DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION-SGSI BAJO LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA “EN LINEA FINANCIERA” DE LA CIUDAD DE CALI-COLOMBIA

JUAN CARLOS OIDOR GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO DE SEGURIDAD INFORMATICA
POPAYAN
2016

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION-SGSI BAJO LA NORMA ISO/IEC 27001PARA LA EMPRESA “EN LINEA FINANCIERA” DE LA CIUDAD DE CALI-COLOMBIA

JUAN CARLOS OIDOR GONZALEZ

Monografía de grado para optar el título de
Especialista en Seguridad Informática

Esp. Ing. Freddy Enrique Acosta
Asesor del proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO DE SEGURIDAD INFORMATICA
POPAYAN
2016

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Popayán, 23 de diciembre de 2016

DEDICATORIA

A mi madre y mi hermana, trabajadoras incansables, que me han acompañado siempre, gracias a su generosidad y amor he logrado mis metas.

Juan Carlos Oidor González.

AGRADECIMIENTOS

Juan Carlos expresa sus agradecimientos a:

Esp. Ing. Freddy Enrique Acosta, asesor del proyecto, gracias a su orientación y gran disponibilidad para resolver inquietudes a tiempo con respecto a la metodología y temas desarrollados en el proyecto.

Directivos y empleados de la empresa “En Línea Financiera” de la ciudad de Cali, su apoyo y colaboración fueron vitales para lograr los objetivos planteados en el proyecto.

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACTIVO: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos[1].

AMENAZA: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización[2].

ATAQUE: Acción de vulnerar la seguridad explotando algún tipo de bug o problema en el software o hardware del sistema[3].

AUDITORIA: Consiste en la capacidad de establecer que acciones o procesos se llevan a cabo en el sistema, como así también quien y cuando los realiza[4].

CONFIDENCIALIDAD: Que la información llegue solamente a las personas autorizadas[5].

CONTROL: O salvaguarda, procedimiento o mecanismo tecnológico que reduce el riesgo[6].

DATO: Unidad mínima que compone cualquier información[7].

DATACENTER: Es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información de componentes asociados, como telecomunicaciones y los sistemas de almacenamientos donde

[1] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012 p. 22.
[2] Ibid., p. 27.
[3] MIERES, Jorge. Fundamentos sobre Seguridad de la Información. Disponible en internet:< http://www.segu-info.com.ar/terceros/>. p. 5.
[4] Ibid., p. 4.
[5] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Op. cit., p. 9.
[6] Ibid., p. 103.
[7] MIERES. Op. cit., p. 5.

generalmente incluyen fuentes de alimentación redundante o de respaldo de un proyecto típico de data center que ofrece espacio para hardware en un ambiente controlado[8].

DISPONIBILIDAD: Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio[9].

HABEAS DATA: Es el derecho que tiene toda persona o institución a solicitar la información que sobre sí mismo se encuentre almacenada en cualquier base de datos y el derecho de ser actualizada o eliminada si así se requiere[10].

HARDWARE: Conjunto de elementos materiales o físicos que componen una computadora[11].

INCIDENTE: Evento con consecuencias en detrimento de la seguridad del sistema de información[12].

INFORMACIÓN: Conjunto de datos que al ser unidos tienen un significado especifico más allá de cada uno de estos[13].

IMPACTO: Costo asociado a un incidente, que puede o no ser medido en términos estrictamente financieros, pérdida de reputación, implicaciones legales, etc.[14].

INTEGRIDAD: Se garantiza la exactitud y confiabilidad de la información y los procesos que la administran, procesan y/o transmiten[15].

OFIMÁTICA: Es el conjunto de métodos, aplicaciones y herramientas informáticas que se usan en labores de oficina con el fin de perfeccionar, optimizar, mejorar el

[8] Disponible en Internet:< http://conceptodefinicion.de/data-center/>
[9] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Op. cit., p. 9.
[10] REMOLINA, Nestor. El habeas data en Colombia. Disponible en Internet:<https://habeasdatacolombia.uniandes.edu.co/ >
[11] MIERES. Op. cit., p. 5.
[12] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Op. cit., p. 101.
[13] MIERES. Op. cit., p. 5.
[14] Sistema de gestión de seguridad de la seguridad de la información, ISO 27001. Disponible en Internet: < http://www.ceeisec.com/nuevaweb/>
[15] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Op. cit., p. 9.

trabajo y operaciones relacionados. La palabra ofimática es un acrónimo compuesto de la siguiente manera ofi (oficina) y mática (informática)[16].

RIESGO: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización[17].

SOFTWARE: Conjunto de programas que pueden ser ejecutados por el hardware para realizar tares solicitadas por los usuarios[18].

VULNERABILIDAD: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte los activos[19].

[16] Disponible en Internet:< https://www.significados.com/ofimatica/>
[17] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Op. cit., p. 9.
[18] MIERES. Op. cit., p. 5.
[19] MIERES. Op. cit., p. 5.

RESUMEN

Un sistema de gestión de la seguridad de la información o SGSI es una herramienta muy importante en la defensa de una organización contra las violaciones de datos. La norma ISO 27001:2013 proporciona un marco para el desarrollo e implementación de un SGSI eficaz. La norma ayuda a reducir los riesgos a la seguridad de la información, facilita el cumplimiento de las leyes y requisitos de seguridad y permite a las organizaciones desarrollar una cultura de seguridad.

El presente proyecto apoyado por las directivas de la empresa En Línea Financiera de la ciudad de Cali, inicia con la evaluación actual de la empresa con respecto a la seguridad de sus datos, identificando los activos que son esenciales en el manejo de la información, realizando el análisis de riesgos correspondiente a estos activos, estas fases se enmarcan en la metodología MAGERIT. Por último teniendo como base la norma ISO 27001:2013 se presentan los controles y políticas que permitan a la empresa cumplir en alto grado la seguridad informática y de la información.

ABSTRACT

An information security management system or ISMS is a very important tool in the defense of an organization against data breaches. ISO 27001: 2013 provides a framework for the development and implementation of an effective ISMS. The standard helps reduce information security risks, facilitates compliance with security laws and requirements, and enables organizations to develop a security culture.

The present project, supported by the directives of the company En Línea Financiera of the city of Cali, begins with the current evaluation of the company with respect to the security of its data, identifying the assets that are essential in the management of the information, realizing The risk analysis for these assets, these phases are part of the MAGERIT methodology. Finally, based on the ISO 27001: 2013 standard, we present the controls and policies that allow the company to comply with a high degree of information and information security.

INTRODUCCIÓN

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos[20].

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo[21].

En concordancia con la necesidad de las empresas de asegurar su información además de sus dispositivos computacionales y de comunicación, de manera organizada, sistemática, documentada y conocida, que involucre todos los aspectos físicos, lógicos y humanos de la organización. ISO como organización internacional de estándares, ha definido el estándar ISO 27001 para la gestión de la seguridad de la información anunciando *: "El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías"* [22].

La empresa En Línea Financiera de la ciudad de Cali, busca asegurar sus activos de información mediante la adopción del estándar ISO 27001:2013, logrando con ello minimizar los riesgos a los que se encuentran expuestos sus sistemas informáticos y su información.

El desarrollo del proyecto tiene como primera fase la revisión de las condiciones actuales de la gestión de seguridad de la empresa en cuestión, esta fase brinda un inventario de los activos de información pertenecientes a la empresa, esto permite identificar los riesgos a los que se enfrentan dichos activos.

---

[20] Sistema de gestión de la seguridad de la información. Disponible en Internet:<http://www.iso27000.es/>.
[21] Ibid., p. 2.
[22] SUAREZ SIERRA, Lorena. SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI. Universidad Nacional Abierta y a Distancia. Bogotá, Colombia julio de 2013. p. 10.

Identificados los activos y sus riesgos, se realiza la evaluación de cada uno de estos para posteriormente establecer controles que permitan minimizar su impacto. Se realiza el análisis y gestión de riesgos utilizando la metodología MAGERIT que brinda un marco sistemático y bien definido para la evaluación del riesgo.

Por último se definen controles y políticas de seguridad acordes a lo establecido por el estándar ISO 27001:2013, la elaboración de una declaración de aplicabilidad permite claridad para la selección de los controles necesarios para la implementación del sistema de gestión de seguridad de la información.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Independientemente del carácter que adopte la información, se acopie o se disemine, debe estar protegida adecuadamente a fin de garantizar en todo momento la confidencialidad, integridad y disponibilidad de los datos[23].

Por ello, el principal objetivo en Seguridad de la Información es justamente ese, proteger de una manera adecuada la información, preservando una serie de parámetros fundamentales para que los activos (todo aquello que puede ser medido a través de un costo) puedan considerarse protegidos y seguros, reduciendo al máximo posible los daños ocasionados por alguna eventualidad que impida el normal funcionamiento de la organización, sea esta comercial o militar[24].

Este objetivo se logra a través de un conjunto de metodologías, prácticas y procedimientos que tienden a proteger la información de cualquier tipo y en cualquier momento y lugar[25].

Dos razones para la adopción de normas como la ISO 27001:2013 son la proliferación de las amenazas a la información y los requisitos legales que se refieren a la protección de la información. Las amenazas de seguridad de la información son globales y afectan indiscriminadamente tanto a individuos como organizaciones, los datos están expuestos a muchos riesgos, como los desastres naturales, los ataques externos e internos, la corrupción y el robo.

Actualmente la empresa En Línea Financiera de la ciudad de Cali carece de controles y/o políticas para la gestión de los activos de información, desconociendo los riesgos tanto internos como externos, a los que se encuentra expuesta, y debido a su rápido crecimiento y al aumento del volumen de información de clientes, requiere herramientas para la gestión de la seguridad informática y de la información.

[23] MIERES, Jorge. Fundamentos sobre Seguridad de la Información. Disponible en internet:< http://www.segu-info.com.ar/terceros/>. p. 3.
[24] Ibid., p. 3.
[25] Ibid., p. 3.

El presente proyecto está motivado por la necesidad que tiene la empresa mencionada de mejorar su gestión del riesgo y la gestión de la seguridad informática y de la información a través de un estándar reconocido internacionalmente, siendo una preocupación de sus directivas ofrecer a sus empleados y socios la seguridad de la continuidad en el negocio.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un sistema SGSI bajo la norma ISO 27001:2013 puede garantizar la seguridad de los sistemas informáticos y de la información de la empresa En Línea Financiera de la ciudad de Cali?

1.3 OBJETIVOS

1.3.1 Objetivo general

Diseñar un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013 para la empresa “En Línea Financiera” de la ciudad de Cali, que permita mitigar y disminuir los riesgos a los que se enfrentan sus activos de información.

1.3.2 Objetivos específicos

- Clasificar los activos informática de la empresa En Línea Financiera de la ciudad de Cali e identificar las amenazas y vulnerabilidades que impactan a estos activos y realizar el análisis de riesgos.

- Establecer controles de seguridad según la norma ISO 27001:2013, que permitan mitigar o eliminar los riesgos a los que están expuestas los sistemas informáticos y la información de la empresa.

- Plantear políticas de seguridad para la empresa En Línea Financiera de la ciudad de Cali, basadas en la norma ISO 27001:2013.

1.4 JUSTIFICACIÓN

Llevar de manera remota los procesos administrativos así como la comunicación entre sus empleados necesarios para su funcionamiento es otro de los beneficios que la tecnología de la Información y las comunicaciones brinda a las empresas. El mismo servicio en la web que las empresas de hoy presta a sus clientes, los ha afectado a ellos de alguna manera, por cuanto a través de los pagos en línea que han realizado para la compra de servicios, consultas, actualización de datos, entre otros son aprovechados también por los delincuentes para acceder a sus claves o contraseñas, a sus computadoras personales para copia y/o eliminación de su información entre otras. Lo anterior hace que de alguna forma, los clientes se nieguen a realizar transacciones a través de estos medios de comunicación masiva como internet perdiendo las organizaciones posibles clientes potenciales a nivel mundial. En este orden, las empresas deben garantizar a sus clientes una transacción protegida, así como las orientaciones pertinentes para evitar fraudes informáticos[26].

Los últimos años han surgido muchas leyes y regulaciones en torno a la seguridad de la información y los datos, esto conlleva una gran responsabilidad por parte de las empresas que almacenan, manipulan y transmiten datos a través de sistemas informáticos. Las entidades financieras están sujetas a estrictas regulaciones por parte de los estados, que exigen el uso de sistemas seguros en todas las etapas de los servicios que prestan, informar a clientes sobre el alcance y limitaciones de los sistemas que utilizan y las disposiciones legales que cumplen[27]. Las empresas que omiten estas responsabilidades están expuestas a líos jurídicos que pueden acarrear su desaparición o causar grandes perjuicios en litigios, sin contar la pérdida de credibilidad y prestigio antes sus clientes.

Es importante mostrar que no es solo un problema de tecnología, ni es exclusivo al departamento de sistemas, mantener la seguridad informática y de la información es una estrategia que compromete a toda la organización, de allí la importancia de poseer un SGSI que a partir de su diseño revele la condición actual de la empresa y promueva la adopción de políticas que mitiguen los riesgos a los que se enfrenta.

Diseñar un SGSI para la empresa En Línea Financiera de la ciudad de Cali, permitirá que la empresa esté mejor preparada ante amenazas actuales y futuras

[26] SUAREZ. Op. cit., p. 10.

[27] ACURIO DEL PINO, Santiago. Fraudes Informáticos: Fundamento de responsabilidad de las Instituciones del Sistema Financiero. Pontificia Universidad Católica del Ecuador. Quito, Ecuador agosto de 2011. p. 7.

sobre sus sistemas informáticos, que pueden afectar su normal funcionamiento, además que permite la adopción de buenas prácticas en el manejo de la información que ayudaran a mitigar los efectos adversos que se puedan presentar y aumentando la confianza de socios y clientes.

De igual forma la empresa podrá responder a las regulaciones y leyes que exigen garantizar la seguridad de la información de individuos almacenada y gestionada en sus sistemas informáticos, evitando líos jurídicos y/o enfrentándolos de manera adecuada.

1.5 ALCANCE Y LIMITACIONES

1.5.1 Alcance

La presente monografía se encuentra entre los proyectos de gestión de la seguridad y lo que pretende es diseñar el sistema de gestión de la seguridad para la empresa “En Línea Financiera” de la ciudad de Cali-Colombia bajo la norma ISO 27001:2013.

1.5.2 Limitaciones

Es conveniente resaltar que el desarrollo del presente proyecto no abarca temas como los que se definen a continuación:

- La implementación del SGSI diseñado.
- No se realizará la implementación de los controles recomendados.
- El proyecto no contempla el seguimiento y medición de la aplicación de las políticas y controles recomendados.
- No se elaboraran todos los documentos exigidos por la norma ISO 27001:2013.

1.6 DISEÑO METODOLÓGICO

1.6.1 Unidad de Análisis

Empresas colombianas que desarrollan y prestan servicios de manejo y gestión de cartera para comerciantes y personas no bancarizadas.

1.6.2 Población y Muestra

1.6.2.1 Población

Las empresas ubicadas en la ciudad de Cali, Colombia, cuyo objeto de negocio es el desarrollo y mantenimiento de plataforma software para el manejo y gestión de cartera para comerciantes y personas no bancarizadas.

1.6.2.2 Muestra

Empresa “En Línea Financiera” de la ciudad de Cali-Colombia.

1.6.3 Estudio metodológico

El presente proyecto es una investigación de tipo proyectiva.

Este tipo de investigación que consiste en la elaboración de una propuesta o de un modelo, para solucionar problemas o necesidades de tipo práctico, ya sea de un grupo social, institución, una área en particular del conocimiento, partiendo de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y las tendencias futuras[28].

Durante el desarrollo del proyecto se usarán diferentes técnicas para recolección de información:

- Investigación en fuentes bibliográficas: Información disponible en tesis de grado, textos y manuales impresos y recopilados de Internet referentes al

[28] CÓRDOBA, Martha Nelly. TIPOS DE INVESTIGACIÓN: Predictiva, proyectiva, interactiva, confirmatoria y evaluativa. p. 3.

tema de seguridad informática y de la información, norma ISO 27001 y SGSI.

- Visitas a la empresa: Se realizaron varias visitas a las instalaciones de la empresa para conocer de primera mano el estado de sus oficinas, equipos, documentación y controles de seguridad. Se llevaron a cabo reuniones con todo el personal que labora en la empresa y entrevistas personales con los encargados de los sistemas informáticos de la empresa.

Para cumplir el primer objetivo del proyecto identificación y valoración de los activos de la empresa En Línea Financiera de la ciudad de Cali, se realizaron las siguientes actividades:

- Entrevistas al personal encargado del área de tecnologías de la empresa.
- Visitas a las instalaciones de la empresa para conocer su infraestructura tecnológica.
- Reporte de inventario de los equipos de cómputo, red y demás que soporten las actividades de la empresa.

El segundo objetivo identificación y análisis de amenazas y vulnerabilidades que impactan a los activos de la empresa, tuvo las siguientes actividades.

- Evaluación de los controles y/o herramientas actuales utilizadas por la empresa para garantizar la seguridad de los sistemas informáticos y de la información.
- Encuesta a todo el personal sobre las tareas que realizan y ponderar sus conocimientos sobre seguridad.
- Uso de una metodología para el análisis y gestión de riesgos.

El último objetivo diseñar el SGSI bajo la norma ISO 27001 versión 2013 para la empresa En Línea Financiera de la ciudad de Cali, se realizarán las siguientes actividades.

- Cálculo de riesgos.

- Selección de controles para mitigar los riesgos según la norma ISO 27001 versión 2013.

- Declaración de políticas de seguridad.

2. MARCO DE REFERENCIA

2.1 MARCO TEORICO

2.1.1 Seguridad informática y de la información.

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales[29].

Se puede afirmar que la seguridad informática es aquella que permite lograr que todos los sistemas informáticos se encuentren seguros ante cualquier amenaza o riesgos, sin importar el agente humano o natural que pueda ponerlo en riesgo ya sea voluntaria o involuntariamente. Para ello es importante contar con un conjunto de herramientas, documentos, estándares y metodologías que permitan aplicar normas y técnicas apropiadas para garantizar la protección de la información[30].

Para muchas empresas modernas la información es el activo más importante, en algunas es la base de su negocio, por tal motivo para estas empresa es importante contar con las herramientas adecuadas para proteger los sistemas informáticos y la información, que abarque componentes tanto tecnológicos, humanos, físicos y demás.

La seguridad de la información consiste generalmente en garantizar la confidencialidad, la integridad y la disponibilidad, las cuales se pueden definir[31]:

- La disponibilidad se refiere al acceso seguro de los usuarios autorizados a la información cuando estos la requieran. La no disponibilidad de los recursos afecta la productividad de las empresas.

[29] GALDÁMEZ, Pablo. Seguridad informática. Disponible en Internet: <http://web.iti.upv.es/>
[30] SUAREZ. Op. cit., p. 11.
[31] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012. p. 9.
.

- La integridad es la protección de la información contra modificación o alteración no autorizada. El correcto de desempeño de una organización se ve afectado por información incorrecta o adulterada sin autorización.

- La confidencialidad es la protección de la información contra el uso por parte de personal no autorizado. Si esta característica se vulnera la organización se puede ver envuelta en líos jurídicos debido a la violación del secreto.

Otras dimensiones cuya vulneración que afectan los activos de información son[32]:

- Autenticidad es la garantía de que la información procede de la fuente que alega ser, esto implica una prueba de identidad para evitar su suplantación.

- Trazabilidad asegurar que se puede determinar que ente o individuo realizo determinada actividad en el sistema. Esta característica es muy importante para el análisis de incidentes, perseguir a la fuente y adquirir experiencia.

Cuando se presenta un indecente que afecta a una de las características antes mencionadas debió existir un riesgo que no fue detectado a tiempo o no se hizo su tratamiento correcto, con ello decimos que un riesgo es la amenaza que aún no se ha materializado e incidente cuando ésta se materializa[33].

Para reducir el impacto o daño producido por un incidente de seguridad se cuenta con un gran número de medidas, que se pueden agrupar en técnicas y de gestión, las primeras corresponden a herramientas hardware y software implantados para evitar daños y recuperar los sistemas afectados por un incidente, las medias de gestión se implementan como parte de planes estratégicos y tácticos que requieren la participación de todos los empleados de la empresa[34].

Las organizaciones deben gestionar de forma efectiva y competente la seguridad de sus activos, demostrar que identifican y gestionan los riesgos a los que están expuestas, para ello es necesario adoptar un conjunto de normas y herramientas

[32] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT. Libro I. Op. cit., p. 9.
[33] SUAREZ. Op. cit., p. 13.
[34] GALDÁMEZ, Pablo. Seguridad informática. Disponible en Internet: <http://web.iti.upv.es/>

que de una forma estructurada, coherente y sistemática garanticen la seguridad informática y de la información.

2.1.2 Amenazas[35]

Es cualquier acción con el potencial de causar un impacto negativo sobre un activo de la empresa. Las amenazas aumentan todos los días, cada vez son más sofisticadas y sus daños más catastróficos.

Los sistemas informáticos y la información se encuentran en constante riesgo debido a amenazas de toda índole, manos criminales, desastres naturales, incendios, mal uso de tecnologías, errores humanos, problemas y errores propios de dispositivos, de acuerdo a esto podemos clasificarlas en 3 grupos:

- Amenaza criminal: El actor viola las normas y leyes establecidas para destruir, sustraer o modificar información, dispositivos o cualquier otro medio que la contenga, manipule o transmita para beneficio propio, de terceros o simplemente para causar daño.

- Eventos de origen físico: En esta categoría están los desastres naturales y aquellas que son propiciados por condiciones establecidas por un humano.

- Negligencia: Aquellos eventos que se dan por desconocimiento o falta de diligencia en la manipulación de los sistemas tecnológicos y/o sistemas de información.

A continuación se enumeran algunas amenazas:

Ataques internos debido personal desleal o deshonesto, generando robo de secretos industriales, sabotaje, etc. Este tipo de amenazas se ve incrementado por el otorgamiento excesivo de permisos a usuarios, a la falta de procesos de auditoria y monitoreo sobre las actividades de los usuarios dentro de los sistemas de información, ausencia de controles de acceso a áreas de computo sensibles.

[35] BENAVIDES RUANO, Mirian del Carmen. SOLARTE SOLARTE, Francisco. Módulo riesgos y control informático. Universidad Nacional Abierta y a Distancia. Pasto, Colombia febrero de 2012. p. 18.

Ingeniería social, conjunto de técnicas usadas por los hackers para apoderarse de información, dispositivos u otros medios aprovechando la ingenuidad, exagerada confianza o desconocimiento de empleados o personal con acceso legitimo a los sistemas.

Uso imprudente de redes públicas, los usuarios las usan sin ningún reparo hacia su seguridad para ingresar a la red de la empresa o para transferir datos empresariales.

Robo o pérdida de dispositivos móviles. Los empleados son víctimas de robo o accidentalmente pierden memorias USB, celulares y portátiles que en muchas ocasiones almacenan datos sensibles de la organización o de ellos mismos que pueden ser usadas para que sean suplantados o para realizar ingeniería social.
Navegación a sitios de alto riesgo dentro de la empresa. Un usuario que navega por sitios no relacionados con el negocio termina invitando a la red corporativa software malicioso. Esta amenaza se ve incrementada por la falta o desactualización de software antivirus en los equipos usados por los usuarios.

Mala configuración de dispositivos hardware y/o software. Se utilizan configuraciones o claves de usuario por defecto, no se bloquean puertos o usuarios inutilizados. Estos datos son conocidos por todos y aprovechados por usuarios malintencionados.

Sustracción, modificación y eliminación de información no autorizados por ataques externos. Esta amenaza se incrementa por múltiples causas como cuentas de usuarios y contraseñas débiles, sistemas mal configurados, falta de herramientas para detección de intrusos, ausencia de controles de acceso físico a las instalaciones de la empresa, virus y software malicioso, los cuales pueden causar la indisponibilidad del sistema.

Desastres naturales, eventos como incendios, terremotos e inundaciones pueden afectar las instalaciones y dejar inoperante todo el sistema. La empresa debe poseer los medios necesarios para garantizar la seguridad en los lugares donde se encuentren los sistemas informáticos y las medidas necesarias para la rápida recuperación de sus sistemas ante este tipo de eventualidades.

Solo se considera una amenaza si existe una vulnerabilidad que pueda ser explotada por ésta, es decir, si hay una condición de debilidad que crea una

oportunidad para la explotación por parte de una o más amenazas. Si no hay vulnerabilidades, no hay amenazas.

Las vulnerabilidades técnicas son las más fáciles de identificar. Los creadores y proveedores de software y hardware suelen publicar boletines de errores y vulnerabilidades, junto con parches que solucionan los errores reportados en sus productos.

Las vulnerabilidades podrían surgir por deficiencias en la gestión de la seguridad, por ejemplo, el personal de la organización podría ser insuficiente para cubrir todas las responsabilidades de seguridad o podrían carecer de una capacitación adecuada. Otras vulnerabilidades podrían estar relacionadas con las operaciones de los sistemas, por ejemplo, viejos discos con datos se disponen en la basura que es accesible al público, sería fácil para cualquier persona recuperar datos descartados.

Una vulnerabilidad puede ser eliminada o mitigada usando controles, que se pueden definir como cualquier dispositivo o acción con la capacidad de reducir la vulnerabilidad. Son las medidas de protección que reducen el nivel de vulnerabilidad. Un control vale la pena sólo si su costo puede ser justificado por la reducción del nivel de riesgo. No todos los costos pueden ser fáciles de identificar, los costos de hardware y software son fáciles de estimar, pero otros como formación de personal, tiempo, recursos humanos adicionales, y la implementación política son difíciles de cuantificar.

2.1.3 Gestión de riesgos.

Los riesgos implican la probabilidad de pérdida total o parcial de los sistemas de información debidas a fallas del hardware o software, errores humanos, fraudes internos y externos, desastres naturales, etc. Igualmente involucran riesgos legales y riesgos en la credibilidad y confianza en la organización por fallas en la seguridad de los sistemas de información[36].

Es importante identificar los riesgos que afecten los sistemas de información, para reducir o gestionar estos riesgos, y desarrollar un plan que dé respuesta en caso de una crisis o incidente. La organización tiene obligaciones legales en relación a

[36] BENAVIDES. Op. cit., p. 13.

.

la privacidad, las transacciones y la capacitación del personal que participan en las estrategias de gestión de riesgos de los sistemas de información.

El análisis de riesgos brinda a la organización la información que necesita para tomar decisiones relativas a la seguridad de la información. El procedimiento identifica los controles existentes, calcula las vulnerabilidades, y evalúa el efecto de las amenazas en cada área.

Se realiza el análisis de las probables consecuencias o riesgos asociados con las vulnerabilidades y proporciona la base para establecer un programa de seguridad acorde a las necesidades y presupuesto de la organización.

En la mayoría de los casos, el procedimiento de análisis de riesgos intenta alcanzar un equilibrio económico entre el impacto de los riesgos y el costo de las soluciones de seguridad destinados para su gestión. En resumen un análisis de riesgos de seguridad define el entorno actual y recomienda acciones correctivas si el riesgo residual es inaceptable. El proceso de análisis de riesgos debe ser llevado a cabo con suficiente regularidad, para garantizar que el enfoque de cada gestión al riesgo es una respuesta realista a los riesgos actuales. La administración debe decidir si acepta el riesgo residual o aplica las medidas recomendadas.

Para la gestión de los riesgos la empresa debe hacer una evaluación de riesgos y desarrollar un plan de continuidad de negocio que pueda ayudarla a recuperarse ante un incidente, existen varias metodologías de análisis de riesgos desarrolladas por varias organizaciones que facilitan esta tarea, entre ellas tenemos[37]:

- Mehari: Es un método para el análisis y gestión de riesgos desarrollado por CLUSIF (Club de la Securit 'e de l'Información' Français), Francia.

- Magerit: Es una metodología de análisis y gestión de riesgos de los sistemas de información desarrollados por CSAE de España.

[37] BENAVIDES. Op. cit., p. 35.

- NIST800-30: Es una guía de gestión de riesgos para los sistemas de información recomendadas por el Instituto Nacional de Estándar y Tecnología (NIST) de Estados Unidos.

- Guía de Gestión de la Seguridad de Microsoft: Es la guía de la gestión de riesgos de seguridad desarrollado por Microsoft.

Para una gestión efectiva de riesgos se deben cumplir las siguientes fases:

2.1.4 Fases del análisis de riesgos.

En general sin importar la metodología, todas cumplen con 3 fases básicas[38]:

- Identificación de activos: Conjunto de todos los elementos que sostienen las actividades de la organización y que requieran ser protegidos debido a su importancia. Es necesario identificar la información que se requiere proteger, su valor, y los elementos del sistema, llámese hardware, software, redes, procesos y personas que soportan el almacenamiento, procesamiento y transmisión de información, en otras palabras, todo el entorno de tecnologías de la información debe caracterizarse en términos de bienes, equipos, flujo de información, y personal

- Evaluación de amenazas y vulnerabilidades: Proceso de identificación de las causas de la amenaza, los activos afectados y el cálculo de la probabilidad de que ocurra, detección de las vulnerabilidades o debilidades de los activos valorados. En esta fase la información detallada sobre el activo se utiliza para determinar la importancia de las vulnerabilidades. Esto incluye cómo es utilizado el activo, la sensibilidad de los datos, la criticidad de la misión, disponibilidad, etc. Por último, el impacto negativo o pérdida esperada para el activo, que se estima mediante el examen de varias combinaciones de amenazas y vulnerabilidades.

- Tratamiento del riesgo: Se analizan los costos para garantizar la seguridad versus costos de exposición a las amenazas, lo que se busca es tener un

[38] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT. Libro I. Op. cit., p. 22.

equilibrio coste beneficios, establecer controles que mitiguen el riesgo pero que a su vez sean viables y acordes a las necesidades de la empresa. La base de la selección de las medidas o controles de protección rentables es la suposición de que el costo de controlar cualquier riesgo no debe exceder la máxima pérdida asociada al riesgo. El objetivo final es llevar el riesgo a un nivel aceptable para la organización.

El nivel de riesgo que queda después de la consideración de los controles, los niveles de vulnerabilidad, y las amenazas relacionadas entre sí, se conoce como riesgo residual. Existen muchas formas para determinar el riesgo residual. Del mismo modo, la métrica para expresar el riesgo residual puede variar de bueno/malo o alta/baja, valores numéricos, etc. Una vez se ha determinado el riesgo residual el siguiente paso es identificar la manera más eficaz y menos costosa de reducir el riesgo a un nivel aceptable. Pero, al final, cualquier análisis de riesgos de seguridad debe indicar el nivel de riesgo actual, las probables consecuencias, y qué hacer al respecto si el riesgo residual es demasiado alto.

El proceso de reducción de ese riesgo es invertir estratégicamente los recursos limitados para cambiar riesgos inaceptables en otros más aceptables. La mitigación del riesgo puede ser una combinación de cambios técnicos y no técnicos. Los primeros implican equipos de seguridad, como por ejemplo, controles de acceso, criptografía, cortafuegos, sistemas de detección de intrusos, seguridad física, software antivirus, registros de auditoría, copias de seguridad, etc. Y la gestión de dichos equipos, cambios no técnicos, podrían incluir cambios de política, capacitación y toma de conciencia de los usuarios. Teniendo en cuenta el resultado del proceso de evaluación de riesgos, los riesgos pueden ser aceptados o mitigados. Para mitigar un riesgo se cuenta con 3 opciones:

- Eliminar la causa del riesgo, eliminando la vulnerabilidad o la posibilidad de la amenaza. Por ejemplo, las vulnerabilidades de software pueden remediarse mediante la aplicación de los parches de actualización. Los controles preventivos tratan de eliminar las vulnerabilidades y así evitar ataques con éxito.

- Limitación del riesgo reduciéndolo a un nivel aceptable, por ejemplo, mediante la implementación de controles para reducir el impacto o la frecuencia esperada. Un ejemplo puede ser el endurecimiento en los servidores de seguridad y controles de acceso para que sea más difícil para los atacantes externos acceder a la red privada de la organización.

- Transferencia del riesgo, cuando asignamos el riesgo a otra parte o tercero. El método más común es adquirir seguros, que permite a una organización convertir el riesgo de pérdida potencialmente catastrófica a una pérdida fija de mucho menos valor.

2.1.5 Metodologías para la gestión del riesgo.

Entre las más reconocidas tenemos.

- ISO 27005:

Forma parte de la familia de Normas ISO/IEC 27000, ofrece recomendaciones, métodos y técnicas para la gestión de riesgos con referencia a la seguridad informática, sirve de soporte para el diseño de un SGSI bajo la norma 27001 de la misma familia[39].

La norma ISO 27005 define el riesgo como una potencial amenaza que explotará las vulnerabilidades de un activo o grupo de activos y por lo tanto causará daño a la organización. Bajo esta norma el proceso de gestión de riesgos incluye muchos pasos superpuestos y no muy bien diferenciados:

- Contexto
- Evaluación de riesgos
- Tratamiento del riesgo
- Aceptación de riesgos
- La comunicación de riesgos
- Monitoreo y revisión de riesgos

Lo que no aparece en esta norma es la medición del riesgo. La alternativa es la estimación cuantitativa. La ISO 27005 indica que esto debe basarse en datos de incidentes históricos, esto dificultad el trabajar con la norma si no se tienen estos datos, además muchos expertos aseguran que la gestión de nuevos riesgos y debilidades debería ser el objetivo de la gestión de riesgos.

[39] SUAREZ. Op. cit., p. 28.

- MAGERIT:

Es una metodología desarrollada por el Ministerio de Administraciones Públicas de España, dirigido especialmente para la administración pública, debido su carácter abierto también se utiliza fuera de la administración pública. En ésta encontramos fases para la estimación e impacto de los riesgos que pueden afectar a los sistemas de información, también la estimación de los tiempos y recursos que el tratamiento de los riesgos conllevará. Las fases finales involucran la gestión de riesgos en sí, se seleccionan soluciones a los riesgos detectados y mecanismos o salvaguardas que implementen dichas soluciones[40].

La metodología busca alcanzar los siguientes objetivos:

- Hacer que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la necesidad de tratarlos a tiempo.
- Ofrecer un método sistemático para el análisis de estos riesgos.
- Ayudar en la descripción y la planificación de las medidas adecuadas para mantener los riesgos bajo control.
- Preparar a las organizaciones en los procesos de evaluación, auditoría, certificación o acreditación.

MAGERIT está estructurado en tres libros:

- Libro I: Metodología. Describe los pasos y tareas básicas para llevar a cabo un proyecto de análisis y gestión de riesgos, la descripción del proyecto, la aplicación para el desarrollo de sistemas de información, así como los fundamentos teóricos.
- Libro II: Catálogo. Proporciona elementos estándares y criterios para los sistemas de información y modelos de riesgo: las clases de activos, las

[40] BENAVIDES. Op. cit., p. 35.

dimensiones de valoración, criterios de valoración, amenazas típicas, y las garantías que deben considerarse, así mismo describe los informes que contienen los resultados y conclusiones.

- Libro III: Técnicas. Describe las técnicas utilizadas para realizar proyectos de análisis y gestión de riesgo tales como: tablas y análisis algorítmico, árboles de amenazas, análisis de costo-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo y análisis Delphi.

La aplicación de la metodología es compatible con el software PILAR/EAR, que explota y aumenta su efectividad. PILAR es de uso exclusivo para la Administración Pública Española. EAR es un producto comercial.

- OCTAVE:

Es un marco de seguridad desarrollado en 2001 por la Universidad Carnegie Mellon para el Departamento de Defensa de los Estados Unidos para determinar el nivel de riesgo y la planificación de las defensas contra ataques cibernéticos.

Define una metodología para ayudar a las organizaciones a minimizar la exposición a posibles amenazas, determinar las posibles consecuencias de un ataque y hacer frente a los ataques que se presenten. Entre sus objetivos principales están que la organización pueda gestionar sus evaluaciones de riesgos, tomar decisiones basándose en estos, salvaguardar los activos de información y comunicar de forma efectiva la información clave de seguridad. La metodología define tres fases:

- Fase 1: Construir de amenazas de activos basada en perfiles.
- Fase 2: Identificar vulnerabilidades en la infraestructura.
- Fase 3: Desarrollo de estrategias y planes de seguridad.

Ha pasado por varias fases evolutivas, existen dos versiones: OCTAVE-S, una metodología simplificada para organizaciones más pequeñas con estructuras jerárquicas planas, y OCTAVE Allegro, versión más completa para grandes organizaciones o con estructuras multinivel.

Se le considera una metodología compleja, y una de sus desventajas es el hecho de que no produce un análisis cuantitativo detallado de la exposición de la seguridad.

- NIST SP 800-30:

Es la metodología de evaluación de riesgos preferida por el gobierno de Estados Unidos, y es obligatorio para las agencias del gobierno de este país. Cuenta con un proceso detallado paso a paso desde las etapas iniciales de la preparación para una evaluación, su ejecución, comunicación de los resultados, y el mantenimiento de la evaluación. Es de libre acceso directamente desde la página web del NIST, pero la búsqueda de apoyo adecuado para ponerla en práctica fuera de los Estados Unidos puede ser difícil, y debe tenerse en cuenta el costo. Como era de esperar, al ser un estándar de Estados Unidos, gran parte de la documentación a menudo se detiene en cuestiones de reglamentación que pueden tener poca relevancia para usuarios fuera de Estados Unidos. La metodología puede ser utilizable por organizaciones de todos los tamaños, tanto públicas como privadas. Está diseñada para ser compatible con las normas ISO, y lo suficientemente flexible como para ser utilizado con otras metodologías de gestión de riesgos[41].

El proceso de evaluación de riesgos en SP 800-30 toma entradas de un paso preparatorio que establece el contexto, el alcance, los supuestos y las fuentes de información clave para el proceso, y luego utiliza las amenazas y vulnerabilidades identificadas para determinar la probabilidad, impacto y riesgo. El proceso siguiente requiere que los resultados se comuniquen y se mantenga la evaluación, incluyendo el seguimiento de la eficacia de los controles y verificar el cumplimiento.

Los siguientes pasos son claves para completar un programa integral de evaluación de riesgos como se indica en el NIST SP 800-30. Estos pasos deben ser personalizados para identificar más eficazmente los riesgos de una organización basada en sus propias necesidades. A pesar de que estos elementos se enumeran como pasos, no son prescriptivos en el orden en que deben llevarse a cabo. Algunos pasos se pueden realizar simultáneamente en lugar de secuencialmente.

[41] SOTELO BEDÓN, Marcos. Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Disponible en internet: < http://www.comtel.pe/>

Paso 1. Caracterización del Sistema: El primer paso en la evaluación de riesgos es definir el alcance. Usando técnicas de recopilación de información, se identifican los límites del sistema de TI, así como los recursos y la información que constituyen el sistema. Tener en cuenta las políticas, las leyes, la fuerza de trabajo a distancia y teletrabajadores, medios extraíbles, dispositivos informáticos portátiles y los medios de copia de seguridad.
Salida - Caracterización del sistema de TI evaluado, una buena imagen del entorno del sistema de TI, y la delineación de los límites del sistema.

Paso 2. Identificación de Amenazas: Para este paso, se identifican y documentan las amenazas potenciales, aquellas que pueden explotar con éxito una vulnerabilidad particular. Una amenaza de código es cualquier circunstancia o evento con el potencial de causar daño, intencional o no, a un sistema informático. Las fuentes comunes de amenazas pueden ser naturales, humanos o el medio ambiente. Se deben Considerar todas las posibles amenazas, revisar incidentes históricos y datos de los servicios de inteligencia, proveedores, el gobierno, etc.
Salida - Una declaración de amenazas que contiene una lista de fuentes de amenazas que podrían aprovechar las vulnerabilidades del sistema.

Paso 3. Identificación de vulnerabilidades: El objetivo es desarrollar una lista de las vulnerabilidades, técnicas y no técnicas, del sistema y que podrían ser explotadas por las amenazas. Las vulnerabilidades pueden variar desde políticas incompletas o contradictorias que rigen el uso de los computadores hasta la falta de suficientes garantías para proteger las instalaciones, u otras deficiencias que componen la infraestructura tecnológica de la organización.
Salida - Una lista de las vulnerabilidades del sistema que podrían ser explotadas por las posibles amenazas.

Paso 4. Análisis de Controles: La finalidad de este paso es documentar y evaluar la eficacia de los controles técnicos y no técnicos que han sido o serán implementados por la organización para minimizar o eliminar la probabilidad de explotación de una vulnerabilidad del sistema.
Salida - Lista de controles actuales o previstos, como políticas, procedimientos, capacitación, herramientas técnicas, seguros, etc., utilizados para mitigar la probabilidad de que una vulnerabilidad que sea explotada y reducir el impacto de un evento adverso.

Paso 5. Determinación de probabilidad: El objetivo es determinar la probabilidad de que una vulnerabilidad pueda ser explotada por una amenaza dados los

controles de seguridad existentes o previstos. Salida - Valoración del Riesgo bajo (0,1), media (0,5) o alta (1).

Paso 6. Análisis de Impacto: En este paso el objetivo es determinar el nivel de efecto adverso que resultaría de que una amenaza explote con éxito una vulnerabilidad. Los factores a considerar deben incluir la importancia de la misión de la organización, sensibilidad y criticidad, costos asociados, pérdida de confidencialidad, integridad y disponibilidad de los sistemas y datos. Salida - Magnitud del impacto baja calificación (10), media (50) o alto (100).

Paso 7. Determinación del Riesgo: Al multiplicar las calificaciones de probabilidad y análisis de impacto, se determina el nivel de riesgo. Esto representa el grado o nivel de riesgo al que un sistema informático, instalación o procedimiento podría estar expuesto si una vulnerabilidad dada fuera explotada. La calificación de riesgo también presenta las acciones que la alta dirección debe tomar para cada nivel de riesgo. Salida - Nivel de riesgo de baja (1-10), media (> 10-50) o alta (> 50-100).

Paso 8. Recomendación de controles: El propósito de este paso es identificar los controles que podrían reducir o eliminar los riesgos identificados. El objetivo de estos controles es reducir el nivel de riesgo para el sistema y los datos a un nivel aceptable. Los factores a considerar pueden incluir efectividad de las opciones recomendadas, la legislación y la regulación, políticas de la organización, el impacto operativo, la seguridad y la fiabilidad. Salida - Recomendación de controles y soluciones alternativas para mitigar el riesgo.

Paso 9. Documentación de resultados: Los resultados de la evaluación de riesgos se documentan en un informe oficial y siempre a la alta dirección para tomar decisiones en materia de políticas, procedimientos, el presupuesto y los cambios del sistema operativo y de gestión. Salida - Un informe de evaluación de riesgos que describe las amenazas y vulnerabilidades, mide el riesgo, y proporciona recomendaciones para la implementación de controles.

2.1.6 Sistema de Gestión de la Seguridad de la Información.

Un Sistema de Gestión de la Seguridad de la Información o SGSI, es una herramienta que le permite a las organizaciones tener procesos sistemáticos,

documentados y conocidos por todos para la correcta y efectiva gestión de la seguridad de la información[42].

Los medios técnicos ofrecen niveles de seguridad limitados e insuficientes. La gestión efectiva de la seguridad implica la participación de toda la organización, con la gerencia al frente, considerando igualmente a clientes y proveedores de bienes y servicios. El modelo debe contemplar procedimientos adecuados y la planificación e implantación de controles basados en una evaluación de riesgos y en la medición de la eficacia de los mismos[43].

Un SGSI proporciona seguridad permanente ya que es un proceso, y no acciones puntuales, gracias a esto las organizaciones deben definir una estrategia de seguridad basada en el negocio y no sólo en la tecnología, el enfoque debe ser integral. La confidencialidad, integridad y disponibilidad de la información crítica pueden llegar a ser muy importantes para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos[44].

Entre los beneficios de implantación de un SGSI se pueden enumerar[45]:

- Aspecto Humano: Concientización y definición de responsabilidades del personal ante la seguridad en la organización.
- Aspecto Financiero: Menores costos vinculados a incidentes de seguridad.
- Aspecto Organizacional: Demuestra que la organización está preparada para afrontar incidentes de seguridad.
- Aspecto Funcional: Gestión de los riesgos.
- Aspecto Legal: Cumplimiento con leyes y regulaciones.
- Aspecto Comercial: Refuerza la credibilidad y confianza de socios y clientes.

[42] Sistema de gestión de la seguridad de la información. Disponible en Internet:<http://www.iso27000.es/>
[43] Ibid. Sistema de gestión de la seguridad de la información.
[44] Ibid. Sistema de gestión de la seguridad de la información.
[45] Sistema de gestión de seguridad de la seguridad de la información, ISO 27001. Disponible en Internet: < http://www.ceeisec.com/nuevaweb/>

Estos beneficios deben sobrepasar los costos asociados al diseño e implementación del SGSI, que muchas veces es considerado como un obstáculo por las empresas para adoptar la norma. Uno de los interrogantes más frecuentes es el costo que tendrá el lograr asegurar los activos de información, para las directivas de la empresa surgen inquietudes con respecto a la efectividad y retorno de la inversión, es tarea de los encargados de la parte técnica hacer visibles los beneficios que trae el mantener está función[46].

La familia de normas ISO/IEC 27000 especifica los requisitos para diseñar, implementar, controlar, revisar y mantener un SGSI[47], que sigue un enfoque basado en procesos, lo que permite a la organización la flexibilidad de operar los procesos que son apropiadas a la misma. Estos pueden incluir los requisitos de seguridad de la información, establecer políticas apropiadas, la gestión de salvaguardas adecuadas, monitoreo y revisión del rendimiento y la eficacia del propio SGSI, y asegurar la mejora continua del sistema.

Estándares como la ISO 27001 y la ISO 9001 especifican intencionalmente sólo los requisitos de un sistema de gestión. La ISO/IEC 27001 especifica los requisitos necesarios para implantar un SGSI, su gestión, responsabilidad de los involucrados, conforme a las normas 27000[48]. Sus puntos más relevantes son la gestión de riesgos y la mejora continua, basando su diseño y ejecución en el modelo PHVA (planear, hacer, verificar y actuar) también conocido como ciclo de Deming.

La ISO 27001 no es una norma técnica que describe el SGSI con detalles técnicos, es muy general, está diseñada para ser aplicable a organizaciones dispares, no se centra solo en la tecnología de información, sino también en otros activos comerciales importantes, recursos y procesos de la organización. La norma posee un enfoque integrado de la seguridad de la información que requiere la evaluación de riesgos en todo los activos de la organización, incluyendo hardware, software, documentación, personas, proveedores, socios, etc., y la selección de los controles aplicables para disminuir esos riesgos.

La ISO 27001 proporciona la metodología para la implementación de la gestión de seguridad de la información en una organización, siguiendo una serie de fases que corresponden a la implementación del SGSI.

---

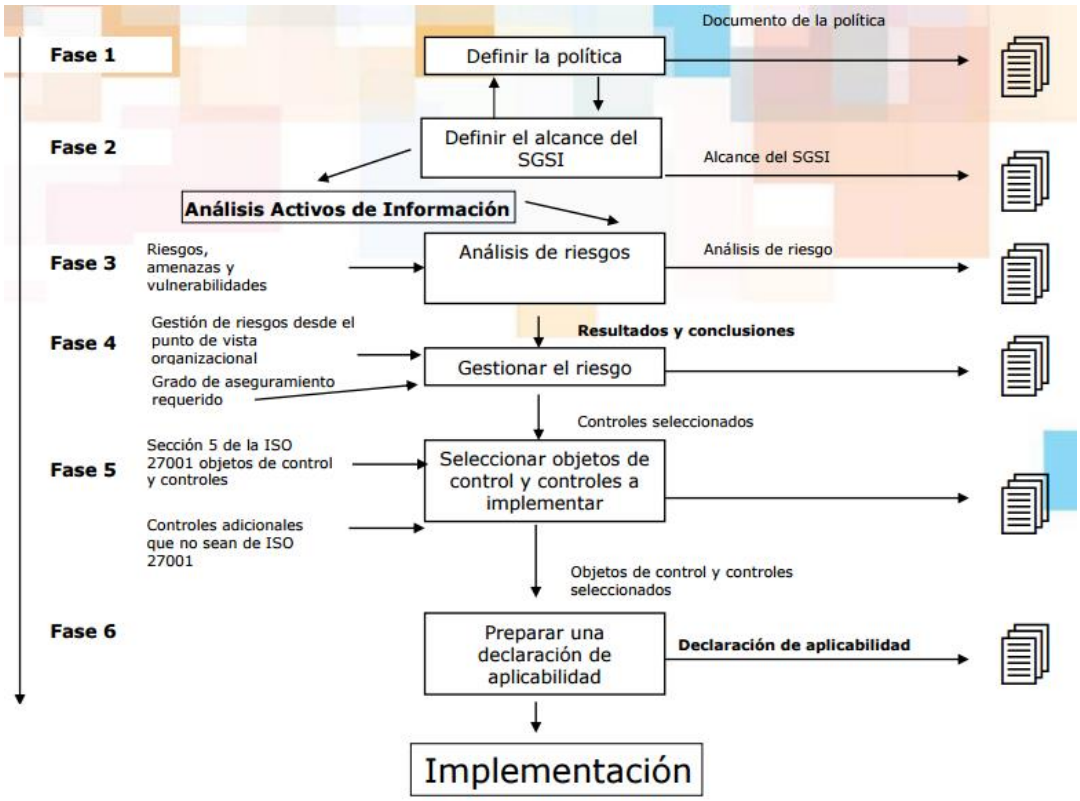
[46] CANO MARTINEZ, Jeimy. Apuntes sobre la Inversión y Gestión de la Seguridad Informática. Universidad de los Andes. Bogotá, Colombia julio de 2004. p. 1.

[47] SUAREZ. Op. cit., p. 30.

[48] SUAREZ. Op. cit., p. 29.

La figura 1 muestra los procesos a realizar en cada fase necesaria para la implementación del SGSI según la ISO 27001.

Figura 1. Metodología de un SGSI según ISO 27001



Fuente: http://www.mondragon.edu/

La norma garantiza que se haga una evaluación del riesgo y que ésta se utilice para seleccionar los controles correctos. El anexo A de la norma ISO 27001:2013, es básicamente un catálogo de controles de seguridad, 114 en total, no todos están relacionados con las tecnologías, lo que reafirma que su adopción no debe ser vista como un proyecto solo tecnológico, si no como un proyecto de toda la empresa, donde las personas relevantes de todos las unidades de negocio deben participar: directivos, personal de tecnologías, expertos legales, gestores de recursos humanos, personal de seguridad física, la parte comercial de la empresa, etc.[49].

[49] Sistema de gestión de la seguridad de la información. Disponible en Internet:<http://www.iso27000.es/>

A continuación se listan los controles del anexo A en cada una de las 14 secciones que éste posee[50].

A.5 Políticas de seguridad, relacionados con la definición y revisión de las políticas.

A.6 Organización de la seguridad de la información, los aplicados a definición de responsabilidades, contacto con autoridades, teletrabajo y dispositivos móviles.

A.7 Seguridad en los recursos humanos, definen los requisitos para la contratación de nuevos empleados, su permanencia y luego de su retiro.

A.8 Gestión de activos, inventario de activos, uso aceptable de los mismos, clasificación de la información y manejo de medios extraíbles.

A.9 Control de acceso, relacionados con el acceso y responsabilidades de los usuarios, control de acceso a aplicaciones y sistemas.

A.10 Criptografía, cifrado de información y administración de claves.

A.11 Seguridad física y del entorno, definición de áreas seguras, salvaguardas contra amenazas, seguridad de equipos, políticas de pantalla limpia, entre otros.

A.12 Seguridad en las operaciones, controles relacionados con la gestión de la infraestructura tecnológica, copias de seguridad, supervisión, etc.

A.13 Seguridad en las comunicaciones, relacionados con seguridad de redes, transferencia de información, mensajería, etc.

A.14 Adquisición, desarrollo y mantenimiento de sistemas, definen requisitos de seguridad en los procesos de desarrollo, mantenimiento y soporte de sistemas.

A.15 Relaciones con proveedores, cómo definir y supervisar los acuerdos con proveedores.

A.16 Gestión de incidentes de seguridad de la información, controles para informar sobre eventos, asignación de responsabilidades, recopilación de evidencias y procedimientos de respuesta.

A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio, controles garanticen la continuidad del negocio y la recuperación ante incidentes.

[50] Ibid. Sistema de gestión de la seguridad de la información.

A.18 Cumplimiento, controles para el cumplimiento de requisitos legales, contractuales y normatividad aplicables.

No todos los controles son obligatorios, cada empresa es libre de seleccionar los que más se ajusten a sus objetivos, igualmente el anexo A no da detalles sobre la implementación de los controles seleccionados por la organización.

Una declaración de aplicabilidad documenta los controles aplicables y es un documento flexible que dependiendo de las vulnerabilidades y amenazas identificadas, va a cambiar para afrontar los retos presentados por nuevos riesgos.

Junto a la norma ISO 27001 existen otras de la misma familia que ayudan a la implementación del SGSI. A continuación se enumeran otras normas de la familia ISO/IEC 27000:

- ISO/IEC 27002: Definición de buenas prácticas para la gestión de la seguridad. Proporciona recomendaciones sobre qué medidas se deben tomar para asegurar los sistemas de información.

- ISO/IEC 27003: Guía de implementación de SGSI e información sobre el uso del modelo PHVA.

- ISO/IEC 27004: Establece las métricas aplicables para determinar la eficacia de un SGSI.

- ISO/IEC 27005: Brinda recomendaciones, métodos y técnicas para evaluación de riesgos de la seguridad de la información.

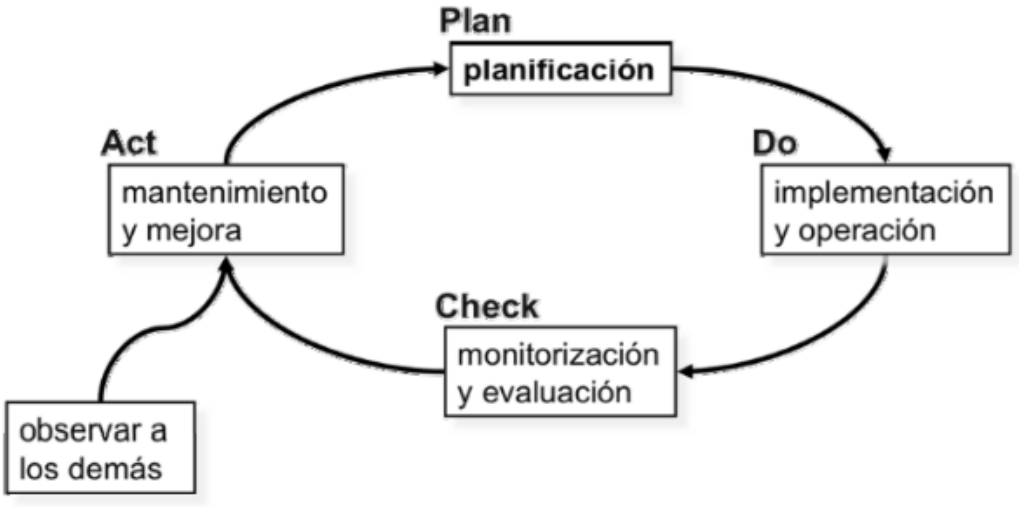
- ISO/IEC 27007: Guía sobre la auditoria de los SGSI conforme a las normas 27000.

2.1.7 Ciclo de Deming[51]

También conocido como el modelo *PHVA* (Planear, Hacer, Verificar, Actuar) o ciclo PDCA por sus siglas en inglés, que traduce Plan, Do, Check y Act. Se refiere a un método de gestión de cuatro fases que predica la mejora continua. Utilizado junto a la norma ISO 27001 consiste en la revaluación constante de los controles y políticas adoptados para garantizar la seguridad de los sistemas informáticos y la información.

El concepto detrás de la mejora continua en la norma ISO 27001 es asegurar la sostenibilidad de la seguridad de información a través del tiempo, realizando actividades estratégicas como auditorías y revisiones periódicas. El ciclo es un primer bucle de actividades que requieren una mejora dinámica a través del tiempo, de igual forma la seguridad informática es dinámica, la organización debe mantener el ritmo de sus cambios. La siguiente figura presenta las fases que se siguen en el ciclo PHVA.

Figura 2. Fases del ciclo de Deming



Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método

Planear: Es la fase en la cual se define el problema a resolver, se recolectan datos y se reconocen las causas del problema. Este paso es donde comienza el ciclo de

[51] SUAREZ. Op. cit., p. 25.

vida de la ISO 27001. El foco principal en esta etapa es establecer el marco ISO 27001 para la organización, en esta fase se realizan las siguientes tareas:

- Establecer el compromiso de los directivos de la empresa para llevar a cabo el proyecto.
- Identificar y evaluar los sistemas informáticos que posee la empresa.
- Planear los objetivos, actividades, procesos y procedimientos relativos a la gestión del riesgo.
- Para la norma ISO 27001 esta fase termina con la declaración de aplicabilidad.

Hacer: En esta fase se desarrolla e implementa una solución, y se seleccionan medidas para evaluar su eficacia. En ésta se da la transición entre el diseño y las actividades del mundo real.

- Implementar y gestionar el SGSI de acuerdo a los objetivos proyectados y trazados en la planeación.
- Definición de acciones preventivas y correctivas.

Verificar: Fase que se enfoca en evaluar los resultados de la solución adoptada. Mantener el rendimiento óptimo es imprescindible para asegurar el éxito de cualquier proceso.

La implementación y el funcionamiento de la norma ISO 27001 deben evaluarse para detectar debilidades que puedan corregirse, hacer más eficiente las actividades, capturar nuevas vulnerabilidades y amenazas. La evaluación de desempeño por lo general se lleva a cabo en forma de auditorías, las cuales tienen como objetivo principal asegurar que el SGSI se adhiera a la norma ISO 27001 de forma correcta, si existen diferencias entre las prácticas actuales en comparación con el estándar, deben realizarse las correcciones respectivas.

- Realizar mediciones y revisiones constantes de las prestaciones de los procesos del SGSI con el objeto de analizar los resultados que se van dando.
- Auditar el SGSI.

Actuar: Documentar los resultados, informar sobre cambios en el proceso, y hacer recomendaciones para los problemas que se abordarán en el próximo ciclo. Este paso es la mejora del ciclo, los resultados de la auditoría son las referencias fundamentales para realizar las actividades de mejora.

- Por medio de acciones preventivas y correctivas apoyadas en auditorías y revisiones alcanzar la mejora continua del SGSI, a través de los resultados obtenidos, se sugieren y proponen acciones para dar inicio nuevamente a las fases PHVA.

2.2 MARCO CONCEPTUAL

Seguridad de la información: La información es un activo que tiene valor para la organización y tiene que ser protegido adecuadamente. La información puede tener varias formas y puede ser almacenada en diferentes medios.

Por otro lado, seguridad de la información puede ser definida como la protección de la confidencialidad, integridad y disponibilidad de la información en todas las formas en las que se encuentre, tales como impresos, electrónicos, etc.

La seguridad de los recursos tecnológicos es sólo la mitad de la seguridad de la información, debido a que ésta última también incluye seguridad física, gestión de recursos humanos, la protección legal, organización, procesos, etc. El propósito de la seguridad de la información es construir un sistema que tenga en cuenta todos los posibles riesgos para la seguridad de la información, tanto tecnológicos como los relacionados a estos, e implementa controles que reducen todo tipo de riesgos inaceptables.

Norma ISO 27001: Es una norma internacional publicada por la Organización Internacional de Normalización (ISO), y describe cómo administrar la seguridad de información en una empresa. La última revisión de esta norma se publicó en 2013, y se conoce como la norma ISO/IEC 27001:2013. La primera revisión de la norma se publicó en 2005, y fue desarrollado teniendo como base a la norma británica BS7799.

La norma ISO 27001 tiene como objetivo la protección de la confidencialidad, integridad y disponibilidad, pero va un paso más allá, explica cómo hacerlo de forma sistemática en empresas de cualquier tipo, a través de un enfoque equilibrado para la construcción de un Sistema de Gestión de la Seguridad de la Información (SGSI), permitiendo un equilibrio entre la gestión de las tecnologías de la información y la gestión administrativa de la empresa, ya que requiere la participación directa de la alta dirección en la implementación de la seguridad de la información, asegurando que la implementación del SGSI sea compatible con los objetivos estratégicos de la empresa[52]. El SGSI juega un papel crítico para proteger la organización y cumplir su misión comercial, no sólo sus activos tecnológicos.

ISO 27001 no sólo explica cómo estructurar la seguridad de la información, sino también cómo aplicar los controles de seguridad que son realmente necesarios para la empresa. Brinda las herramientas para revisar de forma permanente todo el sistema y mejorarlo siempre que sea posible, provee un sistema para entrenar a los empleados y que sean conscientes de la importancia de la seguridad de la información. Proporciona un marco de gestión sobre cómo evaluar si la seguridad de la información ha alcanzado los objetivos y medir si estos objetivos se cumplen.

Gestión de riesgos: Los riesgos se refieren a eventos no deseados que pueden tener un impacto negativo en la seguridad de la información, y por lo tanto, a la empresa[53]. Podemos decir que la evaluación de riesgos es una visión sistemática de lo que puede salir mal, y el tratamiento de los riesgos consiste en seleccionar qué medidas de seguridad se ponen en práctica para evitar que aquellos eventos sucedan.

La gestión de riesgos es la idea central de la norma ISO 27001, ésta básicamente describe cómo desarrollar un SGSI que su vez representa un conjunto de políticas, procedimientos, y otros mecanismos de control que establecen las reglas de seguridad de la información en una organización. La decisión de cuales controles se requerirán está basada en los resultados de la evaluación del riesgo y

[52] ISO 27001.El portal de ISO 27001 en Español. Disponible en Internet: <http://www.iso27000.es/iso27000.html>

[53] BENAVIDES. Op. cit., p. 13.

de los requisitos de la empresa. Para cada riesgo a ser tratado, se necesitará una combinación de diferentes tipos de controles.

La gestión del riesgo y la evaluación del riesgo son componentes importantes del Sistema de Gestión de la Seguridad de la Información. La gestión del riesgo incluye identificar los riesgos, su evaluación y la toma de medidas para reducirlos a niveles aceptables para la organización. Este proceso de gestión de riesgos incluye algunas fases[54]:

1. La evaluación de riesgos requiere tres pasos: identificación, análisis y evaluación. Cada organización está continuamente expuesta a un sinnúmero de amenazas y vulnerabilidades que puedan afectar su funcionamiento o el cumplimiento de sus objetivos. La identificación, el análisis y la evaluación de estas amenazas y vulnerabilidades son la única forma de comprender y medir el impacto del riesgo involucrado y, por lo tanto, decidir sobre las medidas y controles para su manejo.

2. El tratamiento de riesgos es el proceso de selección e implementación de medidas para modificar el riesgo y mitigar su impacto. Las medidas de tratamiento pueden incluir evitar, optimizar, transferir o retener el riesgo.

3. Monitoreo y revisión es un proceso para medir la eficiencia y efectividad de las medidas adoptadas para la gestión del riesgo. Este proceso asegura que los planes de acción se actualicen a las nuevas amenazas y vulnerabilidades.

4. Comunicación y concientización, procesos necesarios para compartir información sobre los riesgos entre las partes interesadas dentro y fuera de la organización.

[54] BENAVIDES. Op. cit., p. 24.

2.3 ANTECEDENTES

El proyecto “análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información” presentado por Hina Luz Garavito Robles en la Universidad Nacional Abierta y a Distancia en la ciudad de Bogotá (Colombia). Su desarrollo aporta conocimientos importantes en la gestión de riesgos que sirven de punto de referencia para el proyecto planteado en el presente documento.

El proyecto “diseño de un sistema de gestión de la seguridad informática– sgsi–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría” presentado por Alexánder Guzmán García y Carlos Alberto Taborda Bedoya en la Universidad Nacional Abierta y a Distancia en la ciudad de Bogotá (Colombia). Aporta elementos claves para el diseño del SGSI en empresas privadas.

2.4 MARCO LEGAL

Las leyes sobre las tecnologías de información deben proporcionar el marco legal para la recopilación, almacenamiento y difusión de la información electrónica. Éstas se definen principalmente por su práctica en lugar de su tema legal y tienen que ver con el cumplimiento de los sistemas con los requisitos legales, la gestión de los riesgos legales que se deriven de los sistemas informáticos, los contratos y acuerdos relativos a los sistemas y la resolución de los litigios relativos a los sistemas.

Los estados están al tanto de crear nuevas leyes para garantizar a sus ciudadanos su privacidad y el derecho a que sus datos estén protegidos y sean usados con fines idóneos.

La legislación Colombiana ampara la seguridad informática y de la información a través de varias leyes. Es necesario tener en cuenta el marco jurídico que se debe cumplir durante cada una de las fases del análisis, diseño e implementación del SGSI, ya que la omisión de alguna ley o norma jurídica puede tener graves consecuencias para el proyecto o incluso la organización.

2.4.1 Decreto 1360 de 1989[55]

"Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

2.4.2 Ley 527 de 1999[56]

“Por medio de la cual 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 y se dictan otras disposiciones”.

2.4.3 Ley 599 de 2000[57]

“Por la cual se expide el Código Penal”.

2.4.4 Decreto 1747 de 2000[58]

“Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales”.

2.4.5 Ley 1121 de 2006[59]

“Por la cual se dictan normas para la prevención, detección, investigación y sanción de la financiación del terrorismo y otras disposiciones”.

2.4.6 Ley 1266 de 2008[60]

“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

[55] COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1360. Bogotá. (Junio 23 de 1989). Diario Oficial 38.871 de junio 23 de 1989.
[56] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527. Bogotá. (Agosto 18 de 1999). Diario Oficial 43.673 de agosto 21 de 1999.
[57] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599. Bogotá. (Julio 24 de 2000). Diario Oficial 44.097 de julio 24 de 2000.
[58] COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1747. Bogotá. (Septiembre 11 de 2000). Diario Oficial 44.160 de septiembre 14 de 2000.
[59] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1121. Bogotá. (Diciembre 29 de 2006). Diario Oficial 46.497 de diciembre 30 de 2006.
[60] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008.

financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

2.4.7 Ley 1273 de 2009[61]

"La cual modifica el Código Penal, creando un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-, cuyo objetivo principal es preservar los sistemas que utilicen las tecnologías de la información y las comunicaciones".

2.4.8 Ley 1340 de 2009[62]

"Por medio de la cual se dictan normas en materia de protección de la competencia".

2.4.9 Ley 1581 de 2012[63]

"Ley apoyada en el artículo 15 de la Constitución Política que reza sobre los derechos, libertades y garantías que posee toda persona, y que debe preservar el derecho que tienen todos a conocer, actualizar y rectificar las informaciones que de ellos se hayan almacenado en bases de datos o archivos, así como el derecho a la información según el artículo 20 de la Constitución Política".

[61] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (5 de enero de 2009). Diario Oficial 47.223 de enero 5 de 2009.
[62] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1340. Bogotá. (24 de julio de 2009). Diario Oficial 47.420 de julio 24 de 2009.
[63] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (17 de octubre de 2012). Diario Oficial 48.587 de octubre 18 de 2012.

3. MARCO CONTEXTUAL

3.1 DESCRIPCION DE LA EMPRESA

La empresa En Línea Financiera tiene como actividad comercial facilitar y sistematizar el proceso de crédito y administración de cartera de las diferentes entidades de actividad comercial, mediante el sistema de inclusión para no bancarizados a través de plataformas tecnológicas de fácil acceso y uso, reduciendo costos de operación para los comerciantes adscritos.

3.1.1 Historia

En 2012 nace nuestra empresa con el objetivo de implementar el sistema de inclusión para no bancarizados en el sector servicios y del comercio, como medio para el manejo adecuado y eficiente de la gestión de crédito y cartera, optimizando la operación, controlando el riesgo y generando liquidez al comercio.

3.1.2 Misión

Implementar el sistema de inclusión para no bancarizados en el sector servicios y del comercio, como medio para la gestión de crédito y cartera, optimizando la operación, controlando el riesgo y generando liquidez al comercio.

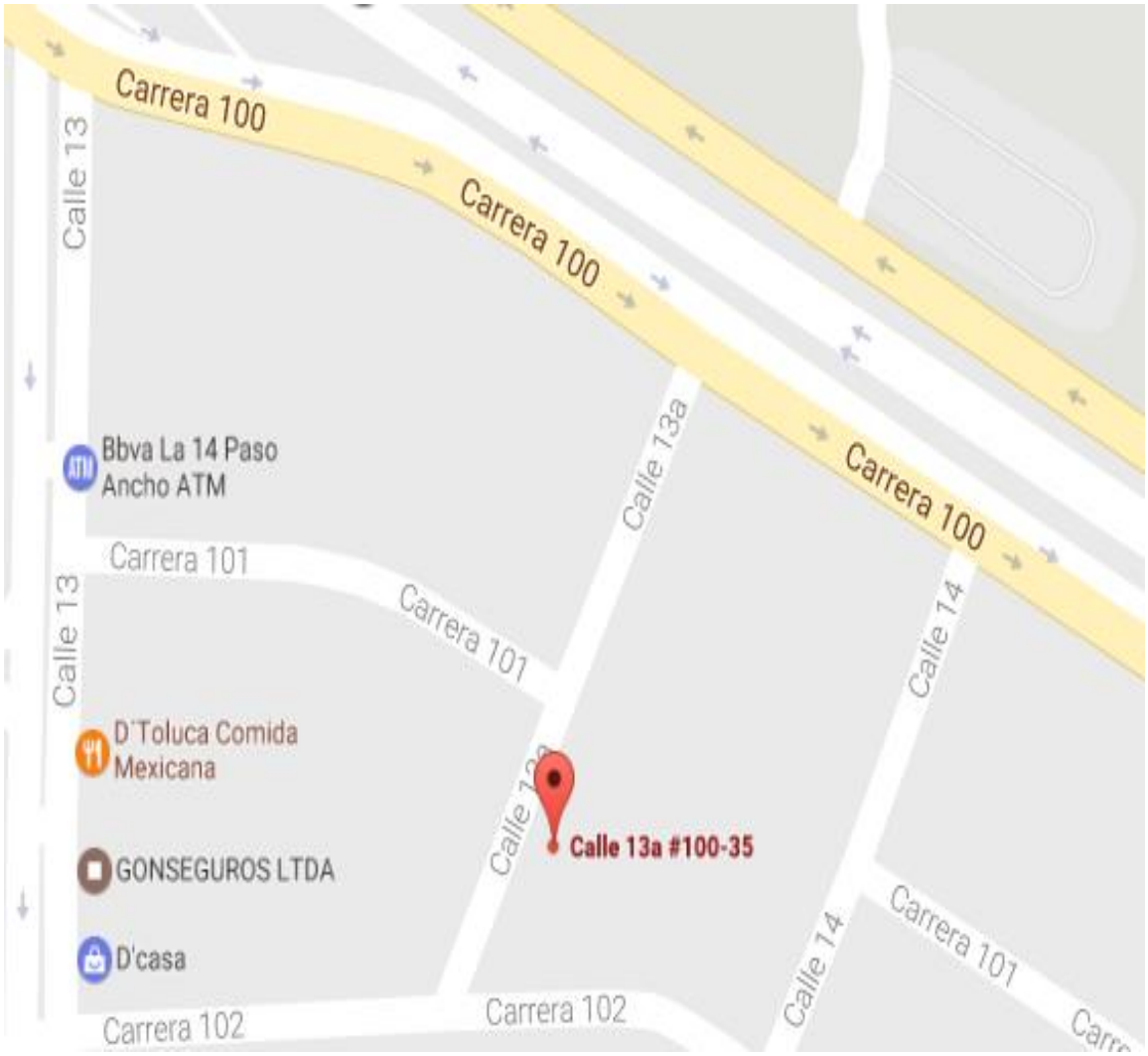
3.1.3 Visión

En el 2020 tener presencia nacional y convertir nuestra aplicación software en el sistema preferido por las empresas para la administración de la información de créditos y manejo de cartera.

3.1.4 Ubicación geográfica

Las oficinas de la empresa se encuentran en la calle 13A # 100-35 oficina 715 edificio Torre Empresarial, Cali, Valle del Cauca, Colombia.

Figura 3. Mapa ubicación de la empresa

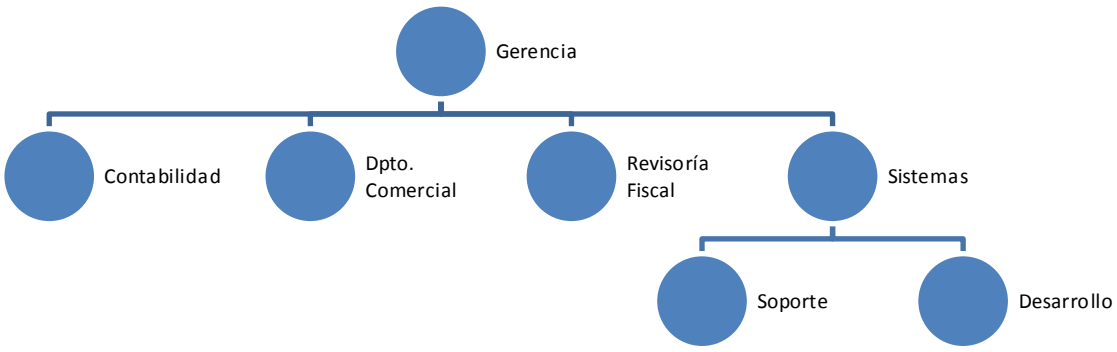


Fuente: Propiedad del autor.

3.2 ESTRUCTURA ORGANIZACIONAL

La empresa posee un organigrama muy plano con una estructura muy sencilla la cual se presenta en la siguiente figura.

Figura 4. Organigrama de la empresa



Fuente: Propiedad del autor.

3.3 AREA DE SISTEMAS

3.3.1 Caracterización del área de sistemas

El área de sistemas cumple funciones de apoyo a las otras áreas de la organización y además se encarga del desarrollo que soporta el negocio de la empresa.

Con respecto al apoyo que presta a otras áreas, éste se centra especialmente en instalación y configuración de aplicaciones de ofimática y colaborar a los demás empleados en dudas básicas con respecto al manejo de estas aplicaciones. La empresa contrata con terceros tareas como mantenimiento y actualización de equipos de cómputo, servidores y redes.

El equipo de desarrollo es de suma importancia en el área de sistemas y es donde se concentra la actividad más importante del negocio, el desarrollo de la aplicación. Existen planes para la ampliación de esta área y poder cubrir mejor los tiempos de entrega y pruebas de la aplicación.

3.3.1.1 Misión

El área de sistemas tiene por misión desarrollar y mantener la aplicación base del negocio de la empresa, mediante la administración eficiente y eficaz de la infraestructura y servicios informáticos de la empresa.

3.3.1.2 Objetivos

- Desarrollar y mantener el software de gestión de cartera de clientes, garantizando alta disponibilidad, seguridad y confiabilidad.
- Brindar soporte a los clientes sobre el uso de la aplicación de gestión de cartera.
- Gestionar soporte técnico para los usuarios internos que permitan mantener la funcionalidad de su equipo y servicios informáticos.

3.3.1.3 Estructura organizacional del área de sistemas

El área de sistemas posee una estructura plana, cuenta con 1 líder de desarrollo y DBA quien cumple las funciones de líder del área, 3 personas de soporte, 2 desarrolladores Java y 2 personas para pruebas. Se pueden distinguir las siguientes subdivisiones de acuerdo a las funciones realizadas dentro del área:

- Soporte: prestan ayuda y dan soluciones a inquietudes de los diferentes usuarios de la aplicación. Al interior hay una persona encargada de dar soporte a los equipos y red privada de la organización.
- Desarrolladores: mantienen la aplicación y agregan nuevas funcionalidades a la misma.

- Líder de desarrollo y DBA: encargado de liderar el desarrollo de la aplicación y de crear y mantener los objetos en la base de datos.

- Pruebas: técnicos dedicados a probar las nuevas funcionalidades de la aplicación y reportar hallazgos al líder de desarrollo.

3.3.1.4 Descripción de cargos y funciones

- Soporte: Técnicos en sistemas que prestan ayuda y dan soluciones a inquietudes de los diferentes usuarios de la aplicación. Al interior hay una persona encargada de dar soporte a los equipos y red privada de la empresa en cuestiones básicas y de fácil resolución. Son personas que tiene acceso básico a la información de la aplicación desarrollada en la empresa.

- Desarrolladores: Ingenieros de sistemas que mantienen la aplicación y agregan nuevas funcionalidades a la misma. Sus habilidades están enfocadas al desarrollo de aplicaciones web. No tienen acceso a los datos reales de la aplicación, tienen datos de pruebas con los cuales realizan sus tareas, aunque conocen como funciona la aplicación, por ello su confidencialidad es muy importante.

- Líder de desarrollo y DBA: Ingeniero de sistema encargado de liderar el desarrollo de la aplicación y de crear y mantener los objetos en la base de datos. Es el perfil técnico más alto dentro de la empresa. Sus responsabilidades abarcan desde el cumplimiento en tiempos de entrega de la aplicación, mejoras continuas, hasta el acceso a los datos reales de la aplicación, dado esto alguien que cuenta con la mayor confianza de toda la empresa.

- Pruebas: Técnicos en sistemas dedicados a probar las nuevas funcionalidades de la aplicación y reportar hallazgos al líder de desarrollo. Tienen acceso a datos de pruebas, pero sobre ellos recae la responsabilidad de probar nuevas funcionalidades de la aplicación y garantizar que no haya fallas o si existen sean mínimas.

3.3.1.5 Infraestructura tecnológica

En la actualidad la empresa tiene los siguientes activos de información e infraestructura tecnológica que son atendidos por el área de sistemas:

Equipos de intercambio de datos:

- Redes de comunicación e Internet.
- Un router principal que pertenece al ISP.

Sistemas de seguridad, prevención y control de acceso:

- La empresa se encuentra ubicada en un edificio que cuenta con vigilancia privada las 24 horas y cámaras de seguridad.
- Sistemas de aire acondicionado.
- Un extintor.

Equipos de cómputo:

- Hay 6 equipos portátiles dedicados a las labores administrativas, como contabilidad, gerencia, área comercial.
- El área de sistemas cuenta con 7 Portátiles y 3 de escritorio.
- El servidor donde se aloja la aplicación que soporta el negocio de la empresa se encuentra en un Data Center externo.

Software:

- Aplicaciones de ofimática.
- Software SINBA para la gestión de cartera de sus clientes.
- Aplicación Help Desk para registrar las solicitudes de usuarios y de cambios y actualizaciones a la aplicación SINBA.

3.4 SISTEMAS DE INFORMACIÒN

La empresa usa el sistema MANAGER ERP de la empresa Quality Colombia para su gestión administrativa.

El otro sistema de información es la aplicación para la gestión de cartera de sus clientes desarrollada por la misma empresa en Java y base de datos Oracle.

3.5 SERVICIOS QUE PRESTAN

Desarrollo y mantenimiento de la aplicación SINBA para la gestión de cartera de los comerciantes adscritos.

3.6 PROCEDIMIENTOS ACTUALES

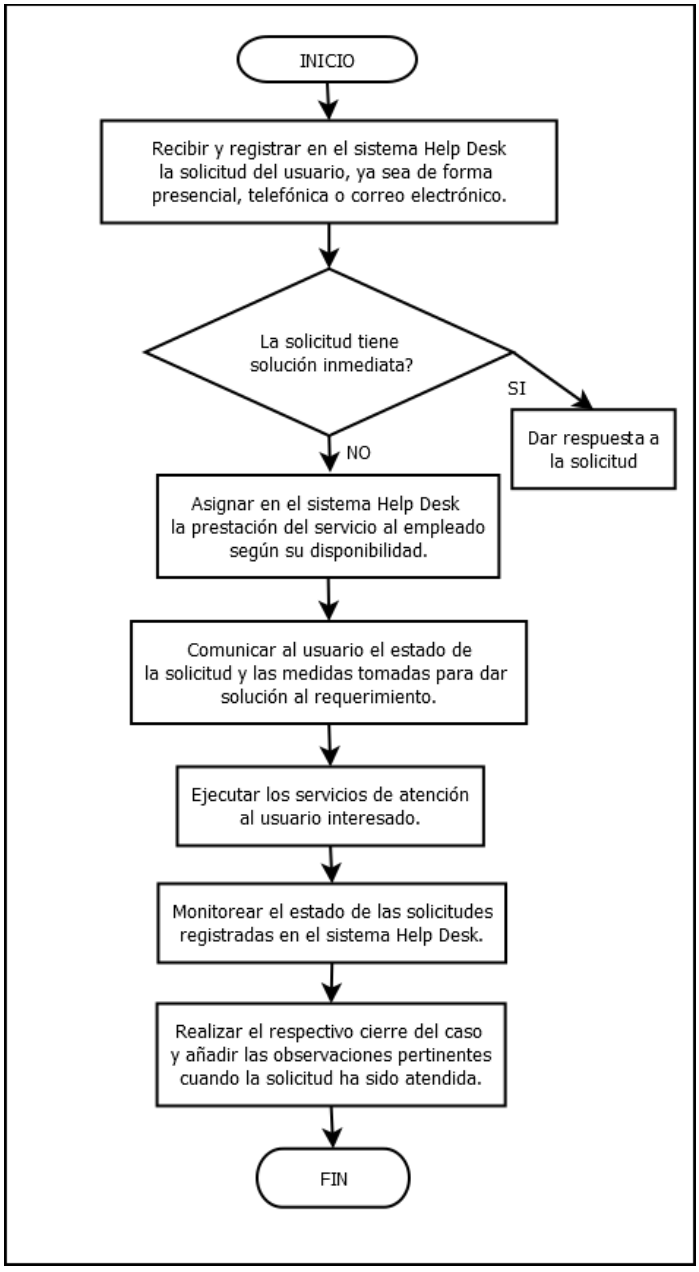
En la tabla 1 se pueden observar los pasos seguidos en el procedimiento de atención a usuarios que se realiza en el área de sistemas por el equipo de soporte.

Tabla 1. Procedimiento atención al usuario.

No.	Actividad / Descripción	Cargo Responsable	Punto de Control
1	Recibir y registrar en el sistema Help Desk la solicitud del usuario, ya sea de forma presencial, telefónica o correo electrónico.	Equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.
2	Dar respuesta a la solicitud cuando esta se pueda solucionar inmediatamente. Si no hay solución inmediata, ésta se debe analizar y priorizar de acuerdo a la disponibilidad de los empleados del área y según la urgencia del servicio.	Líder del área, equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.
3	Asignar en el sistema Help Desk la prestación del servicio al empleado según su disponibilidad.	Líder del área, equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.
4	Comunicar al usuario el estado de la solicitud y las medidas tomadas para dar solución al requerimiento.	Equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.
5	Ejecutar los servicios de atención al usuario interesado.	Equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.
6	Monitorear el estado de las solicitudes registradas en el sistema Help Desk.	Líder del área, equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.
7	Realizar el respectivo cierre del caso y añadir las observaciones pertinentes cuando la solicitud ha sido atendida.	Líder del área, equipo de soporte.	Revisar registro en el Help Desk cada vez que sea necesario.

Fuente: Autor

Figura 4. Diagrama de flujo procedimiento atención al usuario.



Fuente: Propiedad del autor.

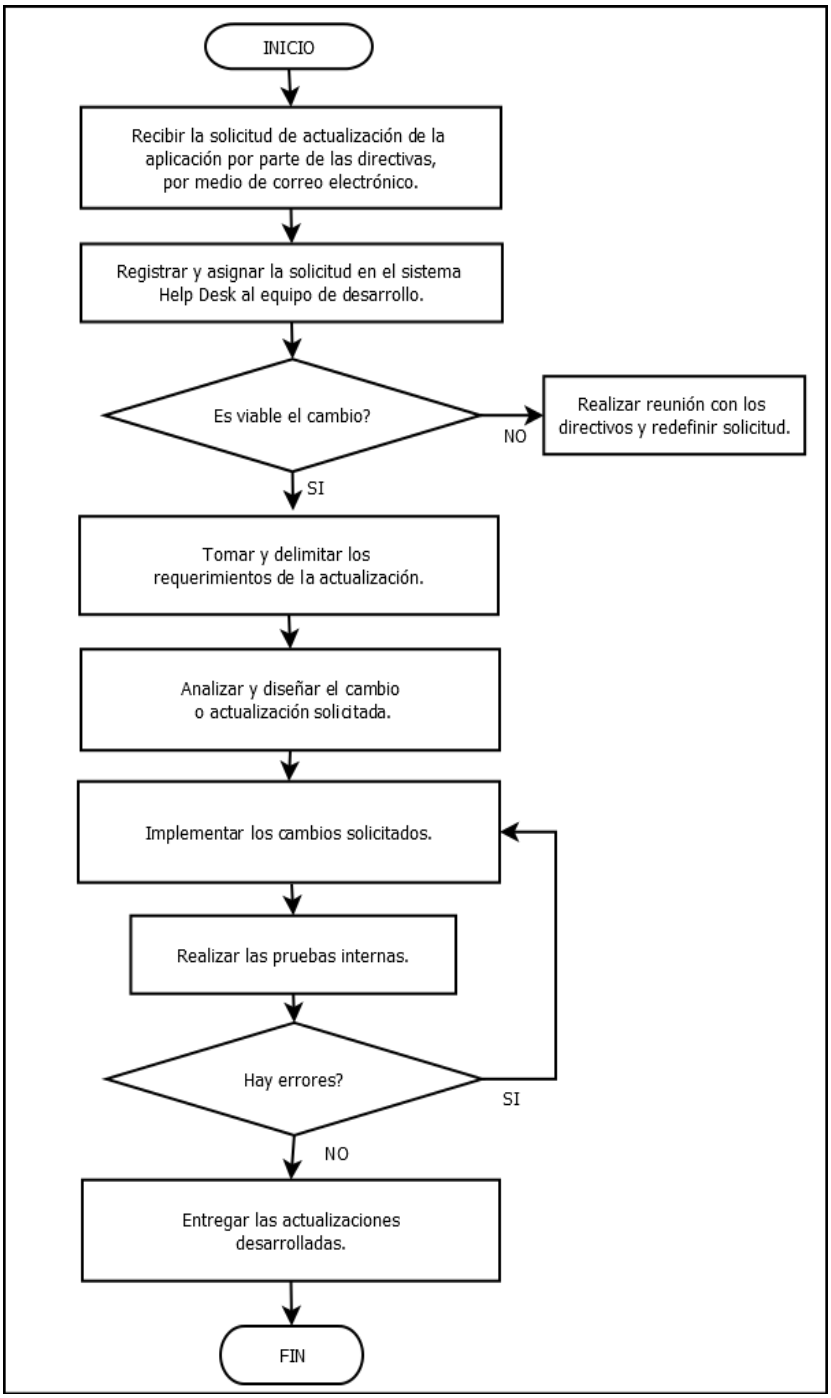
La tabla 2 presenta los pasos a seguir por el equipo de desarrollo en el procedimiento de cambios a la aplicación SINBA en el área de sistemas.

Tabla 2. Procedimiento cambios a la aplicación SINBA.

No.	Actividad / Descripción	Cargo Responsable	Punto de Control
1	Recibir la solicitud de actualización de la aplicación por parte de las directivas, por medio de correo electrónico.	Líder del área.	Reuniones semanales.
2	Registrar y asignar la solicitud en el sistema Help Desk al equipo de desarrollo.	Líder del área y desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.
3	Revisar y aprobar la viabilidad del cambio o actualización a desarrollar. Si el cambio o actualización no es viable, se debe realizar reunión con los directivos.	Líder del área y desarrolladores.	Reuniones semanales.
4	Tomar y delimitar los requerimientos de la actualización.	Líder del área y desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.
5	Analizar y diseñar el cambio o actualización solicitada.	Líder del área y desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.
6	Implementar la solución para adaptarse a los requerimientos solicitados.	Desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.
7	Realizar las pruebas internas.	Líder del área, equipo de pruebas y desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.
8	Efectuar las modificaciones resultado de las pruebas.	Líder del área, equipo de pruebas y desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.
9	Entregar las actualizaciones desarrolladas e implementadas. Todo proceso de desarrollo es documentado y guardado en un repositorio en la nube.	Líder del área y desarrolladores.	Revisar el registro en el archivo del área y Help Desk cada vez que sea necesario.

Fuente: Autor

Figura 5. Diagrama de flujo procedimiento cambios a la aplicación SINBA.



Fuente: Propiedad del autor.

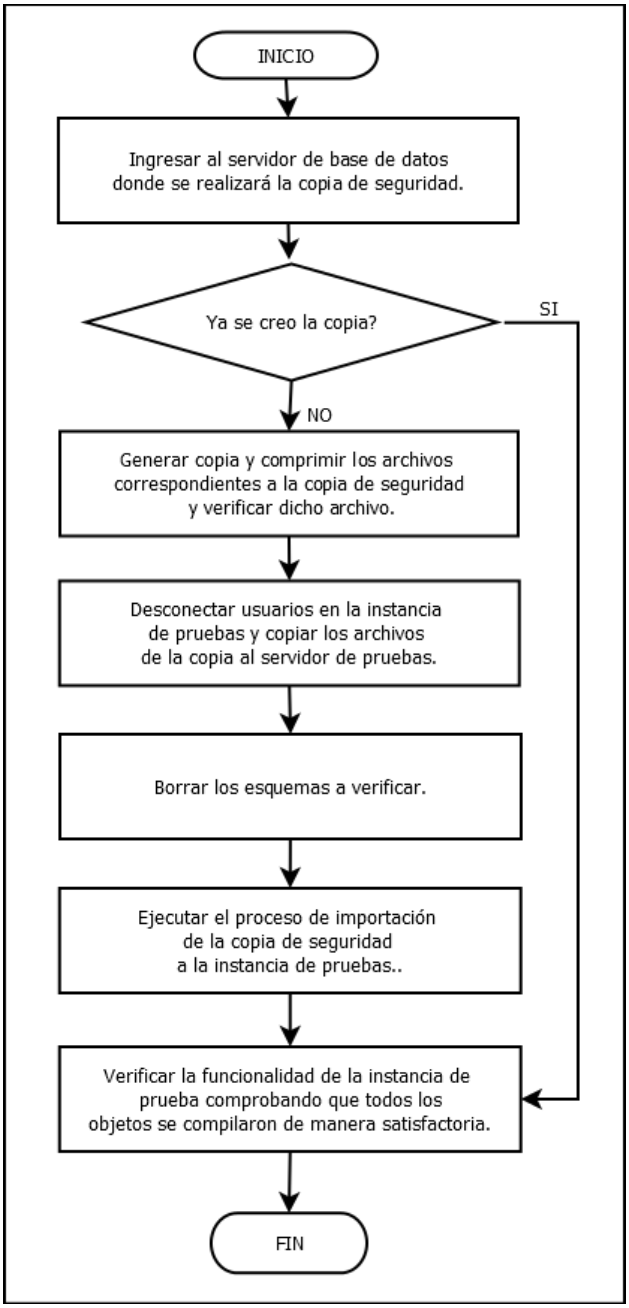
En la tabla 3 se presentan los pasos seguidos en el procedimiento de copias de seguridad bases de datos que se realiza en el área de sistemas por el DBA.

Tabla 3. Procedimiento copias de seguridad bases de datos.

No.	Actividad / Descripción	Cargo Responsable	Punto de Control
1	Ingresar al servidor de base de datos donde se realizará la copia de seguridad.	DBA.	Log de acceso al servidor.
2	Verificar que la copia de seguridad está creada. Si no está creada se procede a generarla.	DBA.	Log del proceso de exportación, cada vez que sea necesario.
3	Comprimir los archivos correspondientes a la copia de seguridad y verificar dicho archivo.	DBA.	Copia de seguridad comprimida, cada vez que sea necesario.
4	Copiar los archivos de la copia de seguridad al servidor de ambiente de pruebas.	DBA.	Archivos copiados en la carpeta correspondiente, cada vez que sea necesario.
5	Verifica si existen usuarios conectados en la instancia de pruebas y que hagan parte de los esquemas que se van a importar. Si se encuentran conectados se procede a desconectarlos.	DBA,	Registro de la actividad realizada satisfactoriamente, cada vez que sea necesario.
6	Borrar los esquemas a verificar.	DBA.	Registro de la actividad realizada satisfactoriamente, cada vez que sea necesario.
7	Ejecutar el proceso de importación de la copia de seguridad a la instancia de pruebas.	DBA.	Log del proceso de importación, cada vez que sea necesario.
8	Verificar la funcionalidad de la instancia de prueba comprobando que todos los objetos se compilaron de manera satisfactoria.	DBA.	Registro en la bitácora de la cantidad de objetos descompilados, cada vez que sea necesario.

Fuente: Autor

Figura 6. Diagrama de flujo procedimiento copias de seguridad bases de datos.



Fuente: Propiedad del autor.

4. CLASIFICACION DE LOS ACTIVOS DE LA EMPRESA E IDENTIFICACION DE AMENAZAS Y VULNERABILIDADES.

Teniendo en cuenta la metodología MARGERIT esta fase ofrece un método que permite la identificación rápida y homogénea de los activos, facilitando la integración de análisis realizados por diferentes equipos.

4.1 TIPOS DE ACTIVOS

Es una clasificación que permite tener referencia sobre los activos para su documentación, identificación de amenazas y establecimiento de controles o salvaguardas.

La metodología propone clasificar los activos para un sistema de información y los define como aquellos que son de gran importancia para el funcionamiento de la organización[64].

Dentro de los tipos de activos que propone la metodología tenemos:

- Esenciales. En un sistema de información hay 2 cosas esenciales La información que se maneja y los servicios que prestan. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema[65].
- [ARCH] Arquitectura del sistema. Existe una dependencia de un tercero para prestar nuestros servicios.
- [D] Datos/Información. Almacenados y/o transmitidos por algún medio de transmisión de datos.
- [S] Servicios. Los prestados por el sistema.
- [SW] Software - Aplicaciones informáticas. Aplicativos y desarrollos.

[64] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. p. 7.
[65] Ibid., p. 8.

- [HW] Equipamiento informático (hardware). Medios físicos que soportan los servicios prestados.

- [COM] Redes de comunicaciones. Medios propios o de terceros para transporte de datos.

- [Media] Soportes de información. Dispositivos electrónicos o no para almacenamiento de información permanente o por largos periodos.

- [AUX] Equipamiento auxiliar. Brindan soporte a los sistemas de información pero no necesariamente están vinculados con datos.

- [L] Instalaciones. Edificios u oficinas donde opera la empresa y que requiere su evaluación ya que su buen estado depende el funcionamiento de la misma

- [P] Personal. El talento humano que por su actividad relacionada con los sistemas de información.

4.2 CLASIFICACION DE LOS ACTIVOS

La tabla 4 presenta los activos identificados y su clasificación de acuerdo a las visitas que se realizaron a las instalaciones de la empresa y con la información que se recopiló de empleados.

Tabla 4. Activos a asegurar y su clasificación

Tipo de activo	**Activo**
[ARCH] Arquitectura	
	[EXT] DataCenter
[D] Datos/Información	
	[INFCL] Información de clientes
	[INFEMP] Información de empresas asociadas
	[INFPROD] Información de productos
	[ICONF] Información de configuración
	[ICOD] Código Fuente
	[EXE] Código ejecutable
	[BACKUP] Copias de respaldo
	[TEST] Datos de prueba

Tipo de activo	Activo
[S] Servicios	
	[ICL] Inscripción clientes
	[EMPASO] Inscripción empresas asociadas
	[CREPROD] Creación de productos
[SW] Software	
	[PRP] Desarrollo propio SINBA
	[STD] Estándar
	[BROWSER] Navegador web
	[APP] Servidor de aplicaciones
	[DBMS] Sistema de gestión de bases de datos
	[OFFICE] Ofimática
	[AV] Anti virus
	[OS] Sistema operativo
	[HRRDES]Herramientas de desarrollo
[HW] Equipamiento informático	
	[PCPRUEBAS] Computadores de pruebas
	[PCDES] Computadores de desarrollo
	[PCSOP] Computadores de soporte
	[IMPSOP] Impresora de soporte
	[LAN] Cableado red de área local
	[SWITCH] Switch
[COM] Redes de comunicaciones	
	[INT] Internet
	[PSTN] Red telefónica
	[LAN] Red local
[Media] Soportes de información	
	[NON_ELECTRONIC] no electrónicos
	[PRINTED] Material impreso. Contratos.
[AUX] Equipamiento auxiliar	
	[AC] Equipos de climatización
	[FURNITURE] Mobiliario
[L] Instalaciones	
	[OFI] Oficina
	[BUILDING] Edificio

Tipo de activo	Activo
[P] Personal	
	[ADM] Administradores de sistemas
	[DBA] Administrador base de datos
	[DES] Desarrolladores
	[SOP] Soporte
	[CMR] Comercial
	[UE] Usuarios externos
	[UI] Usuarios internos

Fuente: Autor

4.3 VALORACIÓN DE ACTIVOS

Para valorar los activos se puede usar cualquier escala de valores. Pero por facilidad y practicidad se recomienda usar una escala común para todas las dimensiones, permitiendo comparar riesgos, o una escala logarítmica, centrada en diferencias relativas de valor, y no en diferencias absolutas y se use un criterio homogéneo que permita comparar análisis realizados por separado[66].

De acuerdo a la metodología MAGERIT para valorar un activo se debe cuantificar el daño o perjuicio que causaría para la organización si una amenaza se materializa, ese daño o perjuicio afecta uno o varios atributos o características valiosas del activo, conocidas como dimensiones.

En esta fase tomamos las dimensiones de valoración en cada activo y aplicamos la escala de valores establecidos en la metodología.

Las dimensiones que se van a valorar son[67]:

- [D] Disponibilidad: El activo puede ser usado por las entidades o procesos autorizados lo requieran.

[66] Ibid., p. 19.
[67] Ibid., p. 19.

- [I] Integridad de los datos: El activo no ha sido alterado por individuos, entidades o procesos no autorizados. Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

- [C] Confidencialidad: Es el aseguramiento de que la información es accesible sólo para aquellos individuos o entidades autorizados.

- [A] Autenticidad: La entidad que accede al activo es quien dice ser.

- [T]Trazabilidad: El acceso a la información protegida y la realización de operaciones debe ser registrada para evitar el repudio por parte de quien ejecuta dicha operación.

Las valoraciones pueden ser económicas o cualitativas, estas últimas quedan sujetas al criterio del usuario.

En la tabla 5 se presenta la escala de valores estándar recomendada por la metodología MAGERIT.

Tabla 5. Escala de valoración que se va a emplear

Valor		**Criterio**
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave a la organización
6-8	Alto	Daño grave a la organización
3-5	Medio	Daño importante a la organización
1-2	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.

En la tabla 6 se presenta la valoración de cada de una de las dimensiones de los activos identificados.

Tabla 6. Valoración de activos

Activo	**Dimensiones**				
	D	**I**	**C**	**A**	**T**
[ARCH] Arquitectura					
[EXT] DataCenter	10	9	9	9	9
[D] Datos/Información					
[INFCL] Información de clientes	7	7	7	9	8
[INFEMP] Información de empresas asociadas	7	7	7	9	9
[INFPROD] Información de productos	7	7	7	7	9
[ICONF] Información de configuración	9	9	9	9	9
[ICOD] Código Fuente	8	9	9	10	9
[EXE] Código ejecutable	7	9	9	8	9
[BACKUP] Copias de respaldo	8	9	10	10	10
[TEST] Datos de prueba	4	5	6	5	5
[S] Servicios					
[ICL] Inscripción clientes	8	9	9	8	9
[EMPASO] Inscripción empresas asociadas	7	9	9	8	9
[CREPROD] Creación de productos	7	8	8	9	9
[SW] Software					
[PRP] Desarrollo propio SINBA	10	10	10	10	10
[STD] Estándar	2	2	2	2	3
[BROWSER] Navegador web	2	3	4	2	4
[APP] Servidor de aplicaciones	9	9	9	9	9
[DBMS] Sistema de gestión de bases de datos	10	9	9	10	10
[OFFICE] Ofimática	2	2	2	1	2
[AV] Anti virus	3	2	2	2	2
[OS] Sistema operativo	6	6	6	6	7
[HRRDES]Herramientas de desarrollo	4	5	4	5	5
[HW] Equipamiento informático					
[PCPRUEBAS] Computadores de pruebas	3	3	4	5	5
[PCDES] Computadores de desarrollo	4	8	9	8	9
[PCSOP] Computadores de soporte	4	4	4	5	6
[IMPSOP] Impresora de soporte	0	0	0	0	0
[LAN] Cableado red de área local	1	3	4	5	7
[SWITCH] Switch	1	5	5	5	4

Activo	Dimensiones				
	D	**I**	**C**	**A**	**T**
[COM] Redes de comunicaciones					
[INT] Internet	1	2	2	2	2
[PSTN] Red telefónica	3	3	3	4	4
[LAN] Red local	1	5	5	5	7
[Media] Soportes de información					
[NON_ELECTRONIC] no electrónicos					
[PRINTED] Material impreso. Contratos.	7	9	9	8	9
[AUX] Equipamiento auxiliar					
[AC] Equipos de climatización	0	0	0	0	0
[FURNITURE] Mobiliario	0	0	0	0	0
[L] Instalaciones					
[OFI] Oficina	7		8	8	8
[BUILDING] Edificio	7		8	8	8
[P] Personal					
[ADM] Administradores de sistemas	6		7	7	
[DBA] Administrador base de datos	7		9	9	
[DES] Desarrolladores	5		8	9	
[SOP] Soporte	4		6	7	
[CMR] Comercial	4		6	7	
[UE] Usuarios externos	1		4	4	
[UI] Usuarios internos	1		6	4	

Fuente: Autor

4.4 IDENTIFICACION Y VALORACION DE AMENAZAS

En esta etapa se muestra el daño que puede causar una amenaza sobre los tipos de activos si ésta se materializa. La valoración de la amenaza está relacionada con el daño que puede causar a una o varias de las dimensiones de un activo identificado, también se mide su probabilidad, es decir, cuán probable es que la amenaza se materialice. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.[68]

[68] Ibid., p. 15..

La metodología presenta un catálogo de amenazas posibles, pero éste no es definitivo.

La tabla 7 presenta los valores para la medir el daño o nivel de degradación que pueden presentar los activos se vean afectados por las amenazas que los acechan.

Tabla 7. Valores para medir degradación

Valor	Descripción	
100%	MA	Muy alta
80%	A	Alta
50%	M	Media
20%	B	Baja
10%	MB	Muy baja

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método.

La tabla 8 presenta la escala de valores que se usarán para medir la probabilidad de que una amenaza se materialice sobre un activo.

Tabla 8. Valores para medir probabilidad de ocurrencia

Valor	Descripción		
100	MF	Muy frecuente	A diario
10	F	Frecuente	Mensualmente
1	N	Normal	Una vez al año
1/10	P	Poco	Cada varios años
1/100	MP	Muy poco frecuente	Siglos

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I- Método.

Para cumplir con este objetivo se toma el listado de amenazas que se presentan en el catálogo de elementos libro II Versión 3.0 de la metodología MAGERIT, las cuales están clasificadas en 4 categorías:

- [N] Desastres naturales

- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Las siguientes tablas muestran las amenazas sobre los activos identificados y la valoración de cada una de las dimensiones de los activos.

Tabla 9. Valoración amenazas DataCenter

Activo: [EXT] DataCenter						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	P	A				
[N.3] Terremotos	P	A				

Fuente: Autor

Tabla 10. Valoración amenazas Servicios

[S] Servicios						
Activo: [IFCL] Inscripción clientes						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	A	A	A		
[E.2] Errores del administrador	P	A	A	A		
[A.5] Suplantación de la identidad del usuario	P		A	A	A	
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	N	M	M	M		
[A.11] Acceso no autorizado	P		A	A		
[A.13] Repudio	P		A			A
[A.18] Destrucción de información	N	A				
[A.19] Divulgación de información	P			A		
[A.24] Denegación de servicio	P	A				
Activo: [EMPASO] Inscripción empresas asociadas						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	A	A	A		
[E.2] Errores del administrador	P	A	A	A		
[A.5] Suplantación de la identidad del usuario	P		A	A	A	

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	M	M	M		
[A.11] Acceso no autorizado	P		A	A		
[A.13] Repudio	P		A			A
[A.18] Destrucción de información	P	A				
[A.19] Divulgación de información	P			A		
[A.24] Denegación de servicio	P	A				
Activo: [CREPROD] Creación de productos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	P	A	A	A		
[E.2] Errores del administrador	P	A	A	A		
[A.5] Suplantación de la identidad del usuario	P		A	A	A	
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P		A	A		
[A.13] Repudio	P		A			A
[A.18] Destrucción de información	P	A				
[A.19] Divulgación de información	P			A		
[A.24] Denegación de servicio	P	A				

Fuente: Autor

Tabla 11. Valoración amenazas Datos/Información

[D] Datos/Información						
Activo: [ICONF] Información de configuración						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	M	M	A		
[E.2] Errores del administrador	N	A	A	A		
[E.4] Errores de configuración	N		A			
[E.15] Alteración accidental de la información	F		M			
[E.18] Destrucción de información	F	A				
[E.19] Fugas de información	P			A		
[A.5] Suplantación de la identidad del usuario	P		A	A	A	

Activo: [ICOD] Código Fuente						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.5] Avería de origen físico o lógico	N	B				
[I.8] Fallo de servicios de comunicaciones	N	B				
[E.3] Errores de monitorización	P	B				B
[E.4] Errores de configuración	N	B	B			
[E.8] Difusión de software dañino	P	M	M	M		
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas	N	M	A	A		
[E.21]Errores de mantenimiento/actualización de programas	P	M	M			
[E.23] Errores de mantenimiento/actualización de equipos	P	B				
[E.25] Pérdida de equipos	P	B				
[E.28] Indisponibilidad del personal	F	M	B	B		
[A.15] Modificación deliberada de la información	P		M			
[A.18] Destrucción de información	P	A				
[A.19] Divulgación de información	P			M		
[A.23] Manipulación de los equipos	P	A		A		
[A.25] Robo	P	M		A		
[A.26] Ataque destructivo	P	M				
[A.28] Indisponibilidad del personal	F	B				
[A.30] Ingeniería social	P	M	A	A		
Activo: [EXE] Código ejecutable						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.4] Errores de configuración	N	B	M			
[E.8] Difusión de software dañino	N	B	M	M	M	
[E.20] Vulnerabilidades de los programas	P		M	M		
[E.21]Errores de mantenimiento/actualización de programas	N		M	M	M	M
[E.25] Pérdida de equipos	P	B				
[A.23] Manipulación de los equipos	N	B	B			
[A.25] Robo	P	B		M	B	
Activo: [BACKUP] Copias de respaldo						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[I.4] Contaminación electromagnética	P	MB				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.5] Avería de origen físico o lógico	P	M				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MB				
[I.10] Degradación de los soportes de almacenamiento de la información	P	M				M
[E.1] Errores de los usuarios	N	B	B	B		
[E.2] Errores del administrador	P	M	M	M		
[E.3] Errores de monitorización	P		M			M
[E.4] Errores de configuración	N	M	M			M
[E.20] Vulnerabilidades de los programas	P	B				M
[A.6] Abuso de privilegios de acceso	P			M		M
[A.7] Uso no previsto	P			A		
[A.11] Acceso no autorizado	P			A		M
[A.15] Modificación deliberada de la información	P	M	A	M		
[A.18] Destrucción de información	P	M				M
[A.19] Divulgación de información	P		B	A		
[A.23] Manipulación de los equipos	P	M		A		M
[A.25] Robo	P	M		A		M
[A.26] Ataque destructivo	P	M				M
Activo: [TEST] Datos de prueba						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	F			B		
[E.2] Errores del administrador	N	M		M	B	
[E.4] Errores de configuración	N			M		
[E.19] Fugas de información	P			M		
[E.25] Pérdida de equipos	P	M		M		
[A.5] Suplantación de la identidad del usuario	P			M		
[A.6] Abuso de privilegios de acceso	P			M		
[A.7] Uso no previsto	P			M		
[A.11] Acceso no autorizado	P			M		
[A.19] Divulgación de información	P			M		
[A.25] Robo	P	M		M		
[A.26] Ataque destructivo	P	M		M		
Activo: [INFCL] Información de clientes						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	N	M	A	M		
[E.2] Errores del administrador	P	M	A	A	M	

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.4] Errores de configuración	P	A		A		
[E.19] Fugas de información	P			A		
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P			A		
[A.11] Acceso no autorizado	P	A	A	A		
[A.19] Divulgación de información	P		A	A		
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		
Activo: [INFEMP] Información de empresas asociadas						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	N	M	A	M		
[E.2] Errores del administrador	P	M	A	A	M	
[E.4] Errores de configuración	P	A		A		
[E.19] Fugas de información	P			A		
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P			A		
[A.11] Acceso no autorizado	P	A	A	A		
[A.19] Divulgación de información	P		A	A		
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		
Activo: [INFPROD] Información de productos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	N	M	A	M		
[E.2] Errores del administrador	P	M	A	A	M	
[E.4] Errores de configuración	P	A		A		
[E.19] Fugas de información	P			A		
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P			A		
[A.11] Acceso no autorizado	P	A	A	A		
[A.19] Divulgación de información	P		A	A		

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		

Fuente: Autor

Tabla 12. Valoración amenazas Software

[SW] Software						
Activo: [PRP] Desarrollo propio SINBA						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	M	A	A	A	A
[E.4] Errores de configuración	P	A		A	A	A
[E.19] Fugas de información	P			A		
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		A
[A.7] Uso no previsto	P	M	A	A		
[A.11] Acceso no autorizado	P	A	A	A		A
[A.15] Modificación deliberada de la información	P		A	A		
[A.18] Destrucción de información	P	A	A	A		A
[A.19] Divulgación de información	P		A	A	A	
[A.24] Denegación de servicio	P	A				
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		
Activo: [STD] Estándar						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	M				
[E.4] Errores de configuración	N	M		M		
[E.21] Errores de mantenimiento / actualización de programas	N	A	A			
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	M				
[A.5] Suplantación de la identidad del usuario	P		M	M		
[A.6] Abuso de privilegios de acceso	P		M	A		

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.7] Uso no previsto	P			A		
[A.11] Acceso no autorizado	P		A	A		
[A.15] Modificación deliberada de la información	P	M	A			
[A.18] Destrucción de información	P	M				
[A.19] Divulgación de información	P			A		
Activo: [BROWSER] Navegador web						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.7] Uso no previsto	N			M		
[E.8] Difusión de software dañino	N		M			
Activo: [APP] Servidor de aplicaciones						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	M				
[E.4] Errores de configuración	P	M				
[E.21] Errores de mantenimiento / actualización de programas	P	A	A			
[E.23] Errores de mantenimiento / actualización de equipos	P	A				
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.6] Abuso de privilegios de acceso	P	M			A	A
[A.11] Acceso no autorizado	P		A	A		A
[A.15] Modificación deliberada de la información	P	M	A			M
[A.19] Divulgación de información	P			A		
[A.24] Denegación de servicio	P	A				
[A.25] Robo	P	A		A		
[A.26] Ataque destructivo	P	A				A
Activo: [DBMS] Sistema de gestión de bases de datos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	A	A	A	A	A
[E.4] Errores de configuración	P	A		A	A	A
[E.19] Fugas de información	P			A		
[E.20] Vulnerabilidades de los programas	N	A	M	M	A	A
[E.21] Errores de mantenimiento / actualización de programas	N	M	A			
[E.23] Errores de mantenimiento / actualización de equipos	P	A				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.24] Caída del sistema por agotamiento de recursos	N	A				
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		A
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P	A	A	A		A
[A.15] Modificación deliberada de la información	P		A	A		
[A.18] Destrucción de información	P	A	A	A		A
[A.19] Divulgación de información	P		A	A	A	
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		A
Activo: [OFFICE] Ofimática						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.8] Difusión de software dañino	N	M	M			
[E.20] Vulnerabilidades de los programas	N	A		M	A	A
[E.21] Errores de mantenimiento / actualización de programas	N	M	A			
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A		A		
[A.7] Uso no previsto	N			M		
[A.11] Acceso no autorizado	P	B		M		
Activo: [AV] Anti virus						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	N	M				A
[E.2] Errores del administrador	P	A				A
[E.4] Errores de configuración	P	A			M	A
[A.11] Acceso no autorizado	P	A	A			A
Activo: [OS] Sistema operativo						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	A			A	A
[E.4] Errores de configuración	P	A			A	A
[E.8] Difusión de software dañino	P	A			A	A
[E.19] Fugas de información	P			A		A

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.20] Vulnerabilidades de los programas	N	A		M	A	A
[E.21] Errores de mantenimiento / actualización de programas	N	M	A		A	A
[E.23] Errores de mantenimiento / actualización de equipos	P	A				
[E.25] Pérdida de equipos	P	A		A		
[A.3] Manipulación de los registros de actividad	P		A			A
[A.4] Manipulación de la configuración	P	A	A	A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		A
[A.11] Acceso no autorizado	P	A	A	A		A
[A.15] Modificación deliberada de la información	P		A	A		
[A.18] Destrucción de información	P	A	A	A		A
[A.19] Divulgación de información	P		A	A	A	
[A.25] Robo	P	A		A		
[A.26] Ataque destructivo	P	A				A
Activo: [HRRDES]Herramientas de desarrollo						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.8] Difusión de software dañino	P	M	M			
[E.20] Vulnerabilidades de los programas	N	A		M	A	A
[E.21] Errores de mantenimiento / actualización de programas	N	M	A			
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A		A		
[A.11] Acceso no autorizado	P	B		M		

Fuente: Autor

Tabla 13. Valoración amenazas Equipamiento informático

[HW] Equipamiento informático						
Activo: [PCPRUEBAS] Computadores de pruebas						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.3] Contaminación mecánica	P	A				
[I.4] Contaminación electromagnética	P	A				
[I.5] Avería de origen físico o lógico	N	A				
[I.6] Corte del suministro eléctrico	N	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P	A				
[E.2] Errores del administrador	N	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.6] Abuso de privilegios de acceso	P	A	M	M		
[A.7] Uso no previsto	P	A	M	M		
[A.11] Acceso no autorizado	P		M	M		
[A.23] Manipulación de los equipos	P	A		M		
[A.25] Robo	P	A		M		
[A.26] Ataque destructivo	P	A				
Activo: [PCDES] Computadores de desarrollo						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.3] Contaminación mecánica	P	A				
[I.4] Contaminación electromagnética	P	A				
[I.5] Avería de origen físico o lógico	N	A				
[I.6] Corte del suministro eléctrico	N	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P	A				
[E.2] Errores del administrador	N	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.25] Pérdida de equipos	P	A				
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P		A	A		A
[A.23] Manipulación de los equipos	P	A		A		
[A.25] Robo	P	A		A		
[A.26] Ataque destructivo	P	A				
Activo: [PCSOP] Computadores de soporte						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.3] Contaminación mecánica	P	A				
[I.4] Contaminación electromagnética	P	A				
[I.5] Avería de origen físico o lógico	N	A				
[I.6] Corte del suministro eléctrico	N	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P	A				
[E.2] Errores del administrador	N	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.6] Abuso de privilegios de acceso	P	A	M	M		
[A.7] Uso no previsto	P	A	M	M		
[A.11] Acceso no autorizado	P		M	M		
[A.23] Manipulación de los equipos	P	A		M		
[A.25] Robo	P	A		M		
[A.26] Ataque destructivo	P	A				
Activo: [LAN] Cableado red de área local						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.*] Desastres industriales	P	A				
[I.3] Contaminación mecánica	P	A				
[I.5] Avería de origen físico o lógico	N	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.23] Manipulación de los equipos	P	A				
[A.25] Robo	P	A				
[A.26] Ataque destructivo	P	A				
Activo: [SWITCH] Switch						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.3] Contaminación mecánica	P	A				
[I.5] Avería de origen físico o lógico	P	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.23] Manipulación de los equipos	P	A				
[A.25] Robo	P	A				
[A.26] Ataque destructivo	P	A				

Fuente: Autor

Tabla 14. Valoración amenazas Redes de comunicaciones

[COM] Redes de comunicaciones						
Activo: [INT] Internet						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.8] Fallo de servicios de comunicaciones	N	A				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	N	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			A		
[E.10] Errores de secuencia	P		A			
[A.5] Suplantación de la identidad del usuario	P		A	A	A	
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.10] Alteración de secuencia	P		A			
[A.11] Acceso no autorizado	P		A	A		
[A.12] Análisis de tráfico	P			A		
[A.14] Interceptación de información	P			A		
[A.15] Modificación deliberada de la información	P		A			
Activo: [PSTN] Red telefónica						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.9] Errores de [re-]encaminamiento	P			A		
[A.7] Uso no previsto	P	A	A	A		
[A.10] Alteración de secuencia	P		A			
[A.14] Interceptación de información	P			A		
Activo: [LAN] Red local						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.2] Errores del administrador	N	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			A		
[E.10] Errores de secuencia	P		A			
[A.5] Suplantación de la identidad del usuario	P		A	A	A	
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.10] Alteración de secuencia	P		A			
[A.11] Acceso no autorizado	P		A	A		
[A.12] Análisis de tráfico	P			A		
[A.14] Interceptación de información	P			A		
[A.15] Modificación deliberada de la información	P		A			

[Media] Soportes de información						
Activo: [PRINTED] Material impreso. Contratos.						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[A.7] Uso no previsto	P	A		A		
[A.11] Acceso no autorizado	P			A		
[A.18] Destrucción de información	P	A				
[A.19] Divulgación de información	P			MA		
[A.25] Robo	P	A		MA		
[A.26] Ataque destructivo	P	A				

Fuente: Autor

Tabla 15. Valoración amenazas Instalaciones

[L] Instalaciones						
Activo: [OFI] Oficina						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P			A		
[E.15] Alteración accidental de la información	P		A			
[E.18] Destrucción de información	P	A				
[E.19] Fugas de información	P			A		
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P		A	A		

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.15] Modificación deliberada de la información	P		A			
[A.18] Destrucción de información	P	M				
[A.19] Divulgación de información	P			A		
[A.26] Ataque destructivo	P	A				
Activo: [BUILDING] Edificio						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P			A		
[E.15] Alteración accidental de la información	P		A			
[E.18] Destrucción de información	P	A				
[E.19] Fugas de información	P			A		
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P		A	A		
[A.15] Modificación deliberada de la información	P		A			
[A.18] Destrucción de información	P	M				
[A.19] Divulgación de información	P			A		
[A.26] Ataque destructivo	P	A				

Fuente: Autor

Tabla 16. Valoración amenazas Personal

[P] Personal						
Activo: [ADM] Administradores de sistemas						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	N	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	N	M				
[A.28] Indisponibilidad del personal	P	M				

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.29] Extorsión	P	B	A	A		
[A.30] Ingeniería social	P	B	A	A		
Activo: [DBA] Administrador base de datos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	B				
[E.19] Fugas de información	P			A		
[E.28] Indisponibilidad del personal	N	A				
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	B	A	A	A	A
[A.30] Ingeniería social	P	B	A	A	A	
Activo: [DES] Desarrolladores						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	M				
[E.19] Fugas de información	P			A		
[E.28] Indisponibilidad del personal	N	A				
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	B	A	A		
[A.30] Ingeniería social	P	B	A	A		
Activo: [SOP] Soporte						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	N	A				
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	B	A	A		
[A.30] Ingeniería social	P	B	A	A		
Activo: [CMR] Comercial						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	N	A				
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	B	M	M		
[A.30] Ingeniería social	P	B	M	M		
Activo: [UE] Usuarios externos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.19] Fugas de información	P			M		
Activo: [UI] Usuarios internos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	B				
[E.19] Fugas de información	P			B		
[E.28] Indisponibilidad del personal	N	A				
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	B	B	B		
[A.30] Ingeniería social	P	B	M	M		

Fuente: Autor

4.5 CÁLCULO DEL RIESGO

Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto.[69]

No es necesario usar herramientas o métodos complejos para identificar la importancia de los activos bajo amenaza.

La metodología MAGERIT ofrece el análisis mediante tablas de fácil aplicación, en el cual se combina el impacto con la probabilidad para calcular el riesgo.

[69] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de técnicas. Madrid, España octubre de 2012. p. 6.

La tabla 17 presenta la descripción de valores para medir el riesgo a que se ve sometido un activo, para ello se parte de las valoraciones hechas anteriormente.

Tabla 17. Descripción de valores del riesgo.

Riesgo	
Valor	Descripción
MA	Crítico
A	Importante
M	Apreciable
B	Bajo
MB	Despreciable

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de técnicas. Madrid, España octubre de 2012.

La tabla 18 presenta los valores que se usaron para medir el riesgo según la probabilidad de ocurrencia y el impacto que puede causar una amenaza.

Tabla 18. Valores de escala cálculo de riesgos.

Riesgo		Probabilidad				
		MP	P	N	F	MF
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de técnicas. Madrid, España octubre de 2012.

Los riesgos que posean valores A o MA requieren atención inmediata. A continuación se presentan las tablas y los resultados obtenidos.

Las siguientes tablas presenta el valor de los riesgos sobre los activos de la empresa.

Tabla 19. Cálculo riesgos DataCenter

Activo:[EXT] DataCenter	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	M	M
[N.2] Daños por agua	P	B	B
[N.3] Terremotos	P	B	B

Fuente: Autor

Tabla 20. Cálculo riesgos Servicios

Activo:[IFCL] Inscripción clientes	Probabilidad	Impacto	Riesgo
[E.1]Errores de los usuarios	F	B	M
[E.2]Errores del administrador	P	A	A
[A.5]Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	N	M	M
[A.11]Acceso no autorizado	P	A	A
[A.13] Repudio	P	A	A
[A.18] Destrucción de información	M	MA	A
[A.19] Divulgación de información	P	A	A
[A.24]Denegación de servicio	P	A	A
Activo:[EMPASO] Inscripción empresas asociadas			
[E.1] Errores de los usuarios	F	B	M
[E.2]Errores del administrador	P	M	B
[A.5] Suplantación de la identidad del usuario	P	M	M
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	M	M
[A.11]Acceso no autorizado	P	A	A
[A.13] Repudio	P	B	B
[A.18] Destrucción de información	P	A	A
[A.19] Divulgación de información	P	M	M
[A.24]Denegación de servicio	P	B	B
Activo: [CREPROD] Creación de productos			
[E.1] Errores de los usuarios	P	M	M
[E.2]Errores del administrador	P	M	M

	Probabilidad	Impacto	Riesgo
[A.5] Suplantación de la identidad del usuario	P	M	M
[A.6]Abuso de privilegios de acceso	P	M	M
[A.7] Uso no previsto	P	B	B
[A.11]Acceso no autorizado	P	M	M
[A.13] Repudio	P	B	B
[A.18] Destrucción de información	P	A	A
[A.19] Divulgación de información	P	B	B
[A.24]Denegación de servicio	P	B	B

Fuente: Autor

Tabla 21. Cálculo riesgos Datos/Información

Activo:[ICONF] Información de configuración	Probabilidad	Impacto	Riesgo
[E.1] Errores de los usuarios	P	B	B
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	P	B	B
[E.15] Alteración accidental de la información	N	M	M
[E.18]Destrucción de información	P	A	A
[E.19] Fugas de información	P	B	B
[A.5] Suplantación de la identidad del usuario	P	M	M
Activo:[ICOD] Código Fuente			
[I.5] Avería de origen físico o lógico	N	B	B
[I.8] Fallo de servicios de comunicaciones	N	B	B
[E.3]Errores de monitorización	P	B	B
[E.4]Errores de configuración	N	B	B
[E.8]Difusión de software dañino	P	M	M
[E.19] Fugas de información	P	M	M
[E.20] Vulnerabilidades de los programas	N	M	M
[E.21]Errores de mantenimiento/actualización de programas	P	M	M
[E.23]Errores de mantenimiento/actualización de equipos	P	B	B
[E.25] Pérdida de equipos	P	B	B
[E.28] Indisponibilidad del personal	F	M	A
[A.15]Modificación deliberada de la información	P	M	M
[A.18]Destrucción de información	P	M	M
[A.19]Divulgación de información	P	M	M

	Probabilidad	Impacto	Riesgo
[A.23] Manipulación de los equipos	P	M	M
[A.25] Robo	P	M	M
[A.26] Ataque destructivo	P	M	M
[A.28] Indisponibilidad del personal	F	M	A
[A.30] Ingeniería social	P	M	M
Activo:[EXE]Código ejecutable			
[E.4]Errores de configuración	N	B	B
[E.8]Difusión de software dañino	N	B	B
[E.20]Vulnerabilidades de los programas	P	M	M
[E.21]Errores de mantenimiento/actualización de programas	N	M	M
[E.25] Pérdida de equipos	P	B	B
[A.23] Manipulación de los equipos	N	B	B
[A.25] Robo	P	B	B
Activo: [BACKUP] Copias de respaldo			
[N.1] Fuego	P	A	A
[I.4]Contaminación electromagnética	P	MB	MB
[I.5] Avería de origen físico o lógico	P	M	M
[I.7]Condiciones inadecuadas de temperatura o humedad	P	MB	MB
[I.10]Degradación de los soportes de almacenamiento de la información	P	M	M
[E.1] Errores de los usuarios	N	B	B
[E.2]Errores del administrador	P	M	M
[E.3]Errores de monitorización	P	M	M
[E.4]Errores de configuración	N	M	M
[E.20] Vulnerabilidades de los programas	P	B	B
[A.6]Abuso de privilegios de acceso	P	M	M
[A.7] Uso no previsto	P	M	M
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	M	M
[A.18]Destrucción de información	P	M	M
[A.19]Divulgación de información	P	A	A
[A.23]Manipulación de los equipos	P	M	M
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo:[TEST] Datos de prueba			
[E.1] Errores de los usuarios	P	M	M

	Probabilidad	Impacto	Riesgo
[E.2]Errores del administrador	N	M	M
[E.4]Errores de configuración	N	M	M
[E.19] Fugas de información	P	M	M
[E.25] Pérdida de equipos	P	M	M
[A.5] Suplantación de la identidad del usuario	P	M	M
[A.6] Abuso de privilegios de acceso	P	M	M
[A.7] Uso no previsto	P	M	M
[A.11] Acceso no autorizado	P	M	M
[A.19]Divulgación de información	P	M	M
[A.25] Robo	P	M	M
[A.26]Ataque destructivo	P	M	M
Activo:[INFCL] Información de clientes			
[E.1] Errores de los usuarios	N	M	M
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	P	A	A
[E.19]Fugas de información	P	A	A
[E.25]Pérdida de equipos	P	A	A
[A.5]Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.19]Divulgación de información	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [INFEMP] Información de empresas asociadas			
[E.1]Errores de los usuarios	N	M	M
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	P	A	A
[E.19] Fugas de información	P	A	A
[E.25] Pérdida de equipos	P	A	A
[A.5]Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.19]Divulgación de información	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A

Activo: [INFPROD] Información de productos	Probabilidad	Impacto	Riesgo
[E.1] Errores de los usuarios	N	M	M
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	P	A	A
[E.19] Fugas de información	P	A	A
[E.25] Pérdida de equipos	P	A	A
[A.5]Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.19]Divulgación de información	P	M	M
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A

Fuente: Autor

Tabla 22. Cálculo riesgos Software

Activo:[PRP] Desarrollo propio SINBA	Probabilidad	Impacto	Riesgo
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	P	A	A
[E.19]Fugas de información	P	A	A
[E.25]Pérdida de equipos	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	M	M
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	A	A
[A.18]Destrucción de información	P	A	A
[A.19]Divulgación de información	P	A	A
[A.24]Denegación de servicio	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [STD] Estándar			
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	N	B	B
[E.21]Errores de mantenimiento / actualización de programas	N	B	B
[E.23]Errores de mantenimiento / actualización de equipos	N	B	B

	Probabilidad	Impacto	Riesgo
[E.25]Pérdida de equipos	P	M	M
[A.5]Suplantación de la identidad del usuario	P	M	M
[A.6]Abuso de privilegios de acceso	P	M	M
[A.7]Uso no previsto	P	M	M
[A.11]Acceso no autorizado	P	M	M
[A.15]Modificación deliberada de la información	P	M	M
[A.18]Destrucción de información	P	M	M
[A.19]Divulgación de información	P	M	M
Activo:[BROWSER] Navegador web			
[A.7] Uso no previsto	N	B	B
[E.8]Difusión de software dañino	N	M	M
Activo:[APP] Servidor de aplicaciones			
[E.2]Errores del administrador	P	M	M
[E.4]Errores de configuración	P	M	M
[E.21]Errores de mantenimiento / actualización de programas	P	A	A
[E.23]Errores de mantenimiento / actualización de equipos	P	A	A
[E.24] Caída del sistema por agotamiento de recursos	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	M	M
[A.19]Divulgación de información	P	M	M
[A.24]Denegación de servicio	P	M	M
[A.25]Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo:[DBMS] Sistema de gestión de bases de datos			
[E.2]Errores del administrador	P	A	A
[E.4]Errores de configuración	P	A	A
[E.19]Fugas de información	P	A	A
[E.20]Vulnerabilidades de los programas	N	A	A
[E.21]Errores de mantenimiento / actualización de programas	N	M	M
[E.23]Errores de mantenimiento / actualización de equipos	P	A	A

	Probabilidad	Impacto	Riesgo
[E.24]Caída del sistema por agotamiento de recursos	N	A	A
[E.25]Pérdida de equipos	P	A	A
[A.5]Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7]Uso no previsto	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	A	A
[A.18]Destrucción de información	P	A	A
[A.19]Divulgación de información	P	A	A
[A.25]Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo:[OFFICE] Ofimática			
[E.8]Difusión de software dañino	N	M	M
[E.20]Vulnerabilidades de los programas	N	A	A
[E.21]Errores de mantenimiento / actualización de programas	N	M	M
[E.23]Errores de mantenimiento / actualización de equipos	N	A	A
[E.25]Pérdida de equipos	P	A	A
[A.7]Uso no previsto	N	M	M
[A.11]Acceso no autorizado	P	B	B
Activo: [AV] Anti virus			
[E.1]Errores de los usuarios	N	M	M
[E.2]Errores del administrador	P	A	A
[E.4]Errores de configuración	P	A	A
[A.11]Acceso no autorizado	P	A	A
Activo:[OS] Sistema operativo			
[E.2]Errores del administrador	P	A	A
[E.4]Errores de configuración	P	A	A
[E.8]Difusión de software dañino	P	A	A
[E.19]Fugas de información	P	A	A
[E.20]Vulnerabilidades de los programas	N	A	A
[E.21]Errores de mantenimiento / actualización de programas	N	M	M
[E.23]Errores de mantenimiento / actualización de equipos	P	A	A
[E.25]Pérdida de equipos	P	A	A

	Probabilidad	Impacto	Riesgo
[A.3] Manipulación de los registros de actividad	P	A	A
[A.4]Manipulación de la configuración	P	A	A
[A.5]Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	A	A
[A.18]Destrucción de información	P	A	A
[A.19]Divulgación de información	P	A	A
[A.25]Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo: [HRRDES]Herramientas de desarrollo			
[E.8]Difusión de software dañino	P	M	M
[E.20]Vulnerabilidades de los programas	N	A	A
[E.21]Errores de mantenimiento / actualización de programas	N	M	M
[E.23]Errores de mantenimiento / actualización de equipos	N	M	M
[E.25]Pérdida de equipos	P	B	B
[A.11]Acceso no autorizado	P	B	B

Fuente: Autor

Tabla 23. Cálculo riesgos equipamiento informático.

Activo: [PCPRUEBAS] Computadores de pruebas	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	B	MB
[N.*]Desastres naturales	P	A	A
[I.1]Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.3]Contaminación mecánica	P	M	M
[I.4]Contaminación electromagnética	P	M	M
[I.5] Avería de origen físico o lógico	N	M	M
[I.6]Corte del suministro eléctrico	N	M	M
[I.7]Condiciones inadecuadas de temperatura o humedad	P	M	M

	Probabilidad	Impacto	Riesgo
[I.11]Emanaciones electromagnéticas	P	M	M
[E.2]Errores del administrador	N	M	M
[E.23]Errores de mantenimiento / actualización de equipos	N	M	M
[E.25]Pérdida de equipos	P	M	M
[A.6]Abuso de privilegios de acceso	P	M	M
[A.7]Uso no previsto	P	M	M
[A.11]Acceso no autorizado	P	M	M
[A.23]Manipulación de los equipos	P	M	M
[A.25]Robo	P	M	M
[A.26]Ataque destructivo	P	M	M
Activo:[PCDES] Computadores de desarrollo			
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*]Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.3]Contaminación mecánica	P	A	A
[I.4]Contaminación electromagnética	P	A	A
[I.5] Avería de origen físico o lógico	N	A	A
[I.6]Corte del suministro eléctrico	N	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[I.11]Emanaciones electromagnéticas	P	A	A
[E.2]Errores del administrador	N	A	A
[E.23]Errores de mantenimiento / actualización de equipos	N	A	A
[E.25]Pérdida de equipos	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.23]Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo: [PCSOP] Computadores de soporte			
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*]Desastres naturales	P	A	A

	Probabilidad	Impacto	Riesgo
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.3]Contaminación mecánica	P	A	A
[I.4]Contaminación electromagnética	P	A	A
[I.5] Avería de origen físico o lógico	N	A	A
[I.6]Corte del suministro eléctrico	N	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[I.11]Emanaciones electromagnéticas	P	A	A
[E.2]Errores del administrador	N	A	A
[E.23]Errores de mantenimiento / actualización de equipos	N	A	A
[E.25]Pérdida de equipos	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.23]Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo: [LAN] Cableado red de área local			
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*]Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.3]Contaminación mecánica	P	A	A
[I.5] Avería de origen físico o lógico	N	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[E.23]Errores de mantenimiento / actualización de equipos	N	A	A
[E.25]Pérdida de equipos	P	A	A
[A.23]Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A
Activo: [SWITCH] Switch			
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M

	Probabilidad	Impacto	Riesgo
[N.*]Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.3]Contaminación mecánica	P	A	A
[I.5] Avería de origen físico o lógico	P	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[E.23]Errores de mantenimiento / actualización de equipos	N	A	A
[E.25]Pérdida de equipos	P	A	A
[A.23]Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A

Fuente: Autor

Tabla 24. Cálculo riesgos redes de comunicaciones.

Activo: [INT] Internet	Probabilidad	Impacto	Riesgo
[I.8]Fallo de servicios de comunicaciones	N	A	A
[E.2]Errores del administrador	N	M	M
[E.9] Errores de [re-]encaminamiento	P	A	A
[E.10]Errores de secuencia	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.10]Alteración de secuencia	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.12]Análisis de tráfico	P	A	A
[A.14]Interceptación de información	P	A	A
[A.15]Modificación deliberada de la información	P	A	A
Activo: [PSTN] Red telefónica			
[I.8]Fallo de servicios de comunicaciones	P	A	A
[E.9] Errores de [re-]encaminamiento	P	A	A
[A.7] Uso no previsto	P	A	A
[A.10]Alteración de secuencia	P	A	A
[A.14]Interceptación de información	P	A	A

	Probabilidad	Impacto	Riesgo
Activo: [LAN] Red local			
[I.8]Fallo de servicios de comunicaciones	P	A	A
[E.2]Errores del administrador	N	M	M
[E.9]Errores de [re-]encaminamiento	P	A	A
[E.10]Errores de secuencia	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6]Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.10]Alteración de secuencia	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.12]Análisis de tráfico	P	A	A
[A.14] Interceptación de información	P	A	A
[A.15]Modificación deliberada de la información	P	A	A

Fuente: Autor

Tabla 25. Cálculo riesgos medios

[Media] Soportes de información	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*]Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.18] Destrucción de información	P	A	A
[A.19] Divulgación de información	P	A	A
[A.25] Robo	P	A	A
[A.26]Ataque destructivo	P	A	A

Fuente: Autor

Tabla 26. Cálculo riesgos instalaciones

Activo: [OFI] Oficina	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*]Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[I.11]Emanaciones electromagnéticas	P	M	M
[E.15]Alteración accidental de la información	P	M	M
[E.18] Destrucción de información	P	M	M
[E.19]Fugas de información	P	M	M
[A.7] Uso no previsto	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	A	A
[A.18] Destrucción de información	P	M	M
[A.19] Divulgación de información	P	M	M
[A.26]Ataque destructivo	P	A	A
Activo: [BUILDING] Edificio			
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*]Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*]Desastres industriales	P	A	A
[I.7]Condiciones inadecuadas de temperatura o humedad	P	A	A
[I.11]Emanaciones electromagnéticas	P	A	A
[E.15]Alteración accidental de la información	P	A	A
[E.18] Destrucción de información	P	M	M
[E.19]Fugas de información	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11]Acceso no autorizado	P	A	A
[A.15]Modificación deliberada de la información	P	A	A
[A.18] Destrucción de información	P	M	M
[A.19] Divulgación de información	P	M	M
[A.26]Ataque destructivo	P	A	A

Fuente: Autor

Tabla 27. Cálculo riesgos personal

Activo: [ADM] Administradores de sistemas	Probabilidad	Impacto	Riesgo
[E.7] Deficiencias en la organización	N	B	B
[E.19] Fugas de información	P	M	M
[E.28] Indisponibilidad del personal	N	M	M
[A.28] Indisponibilidad del personal	P	M	M
[A.29] Extorsión	P	B	B
[A.30]Ingeniería social	P	B	B
Activo: [DBA] Administrador base de datos			
[E.7] Deficiencias en la organización	P	B	B
[E.19]Fugas de información	P	A	A
[E.28] Indisponibilidad del personal	N	A	A
[A.28] Indisponibilidad del personal	P	A	A
[A.29] Extorsión	P	B	B
[A.30]Ingeniería social	P	B	B
Activo: [DES] Desarrolladores			
[E.7] Deficiencias en la organización	P	M	M
[E.19]Fugas de información	P	A	A
[E.28] Indisponibilidad del personal	N	A	A
[A.28] Indisponibilidad del personal	P	A	A
[A.29] Extorsión	P	B	B
[A.30] Ingeniería social	P	B	B
Activo: [SOP] Soporte			
[E.7] Deficiencias en la organización	P	B	B
[E.19]Fugas de información	P	B	B
[E.28] Indisponibilidad del personal	N	A	A
[A.28] Indisponibilidad del personal	P	A	A
[A.29] Extorsión	P	B	B
[A.30] Ingeniería social	P	B	B
Activo: [CMR] Comercial			
[E.7] Deficiencias en la organización	P	B	B
[E.19]Fugas de información	P	B	B
[E.28] Indisponibilidad del personal	N	A	A
[A.28] Indisponibilidad del personal	P	A	A
[A.29] Extorsión	P	B	B
[A.30] Ingeniería social	P	B	B

	Probabilidad	Impacto	Riesgo
Activo: [UE] Usuarios externos			
[E.19] Fugas de información	P	M	M
Activo: [UI] Usuarios internos			
[E.7] Deficiencias en la organización	P	B	B
[E.19]Fugas de información	P	B	B
[E.28]Indisponibilidad del personal	N	A	A
[A.28]Indisponibilidad del personal	P	A	A
[A.29]Extorsión	P	B	B
[A.30]Ingeniería social	P	B	B

Fuente: Autor

5. ESTABLECIMIENTO DE CONTROLES DE SEGURIDAD BAJO LA NORMA ISO 27001:2013

Una vez evaluados los riesgos se sigue con la selección de los controles para mitigar o eliminar dichos riesgos. La norma ISO 27001 versión 2013 tiene dentro de sus documentos la declaración de aplicabilidad, que representa el vínculo entre la evaluación de riesgos y el tratamiento y la puesta en práctica de la seguridad de la información, la cual posee un listado de los controles que la empresa debería tener en cuenta para cumplir con el estándar.

La tabla 28 presenta los controles que se deben implementar, las últimas cuatro columnas expresan brevemente la razón para tomar el control, la descripción de estas razones es la siguiente:

RL: REQUERIMIENTO LEGAL
OC: OBLIGACIONES CONTRACTUALES
RN: REQUERIMIENTOS DEL NEGOCIO
AR: ANALISIS DE RIESGOS

Tabla 28. Declaración de aplicabilidad.

A 5. POLITICA DE SEGURIDAD								
A 5.1 Política de Seguridad de la Información								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 5.1.1	Políticas de seguridad de la información	**X**		Un documento de política de seguridad de la información ha sido aprobado por la administración.			**X**	**X**
A 5.1.2	Revisión de las políticas para seguridad de la información		**X**	Aún se encuentra en implementación.			**X**	**X**

A 6. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN								
A 6.1 Organización Interna								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 6.1.1	Roles y responsabilidades para la seguridad de la información		**X**	No todas las responsabilidades de seguridad de la información están definidas y asignadas.				**X**
A 6.1.2	Separación de deberes	**X**		No existen funciones en conflicto y las áreas de responsabilidad están separadas para reducir las posibilidades de modificación o mal uso de los activos de la empresa.				**X**
A 6.1.3	Contacto con las autoridades	**X**		Se mantienen contactos con las autoridades pertinentes.				**X**
A.6.2. Dispositivos móviles y Teletrabajo.								
A 6.2.1	Política para dispositivos móviles		**X**	Controles de seguridad serán adoptadas para gestionar los riesgos debidos al uso de dispositivos móviles.				**X**
A 6.2.2	Teletrabajo			La empresa no ha implementado el Teletrabajo.				
A 7. SEGURIDAD DE LOS RECURSOS HUMANOS								
A 7.1 Antes de asumir el empleo								
A 7.1.1	Selección	**X**		Se realiza verificación de datos sobre los candidatos para el empleo.		**X**		**X**
A 7.1.2	Términos y condiciones del empleo	**X**		Existen acuerdos contractuales con los empleados y contratistas.		**X**		**X**
A 7.2 Durante la ejecución del empleo								
A 7.2.1	Responsabilidades de la dirección	**X**		La administración exige a empleados y contratistas la aplicación de controles para la seguridad de la información.		**X**		**X**
A 7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		**X**	Aún se encuentra en implementación.		**X**		**X**
A 7.2.3	Proceso disciplinario		**X**	Falta documentar un proceso disciplinario formal.		**X**		**X**
A 7.3 Terminación y Cambio de Empleo								
A 7.3.1	Terminación o cambio de responsabilidades de empleo	**X**		Se comunican las responsabilidades de seguridad de la información y de los derechos que permanezcan válidos después de la terminación o el cambio de puesto de trabajo.		**X**		**X**

A 8. GESTIÓN DE ACTIVOS								
A 8.1 Responsabilidad por los Activos								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 8.1.1	Inventario de Activos	**X**		Se identifican los activos asociados a las instalaciones de procesamiento de la información y la información.				**X**
A 8.1.2	Propiedad de los activos	**X**		Cada activo tendrá un responsable de su seguridad y funcionamiento correcto.				**X**
A 8.1.3	Uso aceptable de los activos	**X**		Se identifican, documentan e implementan las reglas para el uso aceptable de la información y de los activos asociados.				**X**
A 8.1.4	Devolución de activos	**X**		Los empleados y usuarios externos deben devolver los activos de la empresa que se encuentren en su posesión a la terminación de su empleo, contrato o acuerdo.				**X**
A 8.2 Clasificación de la Información								
A 8.2.1	Clasificación de la información		**X**	La información se clasificará en términos de requisitos legales, valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.				**X**
A 8.2.2	Etiquetado de la información		**X**	Se elaborará un conjunto de procedimientos para el etiquetado de información y éstos se aplicarán de acuerdo con el esquema de clasificación de la información adoptado por la empresa				**X**
A 8.2.3	Manejo de activos		**X**	Se elaborarán procedimientos para el manejo de los activos de acuerdo con el esquema de clasificación de la información adoptado por la empresa.				**X**
A 8.3 Manejo de Medios								
A 8.3.1	Gestión de los medios removibles		**X**	Aún se encuentra en implementación.				**X**
A 8.3.2	Disposición de los medios		**X**	Aún se encuentra en implementación.				**X**
A 8.3.3	Transferencia de medios físicos		**X**	Aún se encuentra en implementación.				**X**

A 9. CONTROL DE ACCESO								
A 9.1 Requisitos del Negocio para el Control de Acceso								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 9.1.1	Política de control de acceso	**X**		Existe una política de control de acceso, documentada y revisada.				**X**
A 9.1.2	Acceso a redes y a servicios de red	**X**		Los usuarios sólo tienen acceso a los servicios y la red que le han sido autorizados.				**X**
A 9.2 Gestión del Acceso de Usuarios								
A 9.2.1	Registro y cancelación del registro de usuarios	**X**		Existe un proceso para el registro de usuarios y la cancelación de estos.				**X**
A 9.2.2	Suministro de acceso a usuarios	**X**		Hay un proceso para asignar y revocar derechos de acceso.				**X**
A 9.2.3	Gestión de derechos de acceso privilegiado	**X**		Se restringe la asignación de los derechos de acceso.				**X**
A 9.2.4	Gestión de información de autenticación secreta de usuarios	**X**		Existe un proceso para la asignación de la información secreta de autenticación.				**X**
A 9.2.5	Revisión de los derechos de acceso de usuarios		**X**	Los propietarios de activos deberán revisar cada cierto tiempo los derechos de acceso de los usuarios.				**X**
A 9.2.6	Retiro o ajuste de los derechos de acceso	**X**		Los derechos de acceso de empleados y usuarios externos deben ser retirados a la terminación de su empleo, contrato o acuerdo.				**X**
A 9.3 Responsabilidades de los Usuarios								
A 9.3.1	Uso de información de autenticación secreta	**X**		Los usuarios deben seguir las prácticas de la empresa en el uso de la información de autenticación secreta.				**X**
A 9.4 Control de Acceso a Sistemas y Aplicaciones								
A 9.4.1	Restricción del acceso a la información	**X**		Existen límites de acuerdo con la política de control de acceso.				**X**
A 9.4.2	Procedimiento de ingreso seguro	**X**		Existen métodos de conexión segura.				**X**
A 9.4.3	Sistema de gestión de contraseñas		**X**	No existe.				**X**
A 9.4.4	Uso de programas utilitarios privilegiados	**X**		Se restringe el uso de programas que puedan anular los controles del sistema.				**X**
9.4.5	Control de acceso al código fuente de los programas	**X**		El acceso al código fuente de los programas está restringido	**X**			**X**

A 10. CRIPTOGRAFIA								
A 10.1 Controles Criptográficos								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 10.1.1	Política sobre el uso de controles criptográficos		**X**	Se implementará una política sobre el uso de controles criptográficos para la protección de la información.				**X**
A 10.1.2	Gestión de llaves		**X**	Se implementará una política sobre el uso y protección de las claves criptográficas.				**X**
A 11. SEGURIDAD FÍSICA Y DEL ENTORNO								
A 11.1 Áreas Seguras								
A 11.1.1	Perímetro de seguridad física	**X**		Existen perímetros de seguridad para proteger las áreas que contienen información y procesamiento de la información.			**X**	**X**
A 11.1.2	Controles de acceso físicos	**X**		Existen controles de entrada.			**X**	**X**
A 11.1.3	Seguridad de oficinas, recintos e instalaciones	**X**		Existen elementos de seguridad física.			**X**	**X**
A 11.1.4	Protección contra amenazas externas y ambientales	**X**		Existen elementos de protección física.			**X**	**X**
A 11.2 Equipos								
A 11.2.1	Ubicación y protección de los equipos	**X**		Los equipos están protegidos para reducir los riesgos de las amenazas ambientales y de acceso no autorizado.				**X**
A 11.2.2	Servicios de suministro	**X**		El equipo está protegido contra fallos del suministro eléctrico y otros trastornos causados por fallas en los servicios públicos.				**X**
A 11.2.3	Seguridad del cableado	**X**		Existen elementos para proteger contra interceptación, interferencia o daños.				**X**
A 11.2.4	Mantenimiento de los equipos	**X**		Existen planes de mantenimiento de equipos para asegurar su disponibilidad e integridad.				**X**
A 11.2.5	Retiro de activos		**X**	No se ha implementado.				**X**
A 11.2.6	Seguridad de los equipos fuera de las instalaciones		**X**	No se ha implementado.				**X**
11.2.7	Disposición segura o reutilización de equipos		**X**	No se ha implementado.	**X**			**X**
11.2.8	Equipo de usuario desatendido	**X**		Existe una política para bloquear el equipo ante la ausencia de su operador.				**X**
11.2.9	Política de escritorio despejado y de pantalla despejada		**X**	No se ha implementado.				**X**

A 12. SEGURIDAD DE LAS OPERACIONES								
A 12.1 Procedimientos Operacionales y Responsabilidades								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 12.1.1	Procedimientos de operación documentados		**X**	No se ha implementado.			**X**	**X**
A 12.1.2	Gestión de cambios		**X**	No se ha implementado.			**X**	**X**
A 12.1.3	Gestión de la capacidad		**X**	No se ha implementado.			**X**	**X**
A 12.2 Protección contra Códigos Maliciosos								
A 12.2.1	Controles contra códigos maliciosos	**X**		Existen herramientas antivirus.				**X**
A 12.3 Copias de Respaldo								
A 12.3.1	Respaldo de la información	**X**		Las copias de seguridad de la información, software y del sistema son realizadas y analizadas periódicamente de acuerdo con una política de copia de seguridad establecida.				**X**
A 12.4 Registro y Seguimiento								
A 12.4.1	Registro de eventos	**X**		Se almacenan y revisan periódicamente los registros de actividades de usuarios, excepciones, errores y eventos sobre la seguridad de la información.				**X**
A 12.4.2	Registros del administrador y del operador	**X**		Las actividades del administrador y el operador del sistema deberán ser registrados y sus registros protegidos y revisados con regularidad.				**X**
A 12.4.3	Sincronización de relojes	**X**		Los relojes de todos los sistemas de procesamiento de información deben estar sincronizados a una sola fuente de tiempo.				**X**
A 12.5 Control de Software Operacional								
A 12.5.1	Instalación de software en sistemas operativos		**X**	No se ha implementado.				**X**
A 12.6 Gestión de la Vulnerabilidad Técnica								
A 12.6.1	Gestión de las vulnerabilidades técnicas		**X**	No se ha implementado.				**X**
A 12.6.2	Restricción sobre la instalación de software		**X**	No se ha implementado.				**X**
A 12.7 Consideraciones sobre Auditorias de Sistemas de Información								
A 12.7.1	Controles de auditorías de sistemas de información	**X**		Las auditorías de las actividades relacionadas con los sistemas están planificadas y acordadas para minimizar las interrupciones a los procesos de negocio.				**X**

A 13 SEGURIDAD DE LAS COMUNICACIONES								
A 13.1 Gestión de la Seguridad de las Redes								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 13.1.1	Controles de las redes	**X**		Las redes están gestionadas y controladas.				**X**
A 13.1.2	Seguridad de los servicios de red	**X**		Se identifican los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red.				**X**
A 13.1.3	Separación en las redes	**X**		Grupos de servicios de información, los usuarios y los sistemas de información estarán separados en las redes.				**X**
A 13.2 Transferencia de Información								
A 13.2.1	Políticas y procedimientos para el intercambio de información		**X**	No se ha implementado.				**X**
A 13.2.2	Acuerdos sobre transferencia de información		**X**	No se ha implementado.				**X**
A 13.2.3	Mensajería electrónica		**X**	No se ha implementado.				**X**
A 13.2.4	Acuerdos de confidencialidad o de no divulgación	**X**		Se identifican y documentan los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejan las necesidades de la empresa para la protección de la información.				**X**

A 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN								
A 14.1 Requisitos de Seguridad de los Sistemas de Información								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 14.1.1	Análisis y especificación de los requisitos de seguridad de la información		**X**	No se ha implementado.				**X**
A 14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		**X**	No se ha implementado.				**X**
A 14.1.3	Protección de transacciones de los servicios de las aplicaciones		**X**	No se ha implementado.				**X**
A 14.2 Seguridad en los Procesos de Desarrollo y Soporte								
A 14.2.1	Política de desarrollo seguro	**X**		Se establecen y aplican reglas para el desarrollo de software y sistemas dentro de la empresa.	**X**			**X**
A 14.2.2	Procedimientos de control de cambios en sistemas	**X**		Los cambios en los sistemas deben realizarse mediante el uso de procedimientos de control de cambios.	**X**			**X**
A 14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	**X**		Cuando se cambian las plataformas en funcionamiento, las aplicaciones deben revisarse para asegurar que no hay impacto adverso sobre las operaciones de la empresa.				**X**
A 14.2.4	Restricciones en los cambios a los paquetes de software	**X**		Las modificaciones necesarias a los paquetes de software se deben controlar de forma estricta				**X**
A 14.2.5	Principios de construcción de los sistemas seguros	**X**		Se establecerán principios de ingeniería para sistemas seguros, documentados.	**X**			**X**
A 14.2.6	Ambiente de desarrollo seguro	**X**		Se establecen y protegen los entornos de desarrollo.				**X**
A 14.2.7	Desarrollo contratado externamente		**X**	No se ha implementado.				**X**
A 14.2.8	Pruebas de seguridad de sistemas	**X**		Se llevan a cabo pruebas de la funcionalidad de seguridad durante el desarrollo.				**X**
A 14.2.9	Prueba de aceptación del sistema	**X**		Se establecen pruebas de aceptación para los nuevos sistemas de información.				**X**
A 14.3 Datos de prueba								
A 14.3.1	Protección de los datos de prueba del sistema	**X**		Los datos de prueba son cuidadosamente seleccionados, protegidos y controlados.				**X**

A 15. RELACIONES CON LOS PROVEEDORES								
A 15.1 Seguridad de la Información en las Relaciones con los Proveedores								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 15.1.1	Política de seguridad de la información para las relaciones con proveedores		**X**	No se ha implementado.		**X**		**X**
A 15.1.2	Cadena de suministro de tecnología de información y comunicación		**X**	No se ha implementado.		**X**		**X**
A 15.2 Gestión de la Prestación del Servicios de Proveedores								
A 15.2.1	Seguimiento y revisión de los servicios de los proveedores		**X**	No se ha implementado.		**X**		**X**
A 15.2.2	Gestión cambios en los servicios de los proveedores		**X**	No se ha implementado.		**X**		**X**
A 16. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN								
A 16.1 Gestión de los Incidentes y las mejoras en la Seguridad de la Información								
A 16.1.1	Responsabilidades y procedimientos	**X**		Se establecen las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.				**X**
A 16.1.2	Reporte sobre las debilidades en la seguridad	**X**		Se requiere que los empleados y contratistas reporten cualquier deficiencia de seguridad de información detectada o sobre sospecha.				**X**
A 16.1.3	Respuesta a incidentes de seguridad de la información	**X**		Los incidentes de seguridad de la información deberán recibir una respuesta de acuerdo con los procedimientos documentados.				**X**
A 16.1.4	Recolección de evidencias	**X**		Se definen procedimientos para la identificación, recolección y conservación de la información, que pueda servir como prueba.				**X**
A 16.1.5	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**X**		Los eventos de seguridad de la información deben ser evaluados.				**X**
A 16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**X**		El conocimiento adquirido a partir del análisis y solución de los incidentes de seguridad de la información se utilizará para reducir la probabilidad o el impacto de los incidentes en el futuro.				**X**

A 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE LA CONTINUIDAD DEL								
A 17.1 Continuidad de Seguridad de la Información								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 17.1.1	Planificación de la continuidad de la seguridad de la información	**X**		Se determina los requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas.			**X**	**X**
A 17.1.2	Implementación de la continuidad de la seguridad de la información	**X**		Se establece, documenta, implementa y mantienen procedimientos y controles para garantizar el nivel necesario de continuidad de la seguridad durante una situación adversa.			**X**	**X**
A.17.2 Redundancias								
A 17.2.1	Disponibilidad de instalaciones de procesamiento de información	**X**		Las instalaciones de procesamiento de información tendrán la redundancia suficiente para garantizar la disponibilidad.				**X**
18. CUMPLIMIENTO								
A 18.1 Cumplimiento de los Requisitos Legales y Contractuales								
A 18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	**X**		Todo lo pertinente al marco legal, los requisitos contractuales, y el enfoque de la empresa para cumplir con estos deben ser identificados, documentados y actualizados.	**X**	**X**		**X**
A 18.1.2	Derechos de propiedad intelectual (DPI)	**X**		Se aplican procedimientos para garantizar el cumplimiento de los derechos de propiedad intelectual.	**X**			**X**
A 18.1.3	Protección de registros	**X**		Se debe evitar pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.				**X**
A 18.1.4	Privacidad y protección de información de datos personales	**X**		Los datos personales deben asegurarse según la legislación.	**X**	**X**		**X**
A 18.2 Revisiones de Seguridad de la Información								
A 18.2.1	Revisión independiente de la seguridad de la información		**X**	No se ha implementado.				**X**
A 18.2.2	Cumplimiento con las políticas y las normas de seguridad	**X**		Se comprobará periódicamente el cumplimiento de las políticas de seguridad.				**X**
A 18.2.3	Revisión del cumplimiento técnico	**X**		Los sistemas de información deben revisarse regularmente para verificar el cumplimiento de las políticas y normas de seguridad de la información de la empresa.				**X**

6. POLITICAS DE SEGURIDAD

Las políticas de seguridad de la Información describen el marco para la gestión de la seguridad de la información dentro de la empresa. Definen normas, procesos y procedimientos que se aplican a todo el personal de la empresa y terceros que tienen acceso a la información y/o a los sistemas de información de la empresa.

Las políticas de seguridad de la información se aplican a todas las formas de información que incluye: Entrevistas, conversaciones, comunicaciones telefónicas o vía radio, datos impresos o escritos en papel, información almacenada en archivadores físicos, información y comunicaciones enviadas por correo, mensajería, fax, correo electrónico, almacenada y procesada a través de servidores, computadores, portátiles, teléfonos móviles, PDA, almacenados en cualquier tipo de medios extraíbles, CD, DVD, cintas, dispositivos de memoria USB, cámaras digitales.

A continuación se describen las políticas de seguridad de la información definidas por la empresa. Para su elaboración y difusión se tienen en cuenta las leyes y demás regulaciones aplicables, y son el punto de referencia para el establecimiento de los controles, procedimientos y estándares definidos.

6.1 POLITICAS DE SEGURIDAD DE LA INFORMACION

6.1.1 Autoridades y grupos de interés.

Objetivo

Contar con el apoyo de autoridades y expertos cuando se presenten incidentes de seguridad y actuar de manera correcta ante un fallo de seguridad.

Aplicabilidad

Directivos y líder área de sistemas.

Directrices

- La política de seguridad de la información deberá ser comunicada a los empleados y colaboradores externos.

- Los procedimientos para el contacto adecuado con las autoridades pertinentes deberán estar en lugar visible y de fácil acceso.

- Los procedimientos para el contacto con grupos de intereses especiales u otros foros de seguridad especializada y las asociaciones profesionales deben estar en lugar visible y de fácil acceso.

6.1.2 Seguridad de los recursos humanos.

Objetivo

Garantizar que empleados y contratistas conozcan sus responsabilidades con respecto a la seguridad informática y de la información de la empresa y eviten exponer a la empresa a amenazas y riesgos por el mal uso de los activos a su cargo.

Aplicabilidad

Directivos, empleados y contratistas.

Directrices

- Todos los candidatos a empleados de la empresa deberán presentar una verificación de antecedentes legales proporcionada por el organismo gubernamental correspondiente.

- Los requisitos de selección se aplicarán también a los contratistas.

- Los acuerdos contractuales con los empleados y contratistas deberán indicar sus responsabilidades respecto a la seguridad de la información.

- La administración deberá asegurarse de que todos los empleados y contratistas sean conscientes de las regulaciones de la empresa respecto a la seguridad de la información.

- La administración velará por que todos los empleados y contratistas reciban formación sobre la seguridad de la información.

- Se definirá un proceso disciplinario formal que se pueda aplicar a aquellos empleados o contratistas que cometan una violación a la seguridad de la información.

- Se definirán, comunicarán y se exigirán las responsabilidades de seguridad de la información y los derechos que permanecen válidos luego del cambio de empleo o la terminación de la vinculación laboral o contrato de empleados y contratistas.

6.1.3 Gestión de activos

Objetivo

Proteger apropiadamente los activos asociados a las instalaciones de procesamiento de información y de información y asegurar su uso correcto.

Aplicabilidad

Empleados y contratistas.

Directrices

- Los activos asociados a procesamiento de la información deberán ser identificados y mantenerse un inventario de éstos.

- Cada activo mantenido en el inventario deberá tener un propietario.

- Se identificarán, documentará e implementarán reglas para el uso aceptable de la información y de los activos asociados al procesamiento de información.

- Los empleados y los usuarios externos que utilicen o tengan acceso a los activos de la empresa deben ser responsables de su uso.

- Todos los empleados y usuarios externos deberán devolver todos los activos de la empresa en su posesión a la terminación de su empleo, contrato o acuerdo.

6.1.4 Clasificación de la información.

Objetivo

Asegurar que la información posea un nivel de protección de acuerdo su criticidad y sensibilidad.

Aplicabilidad

Directivos y empleados.

Directrices

- La información se clasificará de acuerdo con las reglas establecidas, cumpliendo con requisitos legales, de valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.

- La información se etiquetará de acuerdo con el esquema de clasificación de la información adoptado por la empresa. Los procedimientos para el etiquetado de información abordarán la información y sus activos, respecto a los formatos físicos y electrónicos.

- La manipulación de los bienes se hará de acuerdo con el esquema de clasificación de la información adoptado por la empresa.

6.1.5 Manejo de los soportes.

Objetivo

Garantizar la confidencialidad de la información contenida en medios extraíbles.

Aplicabilidad

Área de sistemas y demás empleados.

Directrices

- Los medios extraíbles se gestionarán de acuerdo con el esquema de clasificación adoptado por la empresa.

- Los medios de comunicación deberán ser desechados de forma segura cuando ya no sean necesarios, utilizando procedimientos formales.

- Los medios que contienen información deberán estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante el transporte.

6.1.6 Control de acceso.

Objetivo

Controlar el acceso de los usuarios a la información que requieren para cumplir sus funciones dentro de la empresa.

Aplicabilidad

Área de sistemas.

Directrices

- Se establecerán reglas de control de acceso, derechos y restricciones de acceso adecuados, documentados y revisados en base a los requisitos de seguridad y de información de la empresa.

- Los usuarios sólo deberán disponer de acceso a los servicios de red y de la red a los cuales han sido específicamente autorizados.

- Existirá un proceso formal para el registro y cancelación de derechos de acceso a los usuarios a todos los sistemas y servicios que pertenecen a la empresa.

- La asignación y utilización de derechos de acceso privilegiados estarán restringidas y controladas.

- Se debe controlar la asignación de información secreta de autenticación.

- Los propietarios de activos deberán revisar los derechos de acceso de los usuarios con cierta regularidad.

- Los derechos de acceso de todos los empleados y usuarios externos a las instalaciones de procesamiento de información deberán ser retirados después de la terminación de su empleo, contrato o acuerdo, o cuando haya cambio de funciones o roles.

- Los usuarios estarán obligados a seguir las prácticas de la empresa en el uso de la información de autenticación secreta.

- El acceso a los sistemas de información y aplicaciones estará restringido.

- El acceso a los sistemas de información y aplicaciones se controla mediante un procedimiento de conexión segura cuando sea necesario.

- Los sistemas de gestión de contraseñas deberán ser interactivos y deberán asegurar contraseñas de calidad.
- El uso de programas que puedan ser capaces de anular los controles del sistema y de las aplicaciones será restringido y estrechamente controlado.

- El acceso a los códigos fuente de los programas se limitará y estará bajo el control del departamento de desarrollo.

- Al usar dispositivos móviles, se debe tener cuidado especial para asegurar que la información no se vea comprometida.

- Los empleados pueden utilizar sus dispositivos móviles privados en el ambiente de trabajo, pero no pueden acceder a la información empresarial.

- Actividades de teletrabajo no están permitidas por la empresa.

6.1.7 Controles criptográficos.

Objetivo

Utilizar herramientas criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información.

Aplicabilidad

Área de sistemas.

Directrices

- Se desarrollarán e implementarán principios sobre el uso de controles criptográficos para la protección de la información.

- Se desarrollarán e implementarán procesos para el uso, la protección y la duración de las claves criptográficas.

6.1.8 Seguridad física y ambiental.

Objetivo

Evitar el acceso no autorizado a las instalaciones de procesamiento de información y mitigar los daños que por razones accidentales comprometan los activos de información y las personas.

Aplicabilidad

Área de sistemas.

Directrices

- Se definirán y utilizarán perímetros de seguridad para proteger las instalaciones de procesamiento de información, ya sea sensible o crítica como se defina en el manual de seguridad.

- Las áreas seguras estarán protegidos por controles de entrada adecuados para garantizar que sólo el personal autorizado se le permite el acceso.

- La seguridad física para oficinas, salas e instalaciones deberá estar diseñada y aplicada como se defina en el manual de seguridad.
- La protección física contra los desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada como se defina en el manual de seguridad.

- Se debe controlar el acceso a las oficinas administrativas donde personas no autorizadas podrían entrar y, si es posible, deberán estar aisladas de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

- Los equipos deberán estar bien dispuestos y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.

- Los equipos deberán estar protegidos contra fallos de alimentación eléctrica y otros trastornos causados por fallas en el apoyo a los servicios públicos.

- El cableado de electricidad y telecomunicaciones que transporta datos o soporta los servicios de información deberá estar protegido contra la interceptación, interferencia o daños.

- Los equipos deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.

- Los equipos, información o software no serán extraídos de las instalaciones de la empresa sin autorización previa.

- Antes de su eliminación o reutilización todos los elementos o medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y software con licencia han sido eliminados o sobrescritos de forma segura.

- Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada para evitar su acceso no autorizado.

- Se adoptará una política de escritorio limpio para los papeles y medios de almacenamiento extraíbles y una política de pantalla bloqueada para las instalaciones de procesamiento de información.

6.1.9 Operaciones de seguridad.

Objetivo

Gestionar de forma adecuada la seguridad en los sistemas en operación.

Aplicabilidad

Área de sistemas y empleados.

Directrices

- Los procedimientos de operación deberán ser documentados y puestos a disposición de todos los usuarios que lo necesiten. Los cambios en la empresa, los procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados.

- El uso de los recursos será supervisado, se ajustará y proyectará a las futuras necesidades de capacidad para asegurar el rendimiento óptimo del sistema requerido.

- Se separarán los entornos de desarrollo, pruebas y producción para reducir los riesgos de acceso o cambios no autorizados al entorno de producción.

6.1.10 Protección contra software malicioso o malware.

Objetivo

Proteger la integridad y disponibilidad de los sistemas informáticos y la información.

Aplicabilidad

Área de sistemas y empleados.

Directrices

- Se aplicarán controles para la detección y prevención de software malicioso, y para la recuperación ante un incidente provocado por software malicioso, combinados con el conocimiento y conciencia de la seguridad de la información por parte de los usuarios.

6.1.11 Copias de seguridad.

Objetivo

Garantizar la integridad y disponibilidad de la información contando con medidas de recuperación efectivas ante cualquier incidente.

Aplicabilidad

Área de sistemas.

Directrices

- Las copias de seguridad de la información, software y del sistema serán tomadas y analizadas con regularidad.

- El número de copias de seguridad, el número de lugares seguros para su almacenamiento y el personal responsable están sujetos a la aprobación de la administración.

6.1.12 Registro y supervisión de actividades.

Objetivo

Asegurar la trazabilidad de las operaciones realizadas por los usuarios y evitar el repudio de sus acciones.

Aplicabilidad

Área de sistemas.

Directrices

- Los registros de actividades de usuario, excepciones, errores y eventos de seguridad de la información se almacenarán y revisarán con regularidad.
- El registro de instalaciones e información estará protegido contra la manipulación y acceso no autorizado.
- Las actividades de los administradores del sistema deberán ser registrados y sus registros protegidos y revisados con regularidad.
- Los relojes de todos los sistemas de procesamiento de información o dominio de seguridad deberán estar sincronizados a una sola fuente de tiempo de referencia.

6.1.13 Control del software operacional.

Objetivo

Garantizar la disponibilidad de los sistemas previendo fallos debidos a mal funcionamiento o falta de mantenimiento.

Aplicabilidad

Área de sistemas.

Directrices

- Se debe controlar la instalación de software en los sistemas operativos. No se permite software ajeno al negocio sin autorización.

- Se mantendrán bitácoras sobre el mantenimiento y actualización de las aplicaciones en uso dentro de la empresa.

6.1.14 Gestión de las vulnerabilidades técnicas.

Objetivo

Documentar de forma adecuada los riesgos que afectan a los sistemas y estandarizar la instalación de software.

Aplicabilidad

Área de sistemas.

Directrices

- Se obtendrá en el momento oportuno, información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan en la empresa, se debe evaluar la exposición de la empresa a tales vulnerabilidades y tomarse medidas adecuadas para hacer frente a los riesgos asociados.

- Se establecerán y aplicarán normas que rigen la instalación de software de los usuarios.

6.1.15 Consideraciones de auditoría de sistemas de información.

Objetivo

Minimizar las interferencias a los sistemas de información durante los procesos de auditoria.

Aplicabilidad

Directivos y área de sistemas.

Directrices

- Los requisitos y las actividades relacionadas con la verificación y auditoria de los sistemas de información deberán ser cuidadosamente planificadas y acordadas para minimizar las interrupciones a los procesos de negocio.

6.1.16 Seguridad de las comunicaciones y redes.

Objetivo

Garantizar la protección de la información en tránsito y la infraestructura de redes de la empresa.

Aplicabilidad

Área de sistemas.

Directrices

- Las redes deberán ser gestionadas y controladas para proteger la información de los sistemas y aplicaciones. Se identificarán los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red y se incluirán en los acuerdos de servicios de red, si estos servicios son subcontratados.

- Debe existir separación de redes, de acuerdo a los servicios y usuarios que las usen.

- Los dispositivos no autorizados no se pueden conectar a la red de la empresa, se tomarán las precauciones necesarias para evitar que esto suceda.

- Cualquier dispositivo que esté conectado a la red de la empresa no puede salir de las instalaciones de la empresa sin pasar por un proceso de limpieza. Sólo después de la aprobación del personal de seguridad de la información que verifique que el dispositivo no incluye ningún dato sensible para la empresa, éste podrá salir de las instalaciones.

- Para cualquier comunicación dentro de la empresa se deben usar los medios expresamente autorizados para ello, y estos no deben ser usados con otros fines ajenos a la empresa.

6.1.17 Transferencia de información.

Objetivo

Asegurar la confidencialidad de la información transferida dentro y fuera de la empresa.

Aplicabilidad

Área de sistemas y empleados.

Directrices

- Deben existir procedimientos y controles sobre la transferencia de información, y verificar su correcto funcionamiento para proteger la información en tránsito en todo tipo de medios de comunicación.

- Los contratos contarán con cláusulas expresas sobre la transferencia segura de información entre la empresa y terceros.

- La información involucrada en la mensajería electrónica deberá estar protegida adecuadamente.

- Se revisarán y documentarán con regularidad los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejan las necesidades de la empresa para la protección de la información.

- Toda información que utilice los canales propios de la empresa para su transferencia es propiedad de la empresa, y está sujeta a procesos de auditoria por parte de los encargados de la seguridad de la información cuando así se requiera.

6.1.18 Adquisición, desarrollo y mantenimiento de sistemas.

Objetivo

Garantizar que la seguridad es parte integral de los sistemas de información y que está deberá verificarse durante todo el ciclo de vida de las aplicaciones, además de minimizar los riesgos por fallos.

Aplicabilidad

Área de sistemas.

Directrices

- Los requisitos relacionados con la seguridad de la información se incluirán en los requerimientos para los nuevos sistemas de información y en las actualizaciones y mejoras a los ya existentes.

- La información que requiera servicios de aplicaciones que pasan a través de redes públicas deberá estar protegida contra la actividad fraudulenta, disputa contractual, y la divulgación y modificación no autorizada.

- La Información involucrada en las transacciones de servicios de aplicación debe ser protegida para evitar la transmisión incompleta, falso enrutamiento, alteración no autorizada, divulgación no autorizada, duplicación no autorizada o todo aquello que ponga en riesgo la integridad y la confidencialidad de la información.

- Se establecerán y aplicarán reglas para el desarrollo de software y sistemas de acuerdo a la evolución de la empresa.

- Los cambios en los sistemas dentro del ciclo de desarrollo deberán realizarse mediante el uso de procedimientos formales de control de cambios.

- Si no hay un compromiso contractual, se requerirá de la aprobación de la administración para todo tipo de liberación de código fuente que salga de la empresa.

- Cuando se cambien las plataformas que estén en operación, las aplicaciones críticas de negocios deben ser revisadas y probadas para asegurar que no hay impacto adverso sobre las operaciones o la seguridad

de la empresa. Las modificaciones necesarias a las aplicaciones software se deben controlar de forma estricta.

- Se establecerán principios de ingeniería para sistemas seguros, éstos se deben documentar y aplicar a los esfuerzos de implementación de cualquier sistema de información.

- Se establecerán entornos seguros de desarrollo que cubran todo el ciclo de vida de desarrollo del sistema, y deberán estar protegidos debidamente.

- La empresa debe supervisar y controlar la actividad de desarrollo del sistema de contratación externa. Se llevarán a cabo pruebas de la funcionalidad de seguridad durante el desarrollo.

- Se establecerán programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.

- Los datos de prueba deben seleccionarse, protegerse y controlarse cuidadosamente.

- Se establecerán procedimientos para ofuscar la información real que se use en pruebas.

6.1.19 Relaciones con proveedores y prestadores de servicios.

Objetivo

Mantener un nivel adecuado de seguridad de la información y de prestación de servicios por parte de terceros.

Aplicabilidad

Directivos.

Directrices

- Se acordaran y documentaran con el proveedor los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la empresa.

- Todos los requisitos pertinentes de seguridad de la información serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TI de la empresa.

- Los acuerdos con proveedores incluirán los requisitos para hacer frente a los riesgos de seguridad asociados con la información de los servicios de tecnologías de la información y las comunicaciones y la cadena de suministro de productos.

- Se deberá controlar, revisar y auditar regularmente a los proveedores de prestación de servicios.

- Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora, serán controlados, teniendo en cuenta la criticidad de la información, los sistemas y los procesos involucrados y la reevaluación de los riesgos.

6.1.20 Gestión de incidentes de seguridad información.

Objetivo

Garantizar que las vulnerabilidades y los eventos que comprometan la seguridad de la información se comunican y corrigen efectiva y oportunamente.

Aplicabilidad

Área de sistemas.

Directrices

- Se establecerán las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- Los eventos de seguridad de la información deben ser reportados por el medio adecuado tan pronto como sea posible.

- Se requiere que los empleados y contratistas que utilizan sistemas y servicios de información de la empresa reporten cualquier deficiencia de seguridad de información detectada o sobre la que se tenga alguna sospecha.

- Los eventos de seguridad de la información deben ser evaluados y se debe decidir si han de ser clasificados como incidentes de seguridad de la información.

- Los incidentes de seguridad de la información deberán recibir una respuesta de acuerdo con los procedimientos documentados.

- El conocimiento obtenido a partir del análisis y la resolución de los incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.

- La empresa debería definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como prueba.

6.1.21 Aspectos de seguridad de información para la continuidad del negocio.

Objetivo

Tomar medidas para contrarrestar las interrupciones a los procesos de negocio y garantizar su oportuna puesta en marcha durante un evento adverso.

Aplicabilidad

Directivos y área de sistemas.

Directrices

- Los requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información serán determinados para seguir en operación durante situaciones de riesgo.

- Se establecerán procesos, procedimientos y controles, documentados, implementados y mantenidos para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación de riesgo.

- Los controles establecidos y aplicados para garantizar la continuidad de seguridad de la información serán verificados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones de riesgo.

6.1.22 Sistemas redundantes.

Objetivo

Asegurar la disponibilidad de la información.

Aplicabilidad

Directivos y área de sistemas.

Directrices

- Las instalaciones de procesamiento de información tendrán la redundancia suficiente para satisfacer los requisitos de disponibilidad.

6.1.23 Cumplimiento de los requisitos legales y contractuales.

Objetivo

Evitar infringir obligaciones legales, reglamentarias o contractuales sobre cualquier requisito de seguridad.

Aplicabilidad

Directivos.

Directrices

- Todo lo pertinente a lo legal, requisitos contractuales y normas regulatorios deberán ser identificados de forma explícita, documentados y actualizados a partir de cada sistema de información.

- Se aplicarán los procedimientos adecuados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario.
- Los registros deben ser protegidos de pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, de conformidad con los requisitos legales, regulatorios y contractuales.

- La privacidad y protección de los datos personales deberán estar aseguradas como se requiere en la legislación y regulación relevante en su caso.

- Los controles criptográficos serán utilizados en el cumplimiento de todos los acuerdos, leyes y reglamentos pertinentes.

- Toda la normativa de propiedad intelectual para proteger los productos de la empresa serán gestionados de acuerdo a la política de propiedad intelectual.

- El enfoque a la gestión de seguridad de la información y su aplicación serán revisadas de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

- Los administradores de cada área deberán comprobar periódicamente el cumplimiento del tratamiento y los procedimientos de información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.

- Los sistemas de información deben ser revisados regularmente para verificar el cumplimiento de las políticas y normas de seguridad de la empresa.

7. PROCESO DE IMPLEMENTACIÒN DEL SISTEMA DE GESTION DE LA INFORMACIÓN BAJO LA NORMA ISO 27001:2013

En esta fase se ponen de manifiesto los requisitos necesarios para que la empresa implemente el SGSI, esto incluye la documentación requerida por la norma ISO 27001. La empresa puede elaborar otros documentos y adicionarlos a los exigidos por la norma. Los documentos obligatorios según la norma son:

- Alcance del SGSI
- Políticas y objetivos de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento del riesgo
- Informe de evaluación de riesgos
- Definición de funciones y responsabilidades de seguridad
- Inventario de activos
- Uso aceptable de los activos
- Política de control de acceso
- Procedimientos operativos para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad para proveedores
- Procedimiento para gestión de incidentes
- Procedimientos de la continuidad del negocio
- Requisitos legales, normativos y contractuales

7.1 DOCUMENTOS

Algunos de estos documentos ya han sido desarrollados en la fase de planeación, otros son abarcados por las políticas de seguridad definidas anteriormente. El diseño del sistema de gestión de la seguridad informática según la norma ISO 27001:2013 exige que la empresa aborde la construcción de los documentos descritos a continuación.

7.1.1 Plan de tratamiento del riesgo

En el plan de tratamiento del riesgo se especifican los controles de seguridad que se necesitan poner en práctica, el responsable de estos controles, cuáles son los

plazos, y qué recursos, financieros y humanos, se requieren. Para ello es importante contar la declaración de aplicabilidad, que ofrece un punto de referencia para conocer donde se necesitan los controles. El plan ofrece las opciones de tratamiento del riesgo, como pueden ser:

- Mitigar: Adoptar controles que reduzcan el impacto del riesgo a niveles aceptables para la empresa.
- Transferir: Contratar pólizas de seguro que asuman las perdidas.
- Aceptar: Establecer los controles puede ser más costoso que el impacto del riesgo.

Luego de la elaboración del documento se debe revisar el registro de riesgos detectados y evaluar sus probabilidades e impacto, para obtener el riesgo residual y presentar el informe de evaluación de riesgos revisado.

7.1.2 Definición de funciones y responsabilidades de seguridad

Debido al tamaño de la empresa En Línea Financiera, no es necesario tener una estructura muy compleja para las funciones y responsabilidades de seguridad, como en muchas empresas pequeñas varias funciones pueden ser llevadas a cabo por la misma persona. Sin embargo, la administración debe identificar explícitamente el papel del oficial de seguridad, el cual tendrá la responsabilidad general de la gestión de la seguridad de la información, y para el resto del personal deben asignarse roles y responsabilidades teniendo en cuenta las habilidades necesarias para realizar el trabajo. Esto es necesario para garantizar que las tareas se llevan a cabo de manera eficiente y efectiva.

Las consideraciones más importantes para la definición de los roles en la gestión de seguridad de la información para la empresa En Línea Financiera son:

- La administración debe mantener la responsabilidad general de las tareas.
- El oficial de seguridad será el responsable de promover y coordinar el proceso de seguridad de la información.
- Cada empleado es responsable de las tareas asignadas y mantener la seguridad de la información en el lugar de trabajo.

7.1.3 Procedimientos operativos para gestión de TI

La según lo detectado en la empresa se requieren documentar los procedimientos referentes a la gestión del cambio de su aplicación, servicios prestados por terceros como internet y datacenter, copias de seguridad de sus sistemas de información y sus desarrollos, seguridad de su red, disposición y destrucción de equipos de cómputo, transferencia de información con sus asociados y monitoreo de las actividades en sus sistemas de información.

7.1.4 Principios de ingeniería para sistema seguro

La empresa debe seleccionar y documentar una metodología de desarrollo que aplique en todo el ciclo de vida de sus proyectos que permita evaluar la seguridad de la información, y cumplir con los requisitos exigidos, así como los mecanismos de actualización para las aplicaciones existentes que adopten los requisitos de seguridad de la información de la empresa según las políticas establecidas.

7.1.5 Procedimiento para gestión de incidentes

La empresa debe garantizar que posee los mecanismos necesarios gestionar los incidentes o eventos adversos que pueden afectar los servicios. Este documento debe definir al menos los siguientes procesos:

Apoyo a la gestión de incidentes: necesario para proporcionar y mantener los recursos para la gestión de incidentes.

El registro de incidentes y clasificación: registrar y asignar niveles de prioridad a los incidentes facilita su solución de forma rápida y eficaz.

Resolución de incidentes: resolver los incidentes dentro del tiempo acordado, teniendo en cuenta soluciones alternativas, los niveles de soporte y la prioridad del incidente.

Seguimiento de incidentes: para monitorear continuamente el estado del trámite de los incidentes, lo que garantiza el despliegue a tiempo de medidas adecuadas si los niveles de servicio se ven comprometidos.

Cierre del incidente y evaluación: garantiza la solución definitiva de los incidentes y su registro para su uso futuro en caso de otra eventualidad.

Informar al usuario: los usuarios deben ser informados utilizando un medio eficaz que existen fallas en el servicio, y que ya se están abordando las soluciones pertinentes, esto evitará que el personal se vea abrumado por consultas de los usuarios e impidan una solución rápida.

Reportes sobre la gestión de incidentes: para proporcionar información relacionada con el incidente y proponer mejoras basadas en incidentes del pasado.

7.1.6 Procedimientos de la continuidad del negocio

La empresa documentará los procedimientos que se implementen para responder y restaurar el funcionamiento de sus servicios luego de una interrupción. El documento debería contener:

- Propósito, alcance y usuarios.
- Roles y responsabilidades.
- Datos de contactos de las personas que participarán en la ejecución del plan.
- Determinar las condiciones de la activación y desactivación del plan.
- Comunicación.
- Respuesta a incidentes.
- Sitios físicos de reubicación y medios de transporte.
- Plan y orden de recuperación para las actividades.
- Recursos necesarios.

7.1.7 Requisitos legales, normativos y contractuales

Es importante tener una lista con todos los requisitos legales, normativos y contractuales, los interesados y las personas responsables de cumplir con los requisitos. Es un deber de la empresa conocer sus obligaciones legales con respecto a la seguridad de la información, documentar y divulgar estas obligaciones a los responsables dentro de la empresa.

RECOMENDACIONES

La administración debe iniciar desde ya la implementación del SGSI, durante el desarrollo del proyecto se detectó el desconocimiento de mínimas normas de seguridad, los empleados no conocen herramientas o controles que pueden implementar para asegurar sus activos, se requiere una capacitación extensiva que permita a los empleados tomar conciencia y facilite el proceso de adopción de la norma.

Falta una mejor relación en cuanto a temas de seguridad con los proveedores, no existen mecanismos de verificación al cumplimiento por parte de ellos de controles de seguridad.

La recomendación más importante es que la administración de la empresa continúe con su apoyo al proceso de adopción de la norma ISO 27001:2013, ya que este factor se considera, según estudios publicados, como el más determinante para el éxito o fracaso en la implementación de un SGSI. De igual forma la administración deberá definir roles más precisos para afrontar la implementación del SGSI y crear medios para mantener la motivación de sus empleados, así como iniciar procesos de capacitación en seguridad informática y de la información, ya que se notó durante el desarrollo del proyecto que sus empleados carecen de conocimientos básicos sobre los temas.

CONCLUSIONES

El proyecto presenta el diseño de un sistema de gestión de la seguridad bajo la norma ISO 27001 para la empresa En Línea Financiera de la ciudad de Cali y proporciona directrices para que la empresa lo implemente. Durante la investigación se detectaron los desafíos y obstáculos que afronta cualquier empresa para cubrir a satisfacción sus necesidades en seguridad informática y de la información, pero de igual forma se adquiere conciencia sobre los beneficios que podrían obtener de la aplicación de tal estándar.

En este proyecto, se ha tratado de arrojar alguna luz sobre los tipos de motivaciones y los resultados que las empresas deben tratar a lo largo de las fases del diseño de un SGSI. Se coincide en que la identificación de los activos de la empresa y la valoración de los riesgos sobre ellos fue una de las tareas más complejas y demandantes, quizás uno de los aspecto que influyó fue la falta de experiencia del equipo.

Mejorar el nivel de seguridad de la empresa y la obtención de ventajas competitivas fueron los factores de motivación más reportados. La administración de la empresa expresó su satisfacción por los resultados, se revitaliza su compromiso para fortalecer sus prácticas de seguridad de la información. El siguiente paso es implementar el SGSI y continuar con el proceso iniciado en este proyecto y en el futuro buscar la certificación por un ente competente.

Por último gracias al desarrollo del proyecto la empresa identifica la información como su activo más importante y como un factor determinante para lograr sus objetivos y garantizar la continuidad en el negocio, por lo tanto considera necesario establecer un marco para asegurar la información de una manera adecuada sin importar la forma o medio en la que ésta sea almacenada, gestionada o transportada.

BIBLIOGRAFÍA

BENAVIDES RUANO, Mirian del Carmen. SOLARTE SOLARTE, Francisco. Módulo riesgos y control informático. Universidad Nacional Abierta y a Distancia. Pasto, Colombia febrero de 2012.

CARVAJAL, Armando. Análisis y gestión de riesgos, base fundamental del SGSI. Bogotá, Colombia (s.f).

GARAVITO ROBLES, Hina. Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, Enfocado en un Sistema de Seguridad de la Información. Bogotá, 2015,108 p. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. Universidad Nacional Abierta y a Distancia.

GUZMÁN GARCÍA, Alexánder. TABORDA BEDOYA, Carlos. Diseño de un Sistema de Gestión de la Seguridad Informática– SGSI–, para Empresas del Área Textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la Auditoría. Bogotá, 2015,311 p. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. Universidad Nacional Abierta y a Distancia.

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

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. Madrid, España octubre de 2012.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de técnicas. Madrid, España octubre de 2012.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información. Bogotá, Colombia (s.f).

ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN ISO. Estándar internacional ISO/IEC 27001. Primera edición 2005.

SUAREZ SIERRA, Lorena. SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI. Universidad Nacional Abierta y a Distancia. Bogotá, Colombia julio de 2013.

WEBGRAFIA

Conceptos y definiciones. Disponible en Internet: < http://conceptodefinicion.de>

CONGRESO DE LA REPUBLICA DE COLOMBIA. 2009. Ley 1273 de 2009. Disponible en Internet: <http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>

Comunidad internacional de implantadores de ISO27000. “Consejos de implantación y métricas de ISO/IEC 27001 y 27002”. Disponible en Internet: <http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf>

GALDÁMEZ, Pablo. Seguridad informática. Disponible en Internet: <http://web.iti.upv.es/>

GANDIN, Isabella. Ley de Delitos Informáticos en Colombia. Disponible en Internet: <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>.

ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación). Documento Norma Técnica Colombiana NTC 1486. Disponible en Internet: <http://datateca.unad.edu.co/contenidos/356025/NTC1486.pdf>

MIERES, Jorge. Fundamentos sobre Seguridad de la Información. Disponible en internet:< http://www.segu-info.com.ar/terceros/>

REMOLINA, Nestor. El habeas data en Colombia. Disponible en Internet:<https://habeasdatacolombia.uniandes.edu.co/ >

SEGOVIA, Antonio. ISO 27001. Resumen del proceso de implementación del SGSI. Disponible en Internet: <http://www.advisera.com>

Sistema de gestión de la seguridad de la información. Disponible en Internet:<http://www.iso27000.es/>

Sistema de gestión de seguridad de la seguridad de la información, ISO 27001. Disponible en Internet: < http://www.ceeisec.com/nuevaweb/>

Universidad Politécnica de Madrid de España. Information Security enciclopedia - Intypedia. Enciclopedia de la Seguridad de la Información. Disponible en Internet: <http://www.intypedia.com/>