resultados para establecer el plan de mejoramiento.
Fuentes Bibliográficas	Aguirre, D., & Palacio, j. (2014). Evaluación Técnica De Seguridades Del Data Center Del Municipio De Quito Según Las Normas Iso/Iec 27001:2005 Sgsie ISO/Iec 27002:2005. Quito: Universidad De Fuerzas Armadas Espe Maestría De Evaluación Y Auditoria De Sistemas Tecnológicos. AMERICAN ACCOUNTING ASSOCIATION. (1972). Auditing Concepts Committee. Reports of the Committee on Basis Concepts (Vol. 47). AVILA ARZUZA, M. (2012). Implantación de un SGSI. Barcelona: Universitat Oberta de Catalunya. Cano, J. J. (2011). La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes. ISACA Journal Online, 5. Chamorro, A. (2012). MODELO PARA LA EVALUACION EN SEGURIDAD INFORMÁTICA A PRODUCTOS SOFTWARE, BASADO EN EL ESTÁNDAR ISO/IEC 15408 COMMON CRITERIA. Cali: Universidad ICESI Maestría en Gestión de Informática y Telecomunicaciones. Colombia, E. C. (1999). Alcaldía Bogotá. Recuperado el 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276 L CONGRESO DE COLOMBIA. (2009). Alcaldía Bogotá. Recuperado el 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 EL CONGRESO DE COLOMBIA. (2009). Alcaldía Bogotá. Recuperado el 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913 EL CONGRESO DE COLOMBIA. (2012). Alcaldía bogotá. Recuperado el 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981 El CONGRESO DE LA REPUBlICA. (2008). Superintendencia de Industria y Comercio. Recuperado el 2016, de http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf

	ICONTEC. (2009). Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana. Bogotá. ISO. (2004). ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management. ISO. (2005). ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements. ISO. (2005). ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management. ISO. (2008). ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management.

Contenido:

El presente trabajo, consistió en determinar los riesgos de seguridad según la norma ISO 27001:2013 en las aulas virtuales de la Universidad Santo Tomás modalidad presencial, esta necesidad, surge debido a que el uso de las aulas virtuales se convierte en política institucional obligatoria para los docentes de Tiempo Completo (TC) y Medio Tiempo (MT); en las Aulas virtuales se registran notas y trabajos de los estudiantes, y material de producción intelectual de los docentes por tanto se debe verificar la información de las aulas virtuales se rige tres principios básicos que dictamina el estándar internacional los cuales son: la confidencialidad, integridad y disponibilidad, demostrando que se aplican las mejores prácticas, en cuanto al manejo de información generando tranquilidad Institucional, tanto a los docentes y estudiantes al usar estas; por tanto se necesita evaluar la seguridad y el control de información de las aulas virtuales cumple y aplican los controles, políticas de acuerdo a la norma ISO 27001: 2013, p

Para estos se realizaron los siguientes objetivos:

GENERAL

Determinar los riesgos de Seguridad Mediante la aplicación de una auditoría según la norma ISO 27001 en las Aulas Virtuales De La Universidad Santo Tomás.

OBJETIVOS ESPECÍFICOS

- Elaborar un plan de Auditoría según la norma ISO 27001.
- Realizar un diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás en relación con la norma ISO 27001.
- Elaborar el informe final de los resultados para establecer el plan de mejoramiento de la seguridad según los requerimientos de la norma ISO 27001 para mejorar el desempeño de la organización.

Para el desarrollo del proyecto se realizó una Investigación Aplicada, en donde se desarrollaron los siguientes pasos:

Análisis fuentes teóricas:
se consultarán diversas fuentes con relación al análisis de riesgos en la seguridad informática y se decidió la norma ISO 27001 para análisis de riesgos

Definición de los objetivos del proyecto y delimitación del alcance de acuerdo al problema planteado:
Se elaboró el plan de auditoria que se presenta en el anexo 1 y el 14 de octubre de 2016 se implementó con el fin de hacer el diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás en relación con la norma ISO 27001:
Diagnóstico de la situación actual
En esta etapa se desarrollarán las siguientes actividades:

Levantamiento de información e identificación de los activos de información que componen el proceso alcance del sistema SGSI, a través de la aplicación de metodologías que contemplen entrevistas y formatos.

Metodología

Se realizó una Investigación aplicada, ésta consiste según los autores consultados en resolver un problema, a través de la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación; para esta investigación es identificar y mitigar los riesgos informáticos que se pueden presentar o que se están presentando en las aulas virtuales de la USTA, tratando y de dar una solución a la problemática identificada.

Metodología de Desarrollo

Los pasos que se implementaron para desarrollar el trabajo propuesto
Análisis fuentes teóricas:
se consultarán diversas fuentes con relación al análisis de riesgos en la seguridad informática y se decidió la norma ISO 27001 para análisis de riesgos.

Definición de los objetivos del proyecto y delimitación del alcance de acuerdo al problema planteado:

Se elaboró el plan de auditoria que se presenta en el anexo 1 y el 14 de octubre de 2016 se implementó con el fin de hacer el diagnóstico de la situación actual de la seguridad de las aulas virtuales en la universidad Santo Tomás en relación con la norma ISO 27001:

Diagnóstico de la situación actual

En esta etapa se desarrollarán las siguientes actividades:

- Levantamiento de información e identificación de los activos de información que componen el proceso alcance del sistema SGSI, a través de la aplicación de metodologías que contemplen entrevistas y formatos.

Análisis de Activos y su Valoración

Se analizaron los activos, se determinaron las amenazas y riesgos, con la metodología Magerit

Conclusiones

La universidad Santo Tomás actualmente su sistema de gestión de la información cuenta:

- Las políticas de seguridad de seguridad en construcción, pero estas se las viene implementando:
- El manual de funciones y competencias laborales en construcción, pero se viene implementando.
- Los procesos están definidos y los procedimientos están documentados.
- El inventario de activos y se realiza seguimiento al inventario desde hace 2 años.
- Su portafolio de servicios está definido, sin embargo, aún está en construcción ya falta socializarlos a la comunidad educativa.
- Realiza el registro de problemas e incidentes con el seguimiento y medidas para mitigarlos.

El riesgo más alto se encontró en los activos aplicaciones php, correo electrónico, servidores web, este consiste en fuga de información, corrupción de la información, destrucción de información, difusión de software dañino. Por tanto, la organización debe implementar los controles indicados para mitigar este riesgo

La ISO 27001, es una norma que define el sistema de gestión de seguridad de la información (SGSI). Por tanto, la implementación de esta es el comienzo del camino hacia la certificación en ISO 27001

Recomendaciones

- Realizar un Plan de tratamiento del riesgo, así como un plan de acción sobre cómo implementar los diversos controles definidos por la Declaración de Aplicabilidad.
- Desarrollar procedimientos de evaluación y tratamiento de riesgos, evitar las situaciones que permitan que se produzcan fugas de información
- Con respecto a los riesgos encontrados se sugiere:
    - Establecer procedimientos para la gestión de los soportes extraíbles.
    - Establecerse políticas, procedimientos y controles formales que protejan el

intercambio de información mediante el uso de todo tipo de recursos de comunicación
    - Establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.
- La documentación del sistema deberá estar protegida contra accesos no autorizados.
- Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se debe incorporar comprobaciones de validación en las aplicaciones.
- Realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.
- Los documentos importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.
- Implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario del sistema y sus conclusiones finales.