ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001"

TESIS DE GRADO

Previa a la obtención del Título de:

LICENCIADO EN SISTEMAS DE INFORMACIÓN

Presentado por:

Diana Elizabeth Tola Franco

Guayaquil - Ecuador

2015

AGRADECIMIENTO

Agradezco a Dios por ser uno de los pilares fundamentales en mi vida y permitirme llegar hasta donde estoy, a mi madre por brindarme su apoyo incondicional y no permitir que me rinda ante ninguna dificultad, a mi padre por sus consejos, a mis hermanos por sus palabras de aliento y a mis amigos que de una u otra forma me ayudaron a lograr culminar este proyecto. Solo me queda decir, misión cumplida.

Diana Tola Franco

DEDICATORIA

Dedico este trabajo a Dios por darme la fortaleza y tenacidad para terminar este proyecto, a mis padres y hermanos que con sus consejos han formado la persona que soy y en especial a mi madre por su amor, dedicación y constante cooperación.

Diana Tola Franco

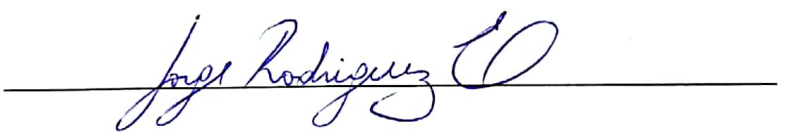
TRIBUNAL DE SUSTENTACIÓN

Ing. Lenín Freire

DIRECTOR DE TESIS

Dr. Sixto Garcia Aguilar

PRESIDENTE DEL TRIBUNAL

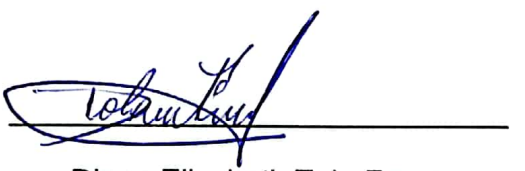


Ing. Jorge Rodríguez

VOCAL PRINCIPAL DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado me corresponde exclusivamente, y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"



Diana Elizabeth Tola Franco

RESUMEN

En el proyecto de titulación se pretende dar una adecuada solución de seguridad a la empresa A&CGroup S.A., la cual consiste en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como base el estándar ISO 27001:2005.

El primer capítulo, el marco teórico, se refiere a revisar los conceptos básicos que van a permitir tener una visión clara del conjunto de acciones necesarias para que la entidad involucrada pueda contar con un sistema para la seguridad y gestión de riesgos de la información. Por otra parte, en el segundo capítulo se presentan los antecedentes del proyecto, en donde se describirá el problema, la solución propuesta, el objetivo general y los objetivos específicos.

En el tercer capítulo, se detalla el levantamiento de información necesario para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información). El cuarto capítulo trata sobre la metodología PDCA (Plan – Do – Check - Act) y los conceptos por cada una de las etapas implicadas en el modelo. Se detalla el

alcance que se desea establecer, indicando los lineamientos y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información dentro de la empresa; continuando con una breve descripción de las políticas generales que se deben aplicar.

El quinto capítulo describe la metodología para la gestión del riesgo con el concepto y ventajas principales de su implementación, se detalla el inventario de activos de información dentro de la organización y se especifica el análisis de riesgo con sus apropiados criterios de valoración; de igual manera se realiza la evaluación del riesgo dentro del cual se procede a describir la metodología para calcular los valores de riesgo y la selección de las estrategias para el tratamiento de los mismos.

El desarrollo del sexto capítulo se centra en la explicación de la implementación de las políticas y el plan de tratamiento a utilizar para la debida gestión de riesgos que se encontraron. Por último, en el séptimo capítulo se muestra el análisis de los resultados obtenidos y las estrategias de difusión aplicadas en la empresa. Se presentan las conclusiones y recomendaciones, así como los anexos del trabajo realizado.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En los últimos años, con el desarrollo de las tecnologías de información y su relación directa con los objetivos de las organizaciones, el universo de amenazas y vulnerabilidades crece, por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando siempre la disponibilidad, confidencialidad e integridad de la misma.

Debido a que actualmente existen diversos escenarios de amenazas, tales como: la fuga de información o un ataque de ingeniería social, que en cualquier momento pueden manifestarse, con el fin de obtener información confidencial y hacer colapsar a la empresa; es necesario que el negocio cuente con una estrategia de continuidad de negocio, claramente definida por cada escenario de amenaza identificado para así poder reanudar las operaciones rápidamente.

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos.

El presente proyecto de titulación reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2005, para asegurar la protección de los activos de información y otorgar confianza a los clientes de A&CGroup S.A. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

CAPÍTULO 1

MARCO TEÓRICO

1.1 ISO

De acuerdo al archivo consultado [1], la Organización Internacional de Normalización (ISO), es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países, uno por cada país.

La ISO es una organización no gubernamental, establecida en 1947 cuya misión es promover el desarrollo de la estandarización y las actividades relacionadas, con el

fin de facilitar el intercambio de servicios y bienes y promover la cooperación en la esfera de lo con Tlintelectual, científico, tecnológico y económico.

Todos los trabajos realizados por la ISO resultan en acuerdos internacionales, los cuales son publicados como Estándares Internacionales.

1.2 ESTÁNDAR

Según el archivo consultado [2], un estándar es una publicación que recoge el trabajo en común de los comités de fabricantes, usuario, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productores, vendedores, compradores, usuarios y reguladores).

En principio, son de uso voluntario, aunque la legislación y las reglamentaciones nacionales pueden hacer referencia a ellos.

1.3 ISO 27001

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como: BS 5750 publicada en 1979, origen de ISO 9001; BS 7750 publicada en 1992, origen de ISO 14001. La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas

ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Esta norma, está constituida por 8 cláusulas y Anexos, de los cuales la parte principal del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas, los mismos que se encuentran distribuidos en 11 dominios que son: A.5 Política de seguridad, A.6 Organización de la seguridad de la información, A.7 Gestión de activos, A.8 Seguridad de los recursos humanos, A.9 Seguridad física y ambiental, A.10 Gestión de las comunicaciones y operaciones, A.11 Control de acceso, A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información, A.13 Gestión de incidentes en seguridad de la información, A.14 Gestión de la continuidad del negocio y A.15 Cumplimiento.

Por lo tanto, ISO 27001, es un estándar que proporciona un modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (del inglés Plan-Do-Check-Act, cuyo significado en español es Planear, Hacer, Verificar y Actuar; o ciclo de Deming) de mejora continua, al igual que otros sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

1.4 SEGURIDAD DE LA INFORMACIÓN

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Entendiéndose por confidencialidad a la propiedad que impide la divulgación de información a personas o sistemas no autorizados, es decir asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización; así mismo, cuando nos referimos a integridad, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, es decir trata de mantener la información tal cual fue generada y al hablar de disponibilidad, nos referimos a la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

CAPÍTULO 2

ANTECEDENTES

2.1 DESCRIPCIÓN DEL PROBLEMA

En los últimos años, el uso de las tecnologías de la información dentro de las organizaciones ha ido aumentando rápidamente, ya que nos ayudan a optimizar y mejorar las actividades de cada proceso de negocio convirtiéndose en una herramienta valiosa. Así mismo la continua evolución de la tecnología, indudablemente representa una fuente de posibles riesgos para las compañías.

Con el uso de estas tecnologías, dentro de las organizaciones, con el fin de almacenar, mantener, transmitir y recuperar información, se ha logrado que también crezca considerablemente la variedad de amenazas que podrían afectar la

confidencialidad, integridad y disponibilidad de los activos de información, provocando graves afectaciones ya sean de tipo financiero, operacional y de reputación en las empresas.

En la actualidad uno de los activos más importantes que poseen las organizaciones, es la información, sin embargo en muchas ocasiones éstas no cuentan con políticas adecuadas para protegerla, generando vulnerabilidades que pueden ser aprovechadas por las amenazas existentes en el entorno y dar como resultado riesgos y por ende las afectaciones antes descritas. El comportamiento observado en las organizaciones ante esta situación mayormente es reactivo, es decir actúan luego de que el incidente de seguridad ha ocurrido.

2.2 SOLUCIÓN PROPUESTA

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos, sobre todo para las empresas dedicadas a la auditoría financiera, como es el caso de A&CGroup S.A., que maneja información sensible de cada uno de sus clientes y por tanto es de vital importancia tener protegida dicha información.

Dada esa premisa, el presente proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de la Seguridad de la Información, basado en la norma ISO 27001:2005, para así garantizar la protección de los activos de información y otorgar confianza a cualquiera de las partes interesadas, sobre todo a los clientes.

La correcta implementación de un SGSI dentro de las empresas, ayudará a prevenir incidentes de seguridad, que generan pérdidas económicas e interrupciones en la continuidad del negocio, mediante la reducción de las probabilidades o impactos que los riesgos identificados pudieran ocasionar a su información.

2.3 OBJETIVO GENERAL

Lograr la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa A&CGroup S.A.

2.4 OBJETIVOS ESPECÍFICOS

1. Definir el alcance, objetivos y políticas del SGSI.
2. Identificar los riesgos sobre los activos definidos en el alcance del SGSI.
3. Analizar las probabilidades e impactos de los riesgos sobre los activos identificados bajo el alcance y calcular los niveles de riesgo, aplicando la metodología MAGERIT.
4. Implementar controles sobre los activos, basado en un plan de tratamiento de riesgo.
5. Asegurar la creación de procedimientos para el monitoreo y revisión del sistema, que cubra: incidentes de seguridad, auditorías internas y revisiones gerenciales.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1 ANTECEDENTES DE LA EMPRESA

A&CGroup es una empresa de servicios que opera en Ecuador con oficinas en Guayaquil y Quito. Sus principales actividades son la prestación de servicios de auditoría financiera externa y la consultoría empresarial en aspectos contables, tributarios y legales.

El servicio de auditoría externa es un proceso sistemático e independiente que tiene por objeto averiguar la razonabilidad, integridad y autenticidad de los estados financieros utilizando procedimientos bajo un criterio de evaluación (por ejemplo normas contables vigentes) para emitir un informe que contenga una opinión basada

en la veracidad de los documentos y de los estados financieros que permita a los usuarios de dicha información tomar decisiones confiando en las declaraciones del Auditor.

A&CGroup, al tratarse de una empresa de servicios, desarrolla sus actividades utilizando personal con capacidad profesional calificada el cual es evaluado periódicamente para asegurar los estándares de calidad establecidos. Así, la ejecución de sus procedimientos de auditoría externa están alineados a las exigencias del Sistema de Gestión de Seguridad de la Información para proteger y utilizar adecuadamente la información de sus clientes. La empresa también sigue sus procedimientos respetando los lineamientos de un Sistema de Gestión de Calidad bajo la norma internacional ISO 9001 para asegurar la satisfacción de sus clientes.

3.2 IDENTIFICACIÓN DE PROCESOS CLAVES DE LA EMPRESA

El Estándar ISO 27001 promueve la adopción de un enfoque de procesos para todas las fases del Sistema de Gestión de Seguridad de la Información. «Enfoque basado en procesos» se denomina a la aplicación de un sistema de procesos dentro de la organización junto con la identificación y gestión sistemática de estas actividades y la interacción entre ellas.

Por consiguiente, para mantenerse alineado al Estándar, la empresa que pretenda implementar un SGSI, debe, si no lo ha hecho aún, organizar sus actividades en procesos. Definiremos como proceso a: una actividad o un conjunto de actividades que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados. Con frecuencia el resultado o salida de un proceso forma directamente la entrada de otro proceso.

Los procesos se ejecutan con la ayuda de recursos (personas, materiales, económicos, aplicaciones, etc.) y de acuerdo a unas directrices, procedimientos, instrucciones de trabajos, etc. Los procedimientos nos describen el método para llevar a cabo cada actividad, es decir, describen quién, cómo, cuándo y dónde se realizan las actividades que se requieren para generar las “entregas o salidas”.

Así, los procesos que se vayan definiendo deben ser clasificados según su naturaleza dentro de una de las tres categorías siguientes: estratégicos, operativos y de soporte.

Estratégicos:

Normalmente no están relacionados de forma directa con el cliente. Sus resultados afectan a la evolución en el tiempo de la organización y de sus competencias esenciales.

Operativos:

Constituyen la razón de ser de la organización. Se orienta a la prestación de servicios y aportan valor añadido al cliente externo, es decir, a los ciudadanos, organizaciones o sociedad en general. Estos procesos deben estar dirigidos a satisfacer las necesidades y expectativas de los ciudadanos. Los procesos clave no son comunes a todas las organizaciones, puesto que dependen del tipo de organización.

Soporte:

Facilitan la ejecución de las actividades que integran los procesos operativos, y generan valor añadido al cliente interno.

El Estándar ISO 27001 utiliza el modelo de proceso Planear-Hacer-Chequear-Actuar (PDCA, por sus siglas en inglés), el cual puede ser aplicado a todos los procesos que forman el SGSI. El modelo macro aplicado al SGSI permite que los requerimientos y expectativas respecto a la seguridad de la información de los clientes y partes interesadas sean gestionadas a través de los procesos implantados produciendo resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas inicialmente identificadas.

Desde una visión general el modelo de proceso PDCA abarca cuatro fases descritas a continuación: 1) Planear (establecer el SGSI).- Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización, 2) Hacer (implementar y operar el SGSI).- Implementar y operar la política, controles, procesos y procedimientos SGSI, 3) Chequear (monitorear y revisar el SGSI).- Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión y 4) Actuar (mantener y mejorar el SGSI).- Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Con el tiempo, la empresa interioriza una filosofía de procesos que señala que es necesario entender los procesos para definirlos, definirlos para medirlos, medirlos para comunicar su desempeño, comunicar su desempeño para administrarlos, administrarlos para mejorarlos continuamente y mejorarlos continuamente para proveer mayor valor al cliente y la empresa. Uno de los aspectos más importantes es controlar un proceso, lo cual significa asegurar que se generan, de manera continua, resultados previsibles y satisfactorios. Para controlar un proceso es necesario asignarle: objetivos, indicadores cuantitativos para medir el logro de los objetivos, un sistema de medida para cada indicador (cuando aplique), un propietario o responsable del proceso, un método de estandarización de su aplicación.

En la figura 3.1 Mapa de procesos, se pueden observar los procesos estratégicos, operativos y de soporte de la empresa A&CGroup, junto con sus secuencias e interacciones de los mismos.

Figura 3.1 Mapa de procesos. Referencia: Autor

Como proceso estratégico tenemos al proceso Gestión Gerencial Estratégica, el cual contendrá actividades como: establecer políticas de seguridad de la información, establecer objetivos y planes de seguridad, establecer roles y responsabilidades para la seguridad, proporcionar recursos para desarrollar, implementar, operar y mantener el SGSI, decidir los criterios de aceptación del riesgo, asegurar que se realicen auditorías internas y realizar revisiones con el fin de cerciorar la continua idoneidad, conveniencia y efectividad del SGSI.

Luego tenemos a los procesos operativos, los cuales son: Planeación, Realización y Finalización.

Dentro del proceso de planeación, se encuentran todas las actividades relacionadas con la negociación y la planificación de las auditorías financieras que se realizarán en los clientes. Estas actividades son: recabar información sobre los requerimientos del cliente, elaborar un presupuesto de tiempo para brindar el servicio, preparar una propuesta basada en los requerimientos del cliente, elaborar el contrato de auditoría externa, enviar el acuerdo de confidencialidad para el cliente, seleccionar el personal requerido para el trabajo y programar visitas al cliente por parte del equipo de trabajo.

Dentro del proceso de realización, se encuentran todas las actividades relacionadas con la ejecución de la auditoría financiera en los clientes, tales como: generación de papeles de trabajo basados en las pruebas realizadas y la información obtenida por parte del cliente y la elaboración de la carta de observaciones y recomendaciones.

Dentro del proceso de finalización, se describen todas las actividades a realizarse una vez que se culmina con el servicio de auditoría financiera. Estas actividades son: actualizar el registro de estrategia de auditoría y revisión analítica, concluir los

papeles de trabajo, generar el informe preliminar, llenar la planilla de ajustes y reclasificaciones, llenar el checklist de liberación de informe y emitir el informe final de auditoría.

Como procesos de soporte tenemos: contabilidad, compras, auditoría interna, control de documentos, talento humano y gestión de seguridad.

Dentro el proceso de contabilidad se realiza actividades como: elaboración de presupuestos, facturación y cobranzas.

El proceso de compras tiene como finalidad obtener de una manera oportuna y efectiva los productos y servicios que requiere la organización, asegurándose de que estos cumplan con las especificaciones señaladas. Entre las actividades que se realizan dentro de este proceso están: Evaluar e incorporar proveedores, generar requerimientos de compras, firmar acuerdo de confidencialidad con proveedores, emitir la orden de compra.

El proceso de auditoría interna consiste en determinar si los objetivos, controles, procesos y procedimientos del SGSI cumplen con: los requerimientos de este estándar y la legislación; con los requerimientos de seguridad identificados con el fin de saber si son mantenidos e implementados de manera efectiva y si se desempeñan como se esperaba. Entre las actividades que se realizan dentro de este proceso están: Establecer e implementar el programa de auditoria, realizar seguimiento, revisar y mejorar el programa de auditoria.

El proceso de control de documentos tiene como finalidad definir las actividades y responsabilidades para la elaboración, codificación, aprobación, distribución, modificación y recolección de documentos internos y externos, asegurando que la documentación este actualizada, legible y disponible en los lugares de uso, para lograr la estandarización en la administración y control de toda la documentación del SGSI. Entre las actividades que se realizan dentro de este proceso están: Revisar y actualizar documentos antes de su emisión, Identificar los cambios en los documentos, controlar la distribución de los documentos, controlar la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

El proceso de talento humano tiene como finalidad definir la competencia necesaria para el personal que realiza los trabajos que afectan el servicio brindado, asegurarse de que el personal es consciente de la pertenencia e importancia de sus actividades y de cómo contribuyen al logro de los objetivos de la organización, asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y obligaciones. Entre las actividades que se realizan dentro de este proceso están: Seleccionar y reclutar de personal, definir los requerimientos basados en el presupuesto, definir y aprobar el perfil de cargo y los roles y responsabilidades de cada cargo en la seguridad de la información, firmar contrato y acuerdo de confidencialidad y exclusividad, asignar activos de información.

El proceso de gestión de seguridad consiste en lograr y mantener la protección apropiada de los activos organizacionales, asegurar que la información reciba un nivel de protección apropiado gestionando los riesgos relacionados; evitar accesos físicos y lógicos no autorizados que podrían generar perdida, daño o robo de los activos y la interrupción de las actividades de la organización; Asegurar la operación correcta de los medios de procesamiento de la información, minimizar el riesgo de fallas en los sistemas, mantener la seguridad en el intercambio de información con entidades externas; Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas; Asegurar la comunicación que los eventos y debilidades en la seguridad sean comunicados al responsable del proceso; Contrarrestar las interrupciones de las actividades comerciales y asegurar la

reanudación oportuna de las operaciones de la empresa; Evitar violaciones de cualquier ley, obligaciones reguladoras y contractuales.

3.3 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El proceso de identificación de activos de información es muy importante, ya que nos permite reconocer cuales son los activos que se encuentran asociados a los procesos de la organización.

La realización de cada proceso involucra activos de información específicos, en sus diversos tipos y formatos, los cuales son listados en la tabla 3.1 Inventario de Activos que se muestra a continuación:

No.	Activo	Tipo de activo
1	Servidores	Hardware
2	Socio, Auditores	Persona
3	File Papeles de trabajo – documentos físicos	Datos/Soportes de información
4	Registros SGSI llenados (formato digital)	Datos/Soportes de información
5	Servicio de correo electrónico	Servicio
6	Red de área local e inalámbrica	Comunicaciones

7	Sistema META, SAFI	Software/ Información
8	Personal administrativo	Persona
9	Software ACL	Software/ Información
10	Sitio Web	Servicio
11	Sistema de comunicación telefónica IP	Comunicaciones
12	Computadores/Laptops	Hardware
13	Impresoras	Hardware

Tabla 3.1 Inventario de Activos. Referencia: Autor

3.4 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA EMPRESA.

Debido a la necesidad de implementar un SGSI, la empresa procede a realizar un diagnóstico de la situación actual respecto a los requisitos de la norma, con el fin de poder tener una idea de que mecanismos tiene instaurada la organización que puedan aprovecharse para así facilitar la implementación de los requisitos exigidos por ISO 27001, ya que la empresa cuenta con un Sistema de Gestión de la Calidad basado en ISO 9001:2008 ya establecido. A continuación, en la tabla 3.2 se presenta el diagnóstico basado en ISO 27001:2005.

REQUISITO NORMATIVO	PORCENTAJE DE CUMPLIMIENTO
4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**26%**
4.1 Requisitos generales	20
4.2 Establecimiento y gestión del SGSI	21
4.3 Requisitos de la documentación	37
5. RESPONSABILIDAD DE LA DIRECCIÓN	**59%**

5.1 Compromiso de la dirección	60
5.2 Gestión de los recursos	58
6 AUDITORÍAS INTERNAS DEL SGSI	**10%**
7 REVISIÓN POR LA DIRECCIÓN DEL SGSI	**7%**
7.1 Generalidades	10
7.2 Elementos de entrada para la revisión	0
7.3 Resultados de la revisión	10
8 MEJORA DEL SGSI	**10%**
8.1 Mejora continua	10
8.2 Acción correctiva	10
8.3 Acción preventiva	10
PORCENTAJE DE CUMPLIMIENTO GENERAL	**22,40%**

Tabla 3.2 Diagnóstico basado en ISO 27001:2005. Referencia: Autor

CAPÍTULO 4

PLANEACIÓN PARA LA IMPLEMENTACIÓN DE UN SGSI

4.1 MODELO PDCA (PLAN – DO – CHECK – ACT)

El modelo PDCA (Plan, Do, Check, Act), en su equivalencia en español: Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua.

Este modelo es muy usado para la implantación de sistemas de gestión, en este caso un Sistema de Gestión de Seguridad de Información, ya que permite una efectiva organización y documentación, lo cual es requerido en este proceso.

En la figura 4.1 Modelo PDCA, se muestra este modelo basado en los procedimientos esenciales para un SGSI.

Figura 4.1 Modelo PDCA. Referencia: Autor

El modelo PDCA es una estrategia de mejora continua, implementada en cuatro pasos detallados a continuación:

4.1.1 PLANIFICAR

1. Planificación de la gestión del servicio.
2. Definir el alcance del SGSI en la empresa.
3. Identificar los activos de información y tasarlos.
4. Hacer el análisis y evaluación del riesgo.
5. Determinar opciones para el tratamiento del riesgo.
6. Definir los procesos.
7. Definir los recursos, equipamiento, presupuestos, herramientas.

4.1.2 HACER

Implementar la gestión y provisión del servicio.

1. Elaborar el plan de tratamiento del riesgo, detallando las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas.

4.1.3 VERIFICAR

1. Monitorear, medir y verificar.
2. Desarrollar procedimientos de monitoreo.
3. Revisar regularmente el SGSI.
4. Revisar objetivos y plan de gestión del servicio.

5. Auditar internamente el SGSI.

4.1.4 ACTUAR

Mantener el SGSI y desarrollar la mejora continua.

1. Identificar e implantar las mejoras.
2. Adoptar acciones correctivas y preventivas.
3. Verificar que las mejoras cumplen su objetivo.

4.2 ALCANCE

En la actualidad existen muchos aspectos que se deben tener en cuenta para asegurar que se cumplan con las expectativas requeridas, es decir que existen una serie de normativas que cuidan hasta lo mínimo para que todo resulte un éxito. Por lo tanto, se debe disponer de todos los recursos para garantizar la seguridad de la información, como es el caso de la empresa de auditoría y consultoría A&CGroup, que maneja información sensible de sus clientes.

La información perteneciente a la compañía debe protegerse de acuerdo a su valor e importancia. Deben usarse medidas de seguridad sin importar como la

información se guarda, procesa o transmite. Esta protección incluye restricciones de acceso a los usuarios según su cargo.

La implementación del Manual de Políticas de Seguridad, corresponde al departamento de Sistemas, el cual tiene a su cargo las siguientes funciones:

- Gestionas proyectos para soportar los requerimientos del negocio y el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión Integrado.
- Gestionar los procesos del Sistema de Gestión Integrado relacionados a sistemas, tecnologías y seguridad de la información.
- Mantener un plan de inversiones y estrategias relacionadas con soluciones y servicios de hardware y software a corto y a largo plazo.
- Informar a la administración acerca del estado actual de la tecnología, posibles futuras tendencias y oportunidades de valor para el negocio.
- Administrar los recursos tecnológicos y plataformas que lo soportan.
- Diseñar soluciones y servicios de sistemas y tecnologías de la información.
- Gestionar los incidentes de seguridad de la información encontrados.
- Monitorear los procesos del Sistema de Gestión Integrado relacionados a sistemas, tecnologías y seguridad de la información.

- Evaluar los controles que aseguren la confidencialidad, integridad y disponibilidad de la información según lo dispuesto en el Sistema de Gestión Integrado.

El alcance del SGSI cubrirá las operaciones contenidas en los procesos de Planeación, Realización y Finalización de Servicios de Auditoría Financiera Externa.

Se excluye el control previsto en A.10.9.1 Comercio electrónico en nuestro SGSI porque nuestra firma no maneja transacciones de comercio electrónico.

4.3 OBJETIVO GENERAL

Proporcionar a la alta gerencia las directrices y el soporte para la seguridad de la información, es decir qué requiere ser protegido, por qué, de qué debe ser protegido y cómo protegerlo; acorde con los requerimientos comerciales, leyes y regulaciones relevantes.

4.4 POLÍTICAS DE SEGURIDAD

Estas políticas representan directrices que deben ser adoptadas por el personal de la empresa. A continuación detallamos las políticas generales.

1. Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
2. Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
3. Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
4. El ingreso de las personas a la oficina será restringido con el uso de un mecanismo electrónico de control de accesos basado en lector de huellas dactilares y el software respectivo que validará el ingreso al personal enrolado en el sistema y que se encuentre autorizado para su ingreso.
5. El acceso al cuarto de servidores estará limitado al responsable del área de Tecnología y Sistemas de Información, y en su ausencia, a la persona que se delegue. Para el ingreso se contará con un mecanismo electrónico de control de accesos basado en lector de huellas dactilares.
6. Las contraseñas contendrán al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.
7. Se debe mantener el escritorio del computador (Windows) limpio de información confidencial para la empresa.
8. En caso de que necesite alejarse del computador inmediatamente, bloquear la sesión activa.

9. Se debe usar un protector de pantalla ante inactividad del computador, el mismo que se establecerá para activarse luego de 2 minutos de inactividad.
10. Los archivos creados deberán ser almacenados en la carpeta “Mis Documentos” la cual mantiene una copia sincronizada en el recurso “Documentos” del servidor.

CAPÍTULO 5

ANÁLISIS DE RIESGO, DISEÑO DE LA EVALUACIÓN DEL RIESGO

5.1 METODOLOGÍA DE CONTROL DE RIESGO

Debido a que las condiciones económicas, industriales, normativas y operacionales se modifican de forma continua, se hacen necesarios mecanismos para identificar y minimizar los riesgos específicos asociados con este cambio.

Por tal motivo, existen varias metodologías para realizar el análisis de riesgo; cada una tiene sus propias características, ventajas y desventajas; por tanto debemos seleccionar la más adecuada acorde a la realidad de la empresa y de esta manera analizar las vulnerabilidades actualmente presentes en la organización.

5.2 METODOLOGÍA MAGERIT

Magerit es una metodología de análisis y gestión de riesgos que proporciona un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para asi poder implementar las medidas de control más adecuadas que permitan mitigar los riesgos.

Magerit se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser aprovechadas por estas amenazas, obteniendo una identificación clara de las medidas preventivas y correctivas más apropiadas.

Esta metodología es muy útil, ya que permite enfocar los esfuerzos en los riesgos que pueden ser más críticos para la empresa, aquellos relacionados con los sistemas de información. En la figura 5.1, se puede observar la metodología.

Magerit persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

5.3 VENTAJAS DE LA METODOLOGÍA

- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.
- Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla.

- Permitirá saber cuánto valor tiene la información o los servicios que maneja la empresa y ayudará a protegerlos.
- Conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos.
- Tener una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Figura 5.1 Metodología MAGERIT

5.4 ANÁLISIS DEL RIESGO

El análisis del riesgo contempla lo siguiente:

1. Identificación de activos de información.

2. Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados.
3. Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
4. Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
5. Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

Es importante entender la exigencia de la norma ISO 27001:2005 en relación con el riesgo. La exigencia es bastante clara y no debería llevar a confusiones. En primera instancia, se deben seguir los pasos para realizar el análisis del riesgo, y posteriormente construir una escala para determinar la evaluación del riesgo. Son dos etapas claramente definidas.

5.4.1 INVENTARIO DE ACTIVOS

Los activos de información en la empresa, dentro del alcance del SGSI, son fundamentales para una correcta implementación de un SGSI. El análisis y la evaluación del riesgo y las decisiones que se tomen en relación con el tratamiento del riesgo en la empresa giran alrededor de estos activos identificados.

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación de la empresa y una continuidad en las operaciones.

Los activos de información son muy amplios y es importante estar conceptualmente claros de que es un activo de información, para así poder realizar un correcto análisis y una evaluación del riesgo y, por ende, establecer adecuadamente el modelo ISO 27001:2005.

En la organización, el proceso de identificación y tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo. Es importante que los dueños de los activos principales conformen un grupo multidisciplinario. Como un dueño de activo se entiende aquella persona que tiene una responsabilidad por el control del mantenimiento, uso y seguridad de los activos, aprobada por la gerencia. Dentro del alcance del SGSI, los activos importantes deben identificarse con claridad, y

posteriormente deben ser tasados para visualizar su impacto en la empresa por su deterioro o por fallas en: confidencialidad, integridad y disponibilidad.

Luego de todo este proceso, la compañía logró identificar 13 activos importantes, los cuales se presentan a continuación en la tabla 5.1:

No.	Activo	Tipo de activo
1	Servidores	Hardware
2	Socio, Auditores	Persona
3	File Papeles de trabajo – documentos físicos	Datos/Soportes de información
4	Registros SGSI llenados (formato digital)	Datos/Soportes de información
5	Servicio de correo electrónico	Servicio
6	Red de área local e inalámbrica	Comunicaciones
7	Sistema META, SAFI	Software/ Información
8	Personal administrativo	Persona
9	Software ACL	Software/ Información
10	Sitio Web	Servicio
11	Sistema de comunicación telefónica IP	Comunicaciones
12	Computadores/Laptops	Hardware
13	Impresoras	Hardware

Tabla 5.1 Inventario de Activos. Fuente: Autor

5.4.2 IDENTIFICACIÓN DE REQUERIMIENTOS LEGALES Y COMERCIALES

Los requerimientos de seguridad en las organizaciones se derivan de tres fuentes:

1. La evaluación de los riesgos que afectan a la organización. Aquí se determinan las amenazas de los activos, luego se ubican las

vulnerabilidades, se evalúa su posibilidad de ocurrencia, y se estiman los potenciales impactos.

2. El aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse.
3. El conjunto de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

Al identificar los activos de información, se debe analizar si existen requerimientos legales y comerciales relacionados con estos activos identificados. De ser el caso, se debe revisar si dichos requerimientos involucran otros activos de información.

En la tabla 5.2 Identificación de requerimientos legales, se muestran los requerimientos legales y comerciales que aplican para A&CGroup:

AuditGroup

Identificacion de requerimientos legales

					Consecuencias o Impactos por incumplimiento								
Ley/Reglamento/estatuto	Lugar de almacenamiento	Clausula/indice especifico	Requisitos a cumplir	Activos de información a los que aplica	Por pérdida / atraso / oportunidad (Disponibilidad)	Por destrucción (Integridad)	Por falsificación (Integridad)	Por divulgación (Confidencialidad)	Responsable de cumplimiento	Evidencia Objetiva de cumplimiento en AuditGroup	Evaluador	Frecuencia	Registros de Evaluacion
Ley de Propiedad Intelectual del Ecuador	Accesible desde sistema LEXIS	Que no se utilicen derechos intelectuales de terceros sin acuerdos	*Evitar la copia y distribución no autorizada de software *Instalar un determinado número de veces según especifique el contrato de licencia de uso	Software: Microsoft, ACL, SAFI, Trend Micro, Documentación de Clientes			Por incumplimiento de contratos de licencia, la empresa se expone a posibles juicios legales		Responsable Area Sistemas	Inventario de software / File Licencias de software	BSA (Business Software Alliance)		Informe de cumplimiento de BSA
Contratos de Auditoría Externa	File Administración	Cumplir con la obligación que tiene el Auditor Externo de remitir contrato a la Superintendencia de Compañías	Mantener en custodia, al menos por cinco años, los papeles de trabajo, evidencias y más documentos en los que se fundamentó la opinión emitida; y, i) guardar en reserva la información contable auditada de la compañía, respecto de terceros	Procesos: Negociación, Planificación, Ejecución y Terminación de Auditoría Externa	Sanción por atraso				Representante Legal de AuditGroup	Informes entregados	SIC, SIB y SRI	Anual	Carta de entrega del informe
Contratos de trabajo	File Administración	Código del Trabajo y Ley de Seguridad Social	Ver R14-016 Contrato de trabajo a plazo fijo (1 año) Renovado a plazo indefinido	Procesos: Negociación, Planificación, Ejecución y Terminación de Auditoría Externa	N/A	N/A	N/A	N/A	Representante Legal de AuditGroup		Inspectoría de Trabajo		
Ley de Compañías	Accesible desde sistema LEXIS	Mantener las condiciones que permitan a la compañía obtener el certificado de cumplimiento de obligaciones		Documentación física	El perder el CCO puede inhabilitar a la compañía				Representante Legal de AuditGroup	CCO	SIC	permanente	
Reglamento para la calificación y registro de las personas naturales y jurídicas que ejerzan actividades de auditoría externa (Resolución No. 02.Q.ICI.007) Normas Internacionales de Información Financiera (NIF) / NIC "Reglamento sobre los requisitos mínimos que deben contener los informes de auditoría externa (Resolución No. 02.Q.ICI.008)" "Normas sobre montos mínimos de activos en los casos de auditoría externa obligatoria (Resolución No. Normas internacionales de auditoría y aseguramiento "NIAA" (Resolución Ley de Mercado de Valores (Título XXI) Codificación de Resoluciones Expedidas por el Consejo Nacional de Valores (Título II, Subtítulo IV, Capítulo IV)	Accesible desde sistema LEXIS	Mantener las condiciones que permitan que la firma mantenga los requisitos para actuar como Auditor Externo ante la SIC y CNV		Documentación física	El perder el Registro del Auditor afectaría a los ingresos de la compañía				Representante Legal de AuditGroup	Registros ante SIC	SIC	5 años	Resolución de SIC

Tabla 5.2 Identificación de requerimientos legales

AuditGroup

Identificacion de requerimientos legales

					Consecuencias o Impactos por incumplimiento								
Ley/Reglamento/estatuto	Lugar de almacenamiento	Clausula/indice especifico	Requisitos a cumplir	Activos de información a los que aplica	Por pérdida / atraso / oportunidad (Disponibilidad)	Por destrucción (Integridad)	Por falsificación (Integridad)	Por divulgación (Confidencialidad)	Responsable de cumplimiento	Evidencia Objetiva de cumplimiento en AuditGroup	Evaluador	Frecuencia	Registros de Evaluacion
Ley General de Instituciones del Sistema Financiero (Arts. 138) Reglamento General de la Ley General de Instituciones del Sistema Financiero Resoluciones de la Superintendencia de Bancos y Seguros y Junta Bancaria (Libro I, Título XXI, Capítulo I) (Libro II, Título X, Capítulo I) Ley General de Seguros "Normas para la contratación y funcionamiento de las firmas de auditoría externa que ejerzan su actividad en las empresas de seguros y compañías de reaseguros (Resolución No. JB-2001-287)"	Accesible desde sistema LEXIS	Mantener las condiciones que permitan que la firma mantenga el registro para actuar como Auditor Externo ante la Superintendencia	Revisar que la contabilidad de las instituciones que se auditen se realice de acuerdo con el CUC y en base a NIAA	Documentación física, Papeles de trabajo e Informes	El perder el Registro del Auditor afectaría a los ingresos de la compañía				Representante Legal de AuditGroup	Registros ante SIC	SD	Anual	Resolución de SD
Código Tributario Ley de Régimen Tributario Interno Reglamento para la Aplicación de la Ley de Régimen Tributario Interno	Accesible desde sistema LEXIS	Pagar los tributos de tal forma de tal forma que no se afecte la continuidad de la firma y realizar el trabajo de auditoría para poder emitir los informes de cumplimiento tributario de los clientes		Documentación física, Papeles de trabajo e Informes	Sanción por atraso				Representante Legal de AuditGroup		SRI	permanente	
Protección de datos personales (Ley del Sistema Nacional de Registro de Datos Públicos)	Accesible desde sistema LEXIS	El Art. 66 de la Constitución de la República, en su parte pertinente dispone: "... Se reconoce y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley". LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS Art. 4.- Responsabilidad de la información.- Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provea toda la información. Las personas afectadas por información falsa o imprecisa, difundida	1. Confidencialidad; y, 2. Responsabilidad	Información generada en Sistemas de información: SAFI, SAAL									
Ley de Comercio Electrónico, Firmas y Mensajes de Datos Ley No. 67, publicada en el Registro Oficial Suplemento No. 577 de 17 de abril del 2002	Accesible desde sistema LEXIS			Firmas electrónicas utilizadas en sistema de correo electrónico									

Tabla 5.3 Identificación de requerimientos legles 2

5.4.3 TASACIÓN DE ACTIVOS

El proceso de identificación y tasación de activos tiene como objetivo conocer el valor que poseen estos activos para la Organización y así comprender cuales tienen una mayor relevancia. Esta información será útil en el proceso de gestión de riesgo ya que se conocerá qué activos tienen un mayor valor y por consiguiente deben tener prioridad en su protección.

La forma de conocer el valor de un activo, es indagando que tanto impactaría en el negocio un deterioro o pérdida de confidencialidad, integridad o disponibilidad en el mencionado activo. Si el impacto sobre el negocio es alto ante una posible falla en la seguridad de la información, mayor será también el valor del activo. Así podremos conocer qué tan crítica y sensible es la información manejada en la Organización.

El valor de un activo vendrá definido por el promedio de la afectación a la Integridad, Disponibilidad y Confidencialidad para su respectivo proceso mediante la siguiente fórmula:

$$VA = \frac{Vi + Vd + Vc}{3}$$

Siendo:

VA = Valor de activo

Vi = Valor en Integridad

Vd = Valor en Disponibilidad

Vc = Valor en Confidencialidad

El primer paso del procedimiento es elegir el proceso de negocio del cual se realizará la identificación y tasación de activos. En el ejemplo que ilustraremos a continuación hemos elegido el proceso de Planeación. Luego iremos identificando los sub-procesos que interactúan en Planeación y las actividades que se llevan a cabo. Para la ejecución de este procedimiento se realizarán reuniones de trabajo en donde deberán participar como mínimo; el líder de Proyecto y el administrador del proceso Planeación. En la reunión de trabajo se irán señalando y describiendo cada una de las actividades que se realizan dentro del proceso y los activos que van interviniendo en las actividades. El resultado se irá registrando en un documento conocido como Matriz de Activos y Valoración.

Para el ejemplo, seleccionamos al sub-proceso “Conocimiento del negocio”. Aquí intervienen las actividades: A) reuniones con jefes de área del cliente y B) preparación del documento de Conocimiento del negocio. Para la actividad “A”

identificamos a los siguientes activos que están presentes en la actividad A: auditores, computadores, documentos físicos. Luego, para cada uno de los activos identificados, continuamos realizando la pregunta “Sin considerar la presencia de salvaguardas, un deterioro o pérdida de confidencialidad, integridad o disponibilidad en el activo Auditores, ¿cómo impacta el proceso PLANEACIÓN? Para cuantificar, hacemos uso de la escala de Likert y asignaremos un valor de 1 si el impacto es muy bajo o un valor de 5 si el impacto es muy alto, como se muestra en la tabla 5.4 Escala de Likert:

1	2	3	4	5
Muy Bajo	Bajo	Medio	Alto	Muy alto

Tabla 5.4 Escala de Likert

Para el caso de la determinación del impacto desde el punto de vista de confidencialidad, los datos reciben una alta valoración cuando su revelación causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

A&CGroup
Selección y Tasación de Activos de Información

Proceso : Planeación — Responsable del proceso: Gerente de Auditoria

1. Para qué sirve la Tasación de activos: Sirve para ver la relevancia que tienen los activos en la empresa

2. Pregunta a ser realizada cada vez que tasamos un activo: Sin considerar la presencia de salvaguardas: un deterioro o pérdida de confidencialidad, integridad o disponibilidad en un activo X, ¿cómo impacta el proceso PLANEACIÓN?

Escala de Likert: 1 Muy Bajo | 2 Bajo | 3 Medio | 4 Alto | 5 Muy alto

Subproceso	ACTIVO	Tipo de Activo	Confidencialidad (acceso no autorizado)	Integridad (alteración)	Disponibilidad	Promedio	Observaciones / Evento	Evaluación del riesgo
Visita de planeación	Carta de requerimiento a Cliente	Información/Documento	2	3	4	3		
	File Permanente de Cliente	Información/Documento	5	5	5	5		
	File Papeles de Trabajo Cliente	Información/Documento	5	5	5	5		
	Carta de Presentación de los auditores	Información/Documento	1	4	2	2,33		
	Socio	Persona	5	5	5	5		
	Auditores	Persona	5	5	5	5		
	Laptops	Hardware	5	5	5	5		
	Registros del Sistema de Gestión de Calidad	Documento	4	5	5	4,67	Registros vacíos	
Conocimiento del negocio	Estrategia de Auditoría	Información/Documento	5	5	5	5		
	Revisión Analítica	Información/Documento	5	5	5	5		
	Partes Relacionadas	Información/Documento	5	5	5	5		
	Materialidad	Información/Documento	5	5	5	5		
	Empresa en Marcha	Información/Documento	5	5	5	5		
	Fraude	Información/Documento	5	5	5	5		
	Documentos de Conocimiento del negocio	Información/Documento	5	5	5	5	Incluye flujos o narrativas de procesos	
	Servidores	Hardware	5	5	5	5		
	Servicio de correo electrónico	Servicio	5	5	3	4,33		
Adaptación de Programas de Auditoría	Registros de Programas de Auditoría	Información/Documento	4	5	5	4,67		
	Determinación de Muestra para Pruebas de Control	Información/Documento	4	5	5	4,67		
	Programa de Auditoría Impositiva	Información/Documento	2	3	2	2,33		
	Checklist Administrativo de Auditoría	Información/Documento	2	3	2	2,33		
Reportes	Sistema M.E.T.A. y base de datos	Software/Información	4	4	2	3,33		
	Reporte del Tiempo	Información/Documento	1	2	1	1,33		
	Liquidación de Gastos de Viaje	Información/Documento	1	1	1	1		

Tabla 5.5 Tasación de activos del proceso Planeación.

Como hemos observado en la tabla 5.5, se ha realizado la tasación de cada uno de los activos que intervienen en la actividad A “Reuniones con jefes de área del cliente”, obteniendo el valor del activo en función de los valores asignados en confidencialidad, integridad y disponibilidad.

Este mismo procedimiento se realiza con los procesos de Realización (ver tabla 5.6) y Finalización (ver tabla 5.7).

A&CGroup
Selección y Tasación de Activos de Información

Proceso : Realización — Responsable del proceso: Gerente de Auditoria

1. Para qué sirve la Tasación de activos: Sirve para ver la relevancia que tienen los activos en la empresa

2. Pregunta a ser realizada cada vez que tasamos un activo: Sin considerar la presencia de salvaguardas: un deterioro o pérdida de confidencialidad, integridad o disponibilidad en un activo X, ¿cómo impacta el proceso REALIZACION?

Escala de Likert: 1 Muy Bajo; 2 Bajo; 3 Medio; 4 Alto; 5 Muy alto

Subproceso	ACTIVO	Tipo de Activo	Confidencialidad (acceso no autorizado)	Integridad (alteración)	Disponibilidad	Promedio	Observaciones / Evento	Evaluación del riesgo
Ejecución de pruebas sustantivas y de control	Asistentes de auditoría	Persona	5	4	4	4,33		
	Encargado de Sistemas	Persona	4	4	3	3,67		
	Laptops	Hardware	5	5	5	5		
	Software ACL	Software	5	5	4	4,67		
	Registros del Sistema de Gestión de Calidad	Documento	4	5	5	4,67	Registros vacíos	
	Servidores	Hardware	5	5	3	4,33		
	Servicio de correo electrónico	Servicio	5	5	3	4,33		
	Impresora	Hardware	2	2	3	2,33		
	Papeles de Trabajo	Información/Documento	5	5	5	5		
	Confirmación de Bancos	Información/Documento	4	5	5	4,67		
	Confirmación a Clientes y Proveedores	Información/Documento	4	5	5	4,67		
	Confirmación a Seguros	Información/Documento	4	5	5	4,67		
	Confirmación a Abogados	Información/Documento	5	5	5	5		
	Confirmación de Inversiones Permanentes	Información/Documento	4	5	5	4,67		
	Control de Confirmaciones	Información/Documento	4	5	5	4,67		
	Checklist para la Observación de Inventarios Físicos	Información/Documento	3	5	5	4,33		
	Documentación física proporcionada por el Cliente	Información/Documento	5	5	5	5		
	Documentación electrónica proporcionada por el Cliente	Información/Documento	5	5	5	5		
Revisión y aprobación de papeles de trabajo	Encargado de auditoría	Persona	5	5	3	4,33		
	Gerente de auditoría	Persona	5	5	3	4,33		
	File Permanente de Cliente	Información/Documento	5	5	5	5		
	File Papeles de Trabajo Cliente	Información/Documento	5	5	5	5		
	Carta de Observaciones y Recomendaciones Preliminar	Información/Documento	5	5	5	5		
	Socio	Persona	5	5	5	5		
Reportes	Carta de envío de Observaciones y Recomendaciones	Información/Documento	1	4	2	2,33		
	Reporte de Observaciones y Recomendaciones	Información/Documento	5	5	5	5		
	Control de Cumplimiento de Servicios	Información/Documento	2	5	2	3		
	Asistente de Gerencia	Persona						

Tabla 5.6 Tasación de Activos del proceso Realización

Proceso :	Finalización					Responsable del proceso: Gerente de Auditoria		
	1. Para qué sirve la Tasación de activos: Sirve para ver la relevancia que tienen los activos en la empresa 2. Pregunta a ser realizada cada vez que tasamos un activo: Sin considerar la presencia de salvaguardas: un deterioro o pérdida de confidencialidad, integridad o disponibilidad en un activo X, ¿cómo impacta el proceso FINALIZACION?							
	Escala de Likert: 1 Muy Bajo	2 Bajo	3 Medio	4 Alto	5 Muy alto			

Subproceso	ACTIVO	Tipo de Activo	Confidencialidad (acceso no autorizado)	Integridad (alteración)	sponibilid	Promedio	Observaciones / Evento	Evaluación del riesgo
Revisión inicial	Asistentes de auditoría	Persona	4	4	4	4		
	Encargado de auditoría	Persona	5	5	3	4,33		
	Laptops	Hardware	5	5	5	5		
	Servidores	Hardware	5	5	4	4,67		
	Servicio de correo electrónico	Servicio	5	5	4	4,67		
	Impresora	Hardware	2	2	4	2,67		
	Copiadora	Hardware	2	2	2	2		
	Registros del Sistema de Gestión de Calidad	Documento	4	5	5	4,67		
	Reporte de Observaciones y Recomendaciones (R8-011)	Información/Documento	4	5	5	4,67		
	Estrategia de Auditoría (R7-003)	Información/Documento	4	5	5	4,67		
	Revisión Analítica (R7-004)	Información/Documento	4	5	5	4,67		
	Socio	Persona	5	5	5	5		
	File Papeles de Trabajo Cliente	Información/Documento	5	5	5	5		
Revisión y Aprobación	Eventos Subsecuentes NEA 19 (R9-001)	Información/Documento	4	5	5	4,67		
	Eventos Subsecuentes - Evaluación a la Gerencia (R9-002)	Información/Documento	4	5	5	4,67		
	Documentación física proporcionada por el Cliente	Información/Documento	5	5	5	5		
	Documentación electrónica proporcionada por el Cliente	Información/Documento	5	5	5	5		
	MAPS (R9-003)	Información/Documento	4	5	5	4,67		
	Planilla de Ajustes y Reclasificaciones (R9-004)	Información/Documento	4	5	5	4,67		
	Carta de Representación (R9-005)	Información/Documento	5	5	5	5		
Revisión de control	Checklist de Papeles de Trabajo (R9-007)	Información/Documento	3	5	3	3,67		
	Checklist Impositivo (R9-008)	Información/Documento	5	5	5	5		
Preparación de Informe Preliminar	Informe Preliminar (R9-009)	Información/Documento	5	5	5	5		
	Checklist de liberación de informe (R9-010)	Información/Documento	3	5	3	3,67		
Revisión de Informe Preliminar (Socio)	Informe Preliminar revisado	Información/Documento	5	5	5	5		
	Carta de envío	Información/Documento	1	4	2	2,33		
	Asistente de Gerencia	Persona	4	4	3	3,67		
Revisión de Informe Preliminar (Cliente)	Carta y comentarios de Cliente sobre Informe	Información/Documento	5	5	5	5		
Emisión de Informe Final	Informe Final	Información/Documento	5	5	5	5		

Tabla 5.7 Tasación de Activos del proceso Finalización

5.4.4 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.

Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza, para así facilitar su ubicación. A continuación mostramos seis tipos en los que se pueden clasificar las amenazas:

1. Amenazas naturales: inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.
2. Amenazas a instalaciones: fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas.
3. Amenazas humanas: huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave.
4. Amenazas tecnológicas: virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas.
5. Amenazas operacionales: crisis financieras, pérdida de proveedores, fallas en equipos, aspectos regulatorios, mala publicidad.
6. Amenazas sociales: motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.

Las amenazas se pueden originar de fuentes o eventos accidentales. Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización.

Una vez identificadas las distintas amenazas que pueden afectar un activo, se debe evaluar su posibilidad de ocurrencia.

Por cada amenaza, para medir su posibilidad de ocurrencia, se recomienda utilizar una escala de Likert, como la que se presenta a continuación en la ilustración 5.4:

1	2	3	4	5
Muy Bajo	Bajo	Medio	Alto	Muy alto

Tabla 5.4 Escala de Likert

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo.

Las vulnerabilidades pueden clasificarse como:

1. Seguridad de los recursos humanos: falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al termino del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al termino del contrato de trabajo, empleados desmotivados.

2. Control de acceso: segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, contraseñas sin modificarse.

3. Seguridad física y ambiental: Control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje.

4. Gestión de operaciones y comunicación: Complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión.

5. Mantenimiento, desarrollo y adquisición de sistemas de información: Protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografías, carencia de validación de datos procesados, carencia

de ensayos de software, documentación pobre de software, mala selección de ensayos de datos.

Una vez identificadas las vulnerabilidades, por cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por la amenaza.

Para este propósito se recomienda utilizar una escala de Likert. Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre amenazas y vulnerabilidades. La pregunta fundamental es: ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades?

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, en la figura 5.2 se muestra la manera en que cada uno de estos elementos se encuentran relacionados.

Figura 5.2 Elementos de análisis del riesgo. Fuente: Diseño de un Sistema de Seguridad de Información - Alberto G. Alexander

En la tabla 5.8, se muestran los activos de información con sus respectivas amenazas y vulnerabilidades identificadas.

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada
Servidores (HW) (1)	5	Ataque lógico intencionado	Vulnerabilidad técnica en el sistema operativo
		Ataque lógico intencionado	Sistema operativo obsoleto
		Ataque lógico intencionado	Ausencia de plan de parcheo de software
		Fallas de origen físico	Desgaste natural de partes
		Fallas de origen físico	Partes defectuosas de fábrica
		Fallas de origen físico	Presencia de polvo, suciedad
		Desastres naturales	Ausencia de diseño antisísmico del edificio
		Fallas de origen físico	Ausencia de mantenimientos preventivos a los equipos.
		Fallas de origen lógico	Contraseña del administrador conocida por otros
		Fallas de origen lógico	Acceso no autorizado
		Caída del sistema por agotamiento de recursos	Falta de límites y control en el uso de recursos
Socio, Auditores (P) (2)	5	Indisponibilidad del personal	Enfermedad
		Errores por omisión o desconocimiento	Empleados desmotivados

		Ingeniería social	Desconocimiento de políticas y mejores prácticas de seguridad
		Malware para dispositivos móviles	Dispositivos móviles sin software de protección
File Papeles de Trabajo - documentos físicos (SI) (3)	5	Uso no previsto	Acceso no autorizado
		Uso no previsto	Ausencia de etiquetado (clasificación) de la información
		Uso no previsto	Ausencia de procedimientos de manejo de información clasificada
Registros SGS llenados (formato digital) (4)	5	Uso no previsto	Ausencia de etiquetado (clasificación) de la información
		Uso no previsto	Ausencia de procedimientos de manejo de información clasificada
		Acceso no autorizado	Ausencia de permisos de acceso
		Acceso no autorizado	Ausencia de revisión de privilegios
		Escapes de información	Uso de dispositivos extraíbles (pen drives)
		Escapes de información	Ausencia de control de contenidos transferidos en la red
		Alteración de la información	Introducción de información errónea
		Pérdida total o parcial	Permisos de acceso no controlados
		Pérdida total o parcial	Ausencia de respaldos de información
Servicio de correo electrónico (S) (5)	4,67	Uso no previsto	Errores (equivocaciones) de los usuarios
		Caída del sistema / Servicio no disponible / Denegación de servicio	Falta de límites y control en el uso de recursos
		Escapes de información	Ausencia de control de contenidos transferidos en la red
		Ataque lógico intencionado	Vulnerabilidad técnica en el sistema
		Ataque lógico intencionado	Sistema obsoleto
		Caída del sistema / Servicio no disponible / Denegación de servicio	Agotamiento de recursos
		Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso
Software ACL (SW) (9)	4,67	Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso
Red de área local e inalámbrica (COM) (6)	4,33	Fallas de origen físico	Desgaste natural de partes
		Fallas de origen físico	Partes defectuosas de fábrica

		Caída del sistema / Interrupción del servicio / Denegación de servicio	Agotamiento de recursos
		Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso
Sistema META, SAFI (SW) (7)	4	Difusión de software dañino	Presencia de bases de datos de antivirus desactualizadas
		Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso
Sitio web (S) (10)	3,67	Caída del sistema / Servicio no disponible / Denegación de servicio	Falta de límites y control en el uso de recursos
Personal administrativo (P) (8)	2,67	Errores por omisión o desconocimiento	Empleados desmotivados
		Indisponibilidad del personal	Enfermedad
		Ingeniería social	Desconocimiento de políticas y mejores prácticas de seguridad
Sistema de comunicación telefónica IP (11)	2,33	Fallas de origen físico	Desgaste natural de partes
		Fallas de origen físico	Partes defectuosas de fábrica
		Caída del sistema / Interrupción del servicio / Denegación de servicio	Agotamiento de recursos
		Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso
Computadores y Laptops (12)	5	Desastres naturales	Ausencia de diseño antisísmico del edificio
		Fallas de origen físico	Ausencia de mantenimientos preventivos a los equipos
		Fallas de origen físico	Desgaste natural de partes
		Fallas de origen físico	Partes defectuosas de fábrica
		Fallas de origen físico	Presencia de polvo, suciedad
		Fallas de origen lógico	Contraseña del administrador conocida por otros
		Fallas de origen lógico	Acceso no autorizado
		Caída del sistema por agotamiento de recursos	Falta de límites y control en el uso de recursos
		Ataque lógico intencionado	Vulnerabilidad técnica en el sistema operativo
Impresoras (HW) (13)	3,33	Fallas de origen físico	Desgaste natural de partes
		Fallas de origen físico	Partes defectuosas de fábrica
		Caída del sistema / Interrupción del servicio / Denegación de servicio	Agotamiento de recursos
		Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso

Tabla 5.8 Amenazas y vulnerabilidades de los activos de información. Fuente: Autor

5.4.5 CÁLCULO DE PROBABILIDAD DE QUE LAS AMENAZAS Y VULNERABILIDADES OCURRAN

Una vez identificadas las amenazas y vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo.

Todo este proceso incluye calcular la posibilidad de la ocurrencia de amenazas y que tan fácil pueden ser explotadas las vulnerabilidades por las amenazas.

El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

5.5 EVALUACIÓN DEL RIESGO

Para realizar la evaluación del riesgo, se recomienda crear una escala para medir los niveles de riesgo. Los criterios que usualmente se recomiendan para esto son:

- Impacto económico del riesgo.

- Tiempo de recuperación de la empresa.
- Posibilidad real de ocurrencia del riesgo.
- Posibilidad de interrumpir las actividades de la empresa.

Una vez identificados los criterios, se debe elaborar una escala para realizar la evaluación y determinar los grados de importancia que representan las amenazas para la empresa. Se recomienda usar una escala de Likert para evaluar los criterios para la importancia del riesgo.

La evaluación del riesgo debe poder identificar los niveles de riesgo generalmente aceptables, aquellos riesgos cuyo nivel y estimación de daño es pequeño para la organización y puede aceptarlo como parte de su trabajo cotidiano y no se requiere de mayor acción.

5.5.1 CÁLCULO DEL RIESGO

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y

del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

Todo riesgo tiene dos factores: uno que expresa el impacto del riesgo si ocurriera y otro que expresa la probabilidad de que el riesgo ocurra.

El impacto del riesgo está basado en la tasación del riesgo. La probabilidad de que el riesgo ocurra se basa en las amenazas y vulnerabilidades y los valores que se le han calculado.

El método para el cálculo del riesgo trata de relacionar los factores del impacto económico de la amenaza y la probabilidad de ocurrencia de la amenaza. Primero se debe evaluar el impacto económico de la amenaza, para esto se puede utilizar

una escala de Likert. Luego se debe medir la posibilidad de ocurrencia de la amenaza, para esto se puede usar nuevamente una escala de Likert.

Posteriormente se debe calcular la medición del riesgo, multiplicando los valores obtenidos del impacto de la amenaza y la probabilidad de ocurrencia de la amenaza. Finalmente las amenazas pueden ordenarse, de acuerdo a su factor de exposición al riesgo. En la figura 5.3, se muestra la manera de realizar el cálculo del riesgo.

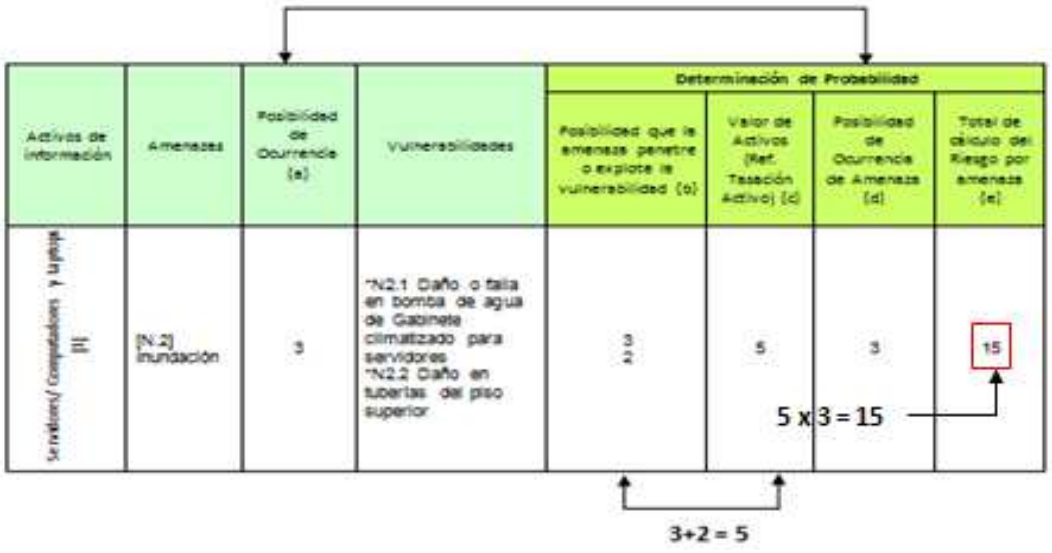


Figura 5.3 Cálculo del Riesgo

En la tabla 5.9, se presenta el análisis y evaluación del riesgo de los activos de información identificados en la empresa:

A&CGroup
Análisis y evaluación del riesgo

Niveles de Aceptación del Riesgo {E}		
Exposición al riesgo	Niveles	Objetivo
1 - 4	Aceptación	No aplica controles
5 - 10	Bajo	Aplica controles para llevar a nivel de aceptación
11 - 15	Medio	Aplica controles para llevar a nivel bajo
16 - 25	Alto	Aplica controles para llevar a nivel medio

								Impacto					
Activo	**Valor del Activo**	**Probabilidad más alta de ocurrencia de amenaza**	**Amenaza**	**Vulnerabilidad asociada**	**Probabilidad**	**Valor de Riesgo**	**Valor Riesgo del Activo (Probabilidad)**	**Económico**	**Tiempo Recuperación**	**Legal**	**Imagen**	**Interrupción de Actividades**	**Valor Total Riesgo (Impacto)**
Servidores (HW) (1)	5	4	Ataque lógico intencionado	Vulnerabilidad técnica en el sistema operativo	4	20	20	3	4	4	3	3	3,4
			Ataque lógico intencionado	Sistema operativo obsoleto	4	20							
			Ataque lógico intencionado	Ausencia de plan de parcheo de software	3	15							
			Fallas de origen físico	Desgaste natural de partes	3	15							

			Fallas de origen físico	Partes defectuosas de fábrica	3	15							
			Fallas de origen físico	Presencia de polvo, suciedad	3	15							
			Desastres naturales	Ausencia de diseño antisísmico del edificio	2	10							
			Fallas de origen físico	Ausencia de mantenimientos preventivos a los equipos.	2	10							
			Fallas de origen lógico	Contraseña del administrador conocida por otros	2	10							
			Fallas de origen lógico	Acceso no autorizado	2	10							
			Caída del sistema por agotamiento de recursos	Falta de límites y control en el uso de recursos	4	10							
Socio, Auditores (P) (2)	5	3	Indisponibilidad del personal	Enfermedad	3	15	15	3	3	3	5	4	3,6

			Errores por omisión o desconocimiento	Empleados desmotivados	3	15							
			Ingeniería social	Desconocimiento de políticas y mejores prácticas de seguridad	3	15							
			Malware para dispositivos móviles	Dispositivos móviles sin software de protección	3	15							
File Papeles de Trabajo - documentos físicos (SI) (3)	5	4	Uso no previsto	Acceso no autorizado	3	15	15	3	3	5	4	4	3,8
			Uso no previsto	Ausencia de etiquetado (clasificación) de la información	4	10							
			Uso no previsto	Ausencia de procedimientos de manejo de información clasificada	4	10							
Registros SGS llenados (formato digital) (4)	5	4	Uso no previsto	Ausencia de etiquetado (clasificación) de la información	4	10	10	3	3	2	2	3	2,6

			Uso no previsto	Ausencia de procedimientos de manejo de información clasificada	4	10							
			Acceso no autorizado	Ausencia de permisos de acceso	2	10							
			Acceso no autorizado	Ausencia de revisión de privilegios	4	10							
			Escapes de información	Uso de dispositivos extraíbles (pen drives)	4	10							
			Escapes de información	Ausencia de control de contenidos transferidos en la red	4	10							
			Alteración de la información	Introducción de información errónea	2	10							
			Pérdida total o parcial	Permisos de acceso no controlados	2	10							
			Pérdida total o parcial	Ausencia de respaldos de información	2	10							

Servicio de correo electrónico (S) (5)	4,67	4	Uso no previsto	Errores (equivocaciones) de los usuarios	4	18,68	18,68	2	2	2	3	2	2,2
			Caída del sistema / Servicio no disponible / Denegación de servicio	Falta de límites y control en el uso de recursos	4	18,68							
			Escapes de información	Ausencia de control de contenidos transferidos en la red	4	18,68							
			Ataque lógico intencionado	Vulnerabilidad técnica en el sistema	4	18,68							
			Ataque lógico intencionado	Sistema obsoleto	4	18,68							
			Caída del sistema / Servicio no disponible / Denegación de servicio	Agotamiento de recursos	3	14,01							
			Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso	3	14,01							

Software ACL (SW) (9)	4,67	3	Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso	3	14,01	14,01	2	2	1	2	2	1,8
Red de área local e inalámbrica (COM) (6)	4,33	3	Fallas de origen físico	Desgaste natural de partes	3	12,99	12,99	2	3	2	2	3	2,4
			Fallas de origen físico	Partes defectuosas de fábrica	3	12,99							
			Caída del sistema / Interrupción del servicio / Denegación de servicio	Agotamiento de recursos	3	12,99							
			Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso	3	12,99							
Sistema META, SAFI (SW) (7)	4	3	Difusión de software dañino	Presencia de bases de datos de antivirus desactualizadas	3	12	12	2	2	1	2	2	1,8

			Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso	3	12							
Sitio web(S) (10)	3,67	4	Caída del sistema / Servicio no disponible / Denegación de servicio	Falta de límites y control en el uso de recursos	4	14,68	14,68	2	2	2	3	2	2,2
Personal administrativo (P) (8)	2,67	4	Errores por omisión o desconocimiento	Empleados desmotivados	4	10,68	10,68	1	3	2	2	2	2
			Indisponibilidad del personal	Enfermedad	3	8,01							
			Ingeniería social	Desconocimiento de políticas y mejores prácticas de seguridad	3	8,01							
Sistema de comunicación telefónica IP (11)	2,33	3	Fallas de origen físico	Desgaste natural de partes	3	6,99	6,99	2	3	2	4	3	2,8
			Fallas de origen físico	Partes defectuosas de fábrica	3	6,99							

			Caída del sistema / Interrupción del servicio / Denegación de servicio	Agotamiento de recursos	3	6,99							
			Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso	3	6,99							
Computadores y Laptops (12)	5	4	Desastres naturales	Ausencia de diseño antisísmico del edificio	2	10	15	2	3	2	4	3	2,8
			Fallas de origen físico	Ausencia de mantenimientos preventivos a los equipos	2	10							
			Fallas de origen físico	Desgaste natural de partes	3	15							
			Fallas de origen físico	Partes defectuosas de fábrica	3	15							
			Fallas de origen físico	Presencia de polvo, suciedad	3	15							

			Fallas de origen lógico	Contraseña del administrador conocida por otros	2	10							
			Fallas de origen lógico	Acceso no autorizado	2	10							
			Caída del sistema por agotamiento de recursos	Falta de límites y control en el uso de recursos	4	10							
			Ataque lógico intencionado	Vulnerabilidad técnica en el sistema operativo	4	10							
Impresoras (HW) (13)	3,33	3	Fallas de origen físico	Desgaste natural de partes	3	9,99	9,99	1	3	1	2	2	1,8
			Fallas de origen físico	Partes defectuosas de fábrica	3	9,99							
			Caída del sistema / Interrupción del servicio / Denegación de servicio	Agotamiento de recursos	3	9,99							

			Abuso de privilegios de acceso	Ausencia de revisiones periódicas de privilegios de acceso	3	9,99							

Tabla 5.9 Análisis y evaluación del riesgo

5.5.2 ESTRATEGIAS PARA EL TRATAMIENTO DEL RIESGO

Despues de realizar el análisis y la evaluación del riesgo, se debe pensar en qué acciones se van de tomar con esos activos que están sujetos a riesgos. Los riesgos revelados pueden manejarse con una serie de controles para la detección y la prevención.

Una vez que el riesgo se ha calculado, se debe iniciar un proceso de toma de decisiones con respecto al tratamiento del riesgo. Esta decisión suele estar influenciada por dos factores:

- El posible impacto si el riesgo se materializa.
- Qué tan frecuente puede suceder.

Estos factores dan una idea de la perdida que se puede esperar si el riesgo ocurriera y si nada se hiciera para mitigarlo.

Existen 4 estrategias para el tratamiento del riesgo, como se muestra en la figura 5.4, que son:

a) **Reducir:** Esto se realiza con la aplicación de contramedidas o salvaguardas, especificadas en los controles del Anexo A de la norma ISO 27001:2005.

b) **Evitar:** Consiste en cambiar las actividades o la manera de desempeñar una actividad en particular, para evitar la presencia del riesgo.

c) **Transferir:** Esta es una opción cuando para la compañía es difícil reducir o controlar el riesgo a un nivel aceptable. Existe una serie de mecanismos para transferir los riesgos a otra organización; por ejemplo, utilizar una aseguradora o una tercerización de servicios.

d) **Aceptar:** Consiste en asumir la responsabilidad de correr dicho riesgo, ya sea porque no se encuentran controles para mitigarlo o la implementación de controles tiene un costo mayor que las consecuencias del riesgo. Cuando la empresa toma esta decisión, deben documentar y definir con precisión el criterio de aceptación del riesgo, el mismo que debe ser aprobado por la gerencia de la firma.

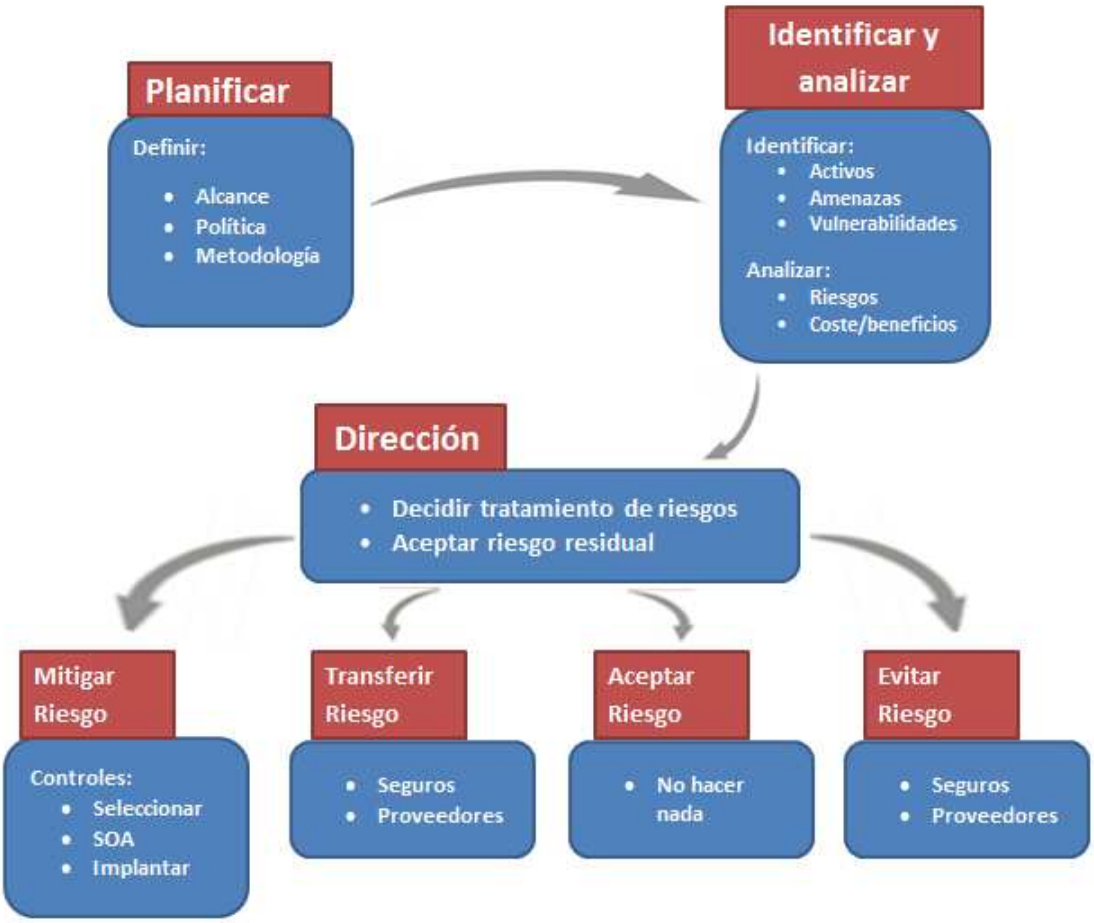


Figura 5.4 Opciones de tratamiento del riesgo. Fuente: ISO27001

CAPÍTULO 6

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1 PLAN DE TRATAMIENTO DEL RIESGO

Una vez que se realiza el proceso de identificar las opciones de tratamiento del riesgo y haberlas evaluado, la empresa debe decidir cuales objetivos de control y controles debe escoger para el tratamiento.

La selección de controles debe efectuarse tomando en cuenta el criterio establecido para la aceptación del riesgo, así como los requerimientos legales, reguladores y contractuales.

De acuerdo con la norma, en la cláusula 4.2.1 Establecer el SGSI, la selección de los objetivos de control y los controles debe ser del Anexo A.

El objetivo de este punto es tomar cual debe ser la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base al cuadro de análisis de riesgo y los criterios de valoración. A continuación, en la tabla 6.1 se muestra el plan de tratamiento para los activos y sus respectivos riesgos identificados.

Activos de información	Responsable de Activo	Amenazas	Vulnerabilidades	Opciones de Tratamiento del riesgo	
				Opción de tratamiento del riesgo	Controles o Salvaguardas
Servidores Socio, Auditores (P) (2)	Jefe TI	[N.1] Incendio	*N1.1 No contar con extintores o sistemas contra incendio *N1.2 Dejar papeles cerca de los equipos electrónicos *N1.3 Personas que fumen dentro de las instalaciones *N1.4 Cortocircuito por ausencia de seguridad eléctrica	Reducción	A.6.1.6 Contacto con autoridades **(N1.1)** A.9.1.1 Perímetro de seguridad física **(N1.1)** A.9.1.4 Protección contra amenazas externas y ambientales **(N1.1, N1.3, I1.1, I1.2, I1.3, N2.1, N2.2)** A.9.2.1 Instalación y protección de equipos A.9.2.2 Servicios públicos de soporte **(I1.2, I1.3)** A.11.3.3 Política de pantalla y escritorio limpio **(N1.2)** A.9.2.3 Seguridad del cableado **(N1.4)**
		[N.2] Inundación	*N2.1 Daño o falla en bomba de agua de Gabinete climatizado para servidores *N2.2 Daño en tuberías del piso superior		
		[N.*] Desastres naturales	*N3.1 Ausencia de diseño antisísmico del edificio		
	Responsable de la Dirección	[E.28] Indisponibilidad del personal (no intencionado)	*E28.1 Enfermedad *E28.2 Alteraciones en el orden publico		A.6.1.6 Contacto con autoridades **(E28.2)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(E28.2)** A.10.1.3 Segregación de tareas **(E28.1)**
		Intrusión en privacidad personal	*A40.1 Publicación de datos personales en redes virtuales de Internet *A40.2 Documentos con datos personales en los escritorios *A40.3 Ausencia de contraseñas en teléfonos inteligentes	Reducción	A.11.3.2 Equipo informático de usuario desatendido **(A40.1)** A.11.3.3 Política de pantalla y escritorio limpio **(A40.2)** A.15.1.4 Protección de los datos y de la privacidad de la información personal **(A40.1)** A.15.1.3 Salvaguarda de los registros de la organización **(A40.2)** A.11.7.1 Computación móvil y comunicaciones **(A40.3)**

		[A.30] Ingeniería social	*A30.1 Desconocimiento de políticas y mejores prácticas de seguridad *A30.2 Roles de seguridad no asignados o comunicados *A30.3 Ausencia de protecciones ante phishing y otros mecanismos de malware		
File Papeles de Trabajo -documentos físicos (SI)	Jefe de Administración	[N.1] Incendio	*No contar con extintores o sistemas contra incendio *Dejar papeles cerca de los equipos electrónicos *Personas que fumen dentro de las instalaciones		A.6.1.6 Contacto con autoridades **(N1.1)** A.9.1.1 Perímetro de seguridad física **(N1.1)** A.9.1.4 Protección contra amenazas externas y ambientales **(N1.1, N1.3, N2.1, N2.2, N3.1)** A.9.2.1 Instalación y protección de equipos A.11.3.3 Política de pantalla y escritorio limpio **(N1.2)** A.9.2.3 Seguridad del cableado **(N1.4)**
		[N.2] Inundación	*N2.1 Daño en tuberías de agua dentro de la oficina *N2.2 Daño en tuberías del piso superior		
		[N.*] Desastres naturales	*N3.1 Ausencia de diseño antisísmico del edificio		
		[I.5] Avería de origen físico	*I5.1 Degradación producto del paso del tiempo *I5.2 Contaminación física por polvo, manchas, líquidos		A.9.1.4 Protección contra amenazas externas y ambientales **(I5.1, I5.2)** A.11.3.3 Política de pantalla y escritorio limpio **(I5.2)** A.15.1.3 Salvaguarda de los registros de la organización **(I5.1)**
		[A.25] Robo	*A25.1 Sitios de almacenamiento desprotegidos		A.9.1.1 Perímetro de seguridad física **(A25.1)** A.9.1.2 Controles físicos de entrada **(A25.1)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(A25.1)**
		[A.26] Destrucción intencionada	*A26.1 Sitios de almacenamiento desprotegidos		A.9.1.1 Perímetro de seguridad física **(A26.1)** A.9.1.2 Controles físicos de entrada **(A26.1)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(A26.1)**

Carta de Representación / Informe Final / Registros del SGC llenados (D/SI) (4)	Jefe de Administración	[A.7] Uso no previsto	*A7.1 Ausencia de etiquetado (clasificación) de la información *A7.2 Ausencia de procedimientos de manejo de información clasificada *A7.3 Ausencia de acuerdos de confidencialidad para el personal	Reducción	A.7.2.1 Guías de clasificación **(A7.1)** A.7.2.2 Marcado y tratamiento de la información **(A7.1)** A.8.1.3 Acuerdos de confidencialidad **(A7.3)** A.10.1.1 Documentación de procedimientos operativos **(A7.2)** A.10.7.3 Procedimientos de manipulación de la información **(A7.2)**
		[A.11] Acceso no autorizado	*A11.1 Ausencia de sistema de identificación *A11.2 Ausencia de permisos de acceso *A11.3 Ausencia de revisión de privilegios *A11.4 Ausencia de controles de red *A11.5 Cambios de contraseña no regulados		A.10.6.1 Controles de red **(A11.5)** A.10.10.6 Sincronización de relojes **(A11.4)** A.11.1.1 Política de control de accesos **(A11.2)** A.11.2.1 Registro de usuarios **(A11.1, A11.2)** A.11.2.2 Gestión de privilegios **(A11.3)** A.11.2.3 Gestión de contraseñas de usuario **(A11.5)** A.11.2.4 Revisión de los derechos de acceso de los usuarios **(A11.3)** A.11.5.1 Procedimientos de registro en el terminal **(A11.1)** A.11.5.2 Identificación y autenticación de usuario **(A11.1)** A.11.5.3 Sistema de gestión de contraseñas **(A11.5)** A.11.5.5 Sesión inactiva **(A11.4)** A.11.5.6 Limitación del tiempo de conexión **(A11.4)** A.11.6.1 Restricción al acceso a la información **(A11.2)** A.12.3.1 Política sobre el uso de controles criptográficos **(A11.1)**

		[AE.14] Escapes de información	*E14.1 Escritorios desatendidos *E14.2 Uso de dispositivos extraíbles (pen drives) *E14.3 Ausencia de control de contenidos transferidos en la red *E14.4 Ausencia de control anti-malware		A.9.1.1 Perímetro de seguridad física **(E14.1)** A.10.7.1 Gestión de los medios removibles **(E14.2)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(E14.1)** A.10.10.2 Uso del sistema de monitoreo **(E14.3)** A.10.4.1 Medidas y controles contra software malicioso **(E14.4)** A.11.3.2 Equipo de usuario desatendido **(E14.1)** A.11.3.3 Política de pantalla y escritorio limpio **(E14.1)** A.12.5.4 Filtración de información **(E14.3)** A.11.7.1 Computación móvil y comunicaciones **(E14.3)**
		[E.19] Divulgación de información	*E15.1 Introducción de información errónea *E15.2 Degradación o corrupción de la información causado por agente externo		A.10.4.1 Controles contra software malicioso **(E15.2)** A.10.1.3 Segregación de tareas **(E15.1)** A.12.2.1 Validación de datos de entrada **(E15.1)** A.12.2.2 Control de procesamiento interno **(E15.2)**
		[E.19] Divulgación de información	*E19.1 Vulnerabilidad técnica en aplicaciones de soporte *E19.2 Indiscreción verbal *E19.3 Deterioro en red de comunicación de voz		A.9.1.1 Perímetro de seguridad física **(E19.2)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(E19.2)** A.10.7.3 Procedimientos de manejo de información **(E19.2)** A.10.8.1 Políticas y procedimientos para el intercambio de información y software **(E19.2)** A.12.6.1 Control de vulnerabilidades técnicas **(E19.1)** A.10.8.5 Sistemas de Información de Negocios **(E19.1)**
		[E.40] Pérdida total o parcial	*E40.1 Escritorios desatendidos *E40.2 Ausencia de sitios o repositorios seguros y centralizados para almacenar archivos digitales *E40.3 Permisos de acceso no controlados *E40.4 Ausencia de respaldos de información		A.8.3.3 Eliminación de derechos de acceso **(E40.3)** 10.7.3 Procedimientos de manipulación de la información **(E40.2)** 10.1.1 Documentación de procedimientos operativos **(E40.2)** A.10.5.1 Back-up o respaldo de la información **(E40.4)** A.11.1.1 Política de control

					de accesos **(E40.3)** A.11.3.3 Políticas de escritorios y pantallas limpias **(E40.1)**
Servicio de correo electrónico (S) (5)	Jefe de TI	[A.7] Uso no previsto	*A7.1 Errores (equivocaciones) de los usuarios *A7.2 Errores del administrador *A7.3 Desconocimiento de políticas de uso del servicio	Reducción	A.6.2.2 Requisitos de seguridad cuando sea trata con clientes **(A7.1)** A.8.1.3 Acuerdos de confidencialidad **(A7.3)** A.10.1.1 Documentación de procedimientos operativos **(A7.1, A7.2)** A.10.7.3 Procedimientos de manipulación de la información **(A7.1)** A.11.1.1 Política de control de accesos **(A7.1)** A.15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información **(A7.3)** A.11.4.1 Política sobre el uso de servicios en red **(A7.3)**
		[E.24] Caída del sistema / Servicio no disponible / Denegación de servicio	*E24.1 Agotamiento de recursos *E24.2 Falta de límites y control en el uso de recursos *E24.3 Abuso en el uso de recursos *E24.4 Errores de configuración *E24.5 Falla en servicios dependientes *E24.6 Ausencia de enlace de internet *E24.7 Ataque intencionado de agente externo *E24.8 Presencia de spam u otro tipo de malware		A.10.3.1 Planificación de la capacidad **(E24.1, E24.2)** A.7.1.3 Uso aceptable de los activos **(E24.3)** A.10.10.2 Monitoreando el uso del sistema **(E24.3)** A.15.1.5 Prevención en el mal uso de los recursos de procesamiento de la información **(E24.3)** A.10.1.1 Documentación de procedimientos operativos **(E24.4)** A.10.6.2 Seguridad de los servicios de red **(E24.5)** A.10.2.1 Servicio de entrega (terceros) **(E24.6)** A.10.2.2 Monitoreo y revisión de los servicios de terceros **(E24.6)** A.11.4.6 Control de conexión a las redes A.12.6.1 Control de las vulnerabilidades técnicas **(E24.7)** A.11.4.4 Diagnostico remoto y configuración de protección de puertos **(E24.7)** A.10.4.1 Controles contra

					software malicioso **(E24.8)**
	Jefe de TI	[N.1] Incendio	*N1.1 No contar con extintores o sistemas contra incendio *N1.2 Dejar papeles cerca de los equipos electrónicos *N1.3 Cortocircuito por ausencia de seguridad eléctrica		A.6.1.6 Contacto con autoridades **(N1.1)** A.9.1.1 Perímetro de seguridad física **(N1.1)** A.9.1.4 Protección contra amenazas externas y ambientales **(N1.1, I1.1, I1.2, I1.3, N2.1, N2.2)** A.9.2.1 Instalación y protección de equipos A.9.2.2 Servicios públicos de soporte **(I1.2, I1.3)** A.11.3.3 Política de pantalla y escritorio limpio **(N1.2)** A.9.2.3 Seguridad del cableado **(N1.3)**
		[N.2] Inundación	*N2.1 Daño o falla en bomba de agua de Gabinete climatizado para servidores *N2.2 Daño en tuberías del piso superior		
		[N.*] Desastres naturales	*N3.1 Ausencia de diseño antisísmico del edificio		
		[I.*] Daño eléctrico	*I1.1 Ausencia de equipo regulador eléctrico *I1.2 Sobrecarga eléctrica *I1.3 Fluctuación eléctrica		
		[I.5] Fallas de origen físico	*I5.1 Ausencia de mantenimientos preventivos a los equipos. *I5.2 Maltrato a los equipos *I5.3 Desgaste natural de partes *I5.4 Partes defectuosas de fábrica *I5.5 Inadecuada climatización (demasiado calor, frío o humedad) *I5.6 Presencia de polvo, suciedad *I5.7 Vibraciones		A.6.2.1 Identificación de riesgos por el acceso de terceros **(I5.1)** A.6.2.3 Requisitos de seguridad en contratos de outsourcing **(I5.1)** A.9.2.4 Mantenimiento de equipos **(I5.1, I5.3, I5.4, I5.6)** A.10.1.1 Documentación de procedimientos operativos **(I5.2)** A.9.2.1 Instalación y protección de equipos: control de temperatura, control de humedad **(I5.5,**

					I5.7)
		[I.6] Corte prolongado de suministro eléctrico	*I6.1 Racionamientos eléctricos en el país *I6.2 Trabajos prolongados en redes eléctricas externas		Acometida a red eléctrica de backup del Edificio **(I6.1, I6.2)** A.9.2.2 Servicios públicos de soporte **(I6.1, I6.2)**
		[E.24] Caída del sistema / Interrupción del servicio / Denegación de servicio	*E24.1 Agotamiento de recursos *E24.2 Falta de límites y control en el uso de recursos *E24.3 Abuso en el uso de recursos *E24.4 Errores de configuración *E24.5 Falla en servicios de red correlacionados *E24.6 Ausencia de enlace de internet *E24.7 Ausencia de controles ante spam, malware o agente externo *E24.8 Destrucción física de medios físicos de transporte de datos		A.10.3.1 Planificación de la capacidad **(E24.1, E24.2)** A.7.1.3 Uso aceptable de los activos **(E24.3)** A.10.10.2 Monitoreando el uso del sistema **(E24.2)** A.15.1.5 Prevención en el mal uso de los recursos de procesamiento de la información **(E24.3)** A.10.1.1 Documentación de procedimientos operativos **(E24.4)** A.10.6.2 Seguridad de los servicios de red **(E24.5)** A.10.2.1 Servicio de entrega (terceros) **(E24.6)** A.10.2.2 Monitoreo y revisión de los servicios de terceros **(E24.6)** A.11.4.6 Control de conexión a las redes **(E24.5)** A.11.4.4 Diagnostico remoto y configuración de protección de puertos **(E24.7)** A.10.4.1 Controles contra software malicioso **(E24.7)** A.9.2.3 Seguridad del cableado **(E24.8)**
		[A.4] Manipulación de la configuración	*A4.1 Ausencia de monitorización (log) / Logs incompletos *A4.2 Acceso no autorizado a los datos de configuración		A.10.10.1 Registro de la auditoria **(A4.1)** A.10.1.3 Segregación de deberes **(A4.2)** A.10.10.3 Protección de la información del registro **(A4.1)** A.10.10.4 Registros del administrador y operador **(A4.1)** A.11.1.1 Política de control de accesos **(A4.2)** A.11.2.2 Gestión de privilegios **(A4.2)**

		[A.5] Suplantación de la identidad del usuario	*A5.1 Controles ausentes o insuficientes de autenticación de usuarios p.e. firmas digitales *A5.3 Contraseñas débiles -fáciles de averiguar		A.10.9.2 Transacciones en línea **(A5.1)** A.11.2.3 Gestión de contraseñas de usuario **(A5.3)** A.11.3.1 Uso de contraseñas **(A5.3)**
Personal administrativo (P) (8)	Responsable de la Dirección	[E.28] Indisponibilidad del personal (no intencionado)	*E28.1 Enfermedad *E28.2 Alteraciones en el orden publico	Reducción	A.6.1.6 Contacto con autoridades **(E28.2)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(E28.2)** A.10.1.3 Segregación de tareas **(E28.1)**
		Intrusión en privacidad personal	*A40.1 Publicación de datos personales en redes virtuales de Internet *A40.2 Documentos con datos personales en los escritorios		A.11.3.2 Equipo informático de usuario desatendido **(A40.1)** A.11.3.3 Política de pantalla y escritorio limpio **(A40.2)** A.15.1.4 Protección de los datos y de la privacidad de la información personal **(A40.1)** A.15.1.3 Salvaguarda de los registros de la organización **(A40.2)**
		Suplantación de identidad	*A41.1 Comunicaciones expuestas a alteraciones o cambios en identidad		11.5.2 Identificación y autenticación del usuario **(A41.1)** 12.2.3 Integridad de mensajes **(A41.1)** 12.3.1 Política de uso de los controles criptográficos **(A41.1)**
		Asalto	*A42.1 Transitar en sitios peligrosos *A42.2 Utilizar servicio de transporte no confiable		Uso de servicio de transporte confiable **(A42.1, A42.2)**
		[A.29] Extorsión			
		[E.1] Errores por omisión o desconocimiento	*E1.1 Falta de entrenamiento en seguridad *E1.2 Roles de seguridad no asignados o comunicados *E1.3 Carencia de toma de conciencia en seguridad *E1.4 Empleados desmotivados		A.5.1.1 Documento de política de seguridad de la información **(E1.1)** A.6.1.2 Coordinación de la seguridad de la información **(E1.1)** A.8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales **(E1.2, A30.2)**

		[A.30] Ingeniería social	*A30.1 Desconocimiento de políticas y mejores prácticas de seguridad *A30.2 Roles de seguridad no asignados o comunicados *A30.3 Ausencia de protecciones ante phishing y otros mecanismos de malware		A.8.1.2 Selección y política de personal **(E1.3)** A.8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información **(E1.1, A30.1, E1.3)** A.8.2.3 Proceso disciplinario **(E1.3)** A.11.3.1 Uso de contraseñas **(A30.3)** A.13.1.1 Reportando los eventos en la seguridad de información **(E1.3)** A.13.1.2 Reportando debilidades en la seguridad de información **(E1.3)** A.13.2.1 Responsabilidades y procedimientos A.13.2.2 Aprendiendo de los incidentes en la seguridad de información **(E1.3)** A.10.4.1 Medidas y controles contra software malicioso **(A30.3)**
	Jefe TI	[E.1] Errores de los usuarios	*E1.1 Falta de capacitación en el uso de los sistemas *E1.2 Ausencia de soporte técnico a los sistemas y ausencia de procedimiento de operación y manejo *E1.3 Mecanismos ausentes de validación de datos de entrada *E1.4 Presencia de personal no calificado *		A.8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales **(E1.1)** A.8.1.2 Selección y política de personal **(E1.1, E1.4)** A.8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información **(E1.1)** A.10.1.1 Documentación de procedimientos operativos **(E1.2)** A.10.7.3 Procedimientos de manipulación de la información **(E1.2)** A.12.2.1 Validación de datos de entrada **(E1.3)** A.12.2.2 Control de procesamiento interno **(E1.3)** A.12.2.4 Validación de datos de salida **(E1.3)**
		[E.8] Difusión de software dañino	*E8.1 Falta de software antimalware *E8.2 Presencia de bases de datos de antivirus desactualizadas *E8.3 Mecanismos ausentes de validación de datos de entrada *E8.4 Errores en mantenimiento o ausencia de actualización periódica de programas		A.10.4.1 Medidas y controles contra software malicioso **(E8.1, E8.2)** A.12.6.1 Control de las vulnerabilidades técnicas **(E8.4, E8.5)** A.12.2.1 Validación de datos de entrada **(E8.3)**

			*E8.5 Presencia de vulnerabilidades técnicas en los programas		
		[AE.14] Escapes de información	*A14.1 Escritorios desatendidos *A14.2 Uso de dispositivos extraíbles (pen drives) *A14.3 Ausencia de control de contenidos transferidos en la red *A14.4 Ausencia de control anti-malware		A.9.1.1 Perímetro de seguridad física **(E14.1)** A.10.7.1 Gestión de los medios removibles **(E14.2)** A.9.1.3 Seguridad de oficinas, despachos y recursos **(E14.1)** A.10.10.2 Uso del sistema de monitoreo **(E14.3)** A.10.4.1 Medidas y controles contra software malicioso **(E14.4)** A.11.3.2 Equipo de usuario desatendido **(E14.1)** A.11.3.3 Política de pantalla y escritorio limpio **(E14.1)** A.12.5.4 Filtración de información **(E14.3)**
		[AE.15] Alteración de la información	*A15.1 Introducción de información errónea *A15.2 Degradación o corrupción de la información		A.10.4.1 Controles contra software malicioso **(E15.2)** A.10.1.3 Segregación de tareas **(E15.1)** A.12.2.1 Validación de datos de entrada **(E15.1)** A.12.2.2 Control de procesamiento interno **(E15.2)**
Sitio web (S) (10)	Jefe TI	[E.24] Caída del sistema / Servicio no disponible / Denegación de servicio	*E24.1 Agotamiento de recursos *E24.2 Falta de límites y control en el uso de recursos *E24.3 Abuso en el uso de recursos *E24.4 Errores de configuración *E24.5 Falla en servicios dependientes *E24.6 Ausencia de enlace de internet *E24.7 Ataque intencionado de agente externo *E24.8 Presencia de spam u otro tipo de malware	Reducción	A.10.3.1 Planificación de la capacidad **(E24.1, E24.2)** A.10.10.2 Monitoreando el uso del sistema **(E24.3)** A.15.1.5 Prevención en el mal uso de los recursos de procesamiento de la información **(E24.3)** A.10.1.1 Documentación de procedimientos operativos **(E24.4)** A.10.6.2 Seguridad de los servicios de red **(E24.5)** A.10.2.1 Servicio de entrega (terceros) **(E24.6)** A.10.2.2 Monitoreo y revisión de los servicios de terceros **(E24.6)** A.11.4.6 Control de conexión

					a las redes A.12.6.1 Control de las vulnerabilidades técnicas **(E24.7)** A.11.4.4 Diagnostico remoto y configuración de protección de puertos **(E24.7)** A.10.4.1 Controles contra software malicioso **(E24.8)**
		[A.4] Manipulación de la configuración	*A4.1 Ausencia de monitorización (log) / Logs incompletos *A4.2 Acceso no autorizado a los datos de configuración		A.10.10.1 Registro de la auditoria **(A4.1)** A.11.1.1 Política de control de accesos **(A4.2)** A.11.2.2 Gestión de privilegios **(A4.2)**
		[A.6] Abuso de privilegios de acceso	*A6.1 Ausencia de revisiones periódicas de privilegios de acceso *A6.2 Asignación de privilegios no controlada		A.10.10.1 Registro de la auditoria **(A6.2)** A.11.2.2 Gestión de privilegios **(A6.2)** A.11.2.4 Revisión de los derechos de acceso de los usuarios **(A6.1)**
		[A.11] Acceso no autorizado	*A11.1 Ausencia de sistema de identificación *A11.2 Ausencia de permisos de acceso *A11.3 Ausencia de revisión de privilegios *A11.4 Ausencia de controles de red *A11.5 Cambios de contraseña no regulados		A.11.1.1 Política de control de accesos **(A11.2)** A.11.2.1 Registro de usuarios **(A11.1, A11.2)** A.11.2.2 Gestión de privilegios **(A11.3)** A.11.2.3 Gestión de contraseñas de usuario **(A11.5)** A.11.2.4 Revisión de los derechos de acceso de los usuarios **(A11.3)** A.11.5.1 Procedimientos de registro en el terminal **(A11.1)** A.11.5.2 Identificación y autenticación de usuario **(A11.1)** A.11.5.3 Sistema de gestión de contraseñas **(A11.5)** A.11.5.5 Sesión inactiva **(A11.4)** A.11.5.6 Limitación del tiempo de conexión **(A11.4)**

					A.11.6.1 Restricción al acceso a la información **(A11.2)**
		[I.5] Fallas de origen físico	*I5.1 Ausencia de mantenimientos preventivos a los equipos. *I5.2 Maltrato a los equipos *I5.3 Desgaste natural de partes *I5.4 Partes defectuosas de fábrica *I5.5 Inadecuada climatización (demasiado calor, frío o humedad) *I5.6 Presencia de polvo, suciedad *I5.7 Vibraciones		A.6.2.1 Identificación de riesgos por el acceso de terceros **(I5.1)** A.6.2.3 Requisitos de seguridad en contratos de outsourcing **(I5.1)** A.9.2.4 Mantenimiento de equipos **(I5.1, I5.3, I5.4, I5.6)** A.10.1.1 Documentación de procedimientos operativos **(I5.2)** A.9.2.1 Instalación y protección de equipos: control de temperatura, control de humedad **(I5.5, I5.7)**

Tabla 6.1 Plan de Tratamiento del riesgo. Fuente: Autor

Después de implementar las decisiones relacionadas con el tratamiento del riesgo, siempre habrá un residuo de ese mismo riesgo. Ese riesgo que queda, después de implantar el plan de tratamiento, se denomina riesgo residual.

Si el riesgo residual se considerara inaceptable, deben tomarse decisiones para resolver su caso, por ejemplo instaurar más controles para reducirlo a un nivel aceptable.

En ciertas circunstancias reducir los riesgos a un nivel aceptable puede no ser posible o financieramente aceptable, por lo tanto se puede optar por aceptar el riesgo. Todos los riesgos residuales que se hayan aceptado deben ser documentados y aprobados por la gerencia.

La declaración de aplicabilidad es un documento, cuyo objetivo es incluir todos los objetivos de control y controles escogidos del Anexo A que son relevantes para el SGSI de la organización y aplicables al mismo. En la tabla 6.2, se muestra la declaración de aplicabilidad de A&CGroup.

También debe detallar la exclusión de cualquier objetivo de control y controles del Anexo A, con la respectiva explicación.

Controles Anexo A de ISO 27001:2005	Objetivo de control	Descripción	Aplica	Justificación
A5. Política de Seguridad				
A5.1	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes	Documento de gestión de seguridad de la información	Si	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes
A5.2		Revisión de la política	Si	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A6. Organización de la seguridad de la información				
A6.1 Organización interna				
A6.1.1	Manejar la seguridad de la información dentro de la organización.	Compromiso gerencial hacia la Seguridad de la Información.	Si	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A6.1.2		Coordinación de la Gestión de la Información	Si	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A6.1.3		Definición de responsabilidades	Si	Se deben definir claramente las responsabilidades de la seguridad de la información.
A6.1.4		Autorización para Instalaciones de Gestión de Información	Si	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A6.1.5		Acuerdos de confidencialidad	Si	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A6.1.6		Contacto con autoridades	Si	Se debe mantener los contactos apropiados con las autoridades relevantes.
A6.1.7		Contacto con grupos de interes especial	Si	Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

A6.1.8		Revisión independiente de la seguridad de la información	Si	El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.
A6.2 Entidades Externas				
A6.2.1	Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.	Identificacion de riesgos relacionados con entidades externas	Si	Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A6.2.2		Tratamiento de la seguridad cuando se trabaja en clientes	Si	Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A6.2.3		Tratamiento de la seguridad en contratos con terceras personas	Si	Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.
A.7 Gestión de Activos				
A.7.1 Responsabilidad por los activos				
A.7.1.1	Lograr y mantener la protección apropiada de los activos organizacionales.	Inventarios de activos	Si	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2		Propiedad de los activos	Si	Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de a organización.
A.7.1.3		Uso aceptable de los activos	Si	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificacion de la informacion				
A.7.2.1	Asegurar que a información reciba un nivel de protección apropiado.	Lineamientos de clasificacion	Si	La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2		Etiquetado y manejo de la informacion	Si	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.
A.8 Seguridad de los recursos humanos				
A.8.1 Antes del empleo				

A.8.1.1	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.	Roles y responsabilidades	Si	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2		Selección	Si	Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3		Terminos y condiciones de empleo	Si	Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 Durante el empleo				
A.8.2.1	Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.	Gestion de responsabilidades	Si	La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2		Capacitacion y educacion en seguridad de la informacion	Si	Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3		Proceso disciplinario	Si	Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo				
A.8.3.1	Asegurar que los empleados, contratistas y terceros salgan de una organización	Responsabilidades de terminacion	Si	Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2		Devolucion de activos	Si	Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.

A.8.3.3	o cambien de empleo de una manera ordenada.	Eliminacion de derechos de acceso	Si	Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 Seguridad fisica y ambiental				
A.9.1 Areas seguras				
A.9.1.1	Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.	Perimetro de seguridad fisica	Si	Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2		Controles de entrada fisicos	Si	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3		Seguridad de oficinas, habitaciones y medios	Si	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4		Protección contra amenazas externas y ambientales	Si	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5		Trabajo en áreas seguras	Si	Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6		Areas de acceso público, entrega y carga	Si	Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 Seguridad del Equipo				
A.9.2.1	Evitar la pérdida, daño, robo o compromiso de los activos y lainterrupción de las actividades de la organización	Ubicación y protección del equipo	Si	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2		Servicios públicos	Si	El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
A.9.2.3		Seguridad en el cableado	Si	El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4		Mantenimiento de equipo	Si	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5		Seguridad del equipo fuera del local	Si	Se debe aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6		Eliminacion segura o re-uso del equipo	Si	Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.

A.9.2.7		Traslado de propiedad	Si	Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
A.10 Gestion de las comunicaciones y operaciones				
A.10.1 Procedimientos y responsabilidades operacionales				
A.10.1.1	Asegurar la operación correcta y segura de los medios de procesamiento de la información	Procedimientos de operación documentados	Si	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2		Gestión de cambio	Si	Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3		Segregacion de deberes	Si	Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4		Separación de los medios de desarrollo y operacionales	Si	Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestion de la entrega del servicio de terceros				
A.10.2.1	Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.	Entrega del servicio	Si	Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2		Monitoreo y revision de los servicios de terceros	Si	Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.
A.10.2.3		Manejar los cambios en los servicios de terceros	Si	Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la reevaluación de los riesgos.
A.10.3 Planeacion y aceptacion del sistema				
A.10.3.1	Minimizar el riesgo de fallas en los sistemas.	Gestion de capacidad	Si	Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2		Aceptacion del sistema	Si	Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 Proteccion contra software malicioso y codigo movil				
A.10.4.1	Proteger la integridad del software y la información.	Controles contra software malicioso	Si	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2		Controles contra codigos moviles	Si	Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no autorizado

A.10.5 Respaldo (back-up)				
A.10.5.1	Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.	Back-up o respaldo de la informacion	Si	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 Gestion de seguridad de redes				
A.10.6.1	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.	Controles de red	Si	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2		Seguridad de los servicios de red	Si	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestion de medios				
A.10.7.1	Evitar la divulgación, modificación, eliminación o destrucción noautorizada de los activos; y la interrupción de las actividades comerciales.	Gestion de los medios removibles	Si	Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2		Eliminacion de medios	Si	Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3		Procedimiento de manejo de la informacion	Si	Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4		Seguridad de documentacion del sistema	Si	Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de informacion				
A.10.8.1	Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.	Procedimientos y politicas de informacion y software	Si	Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2		Acuerdos de intercambio	Si	Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3		Medios fisicos en transito	Si	Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4		Mensajes electronicos	Si	Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5		Sistemas de informacion comercial	Si	Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electronico				
A.10.9.1	Asegurar la seguridad de	Comercio electronico	No	Nuestra Firma no maneja transacciones de comercio electrónico

A.10.9.2	los servicios de comercio electrónico y su uso seguro	Transacciones en linea	Si	Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no autorizado del mensaje.
A.10.9.3		Informacion disponible publicamente	Si	Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo				
A.10.10.1	Detectar actividades de procesamiento de información no autorizadas.	Registro de auditoria	Si	Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2		Uso del sistema de monitoreo	Si	Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3		Proteccion de la informacion del registro	Si	Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4		Registros del administrador y operador	Si	Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5		Registro de fallas	Si	Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6		Sincronizacion de relojes	Si	Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
A.11 Control de acceso				
A.11.1 Requerimiento comercial para el control de acceso				
A.11.1.1	Controlar acceso a la información	Politica de control de acceso	Si	Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestion del acceso del usuario				
A.11.2.1	Asegurar el acceso del usuario autorizado y evitar el acceso noautorizado a los sistemas de información.	Inscripcion del usuario	Si	Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2		Gestion de privilegios	Si	Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3		Gestion de la clave del usuario	Si	La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4		Revision de los derechos de acceso del usuario	Si	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario				
A.11.3.1	Evitar el acceso de usuarios no autorizados, y el compromiso o	Uso de clave	Si	Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2		Equipo de usuario desatendido	Si	Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido

A.11.3.3	robo de la información y los medios de procesamiento de la información.	Politica de pantalla y escritorio limpio	Si	Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes				
A.11.4.1	Evitar el acceso no-autorizado a los servicios en red.	Politica sobre el uso de servicios en red	Si	Los usuarios solo deben tener acceso a los servicios para los cuales han sido especificamente autorizados a usar
A.11.4.2		Autenticacion del usuario para conexiones externas	Si	Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3		Identificacion del equipo de red	Si	Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4		Proteccion del puerto de diagnostico remoto	Si	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5		Segregacion en redes	Si	Los servicios de informacion, usuarios y sistemas de informacion se deben segregar en las redes
A.11.4.6		Control de conexión de redes	Si	Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales
A.11.4.7		Control de routing de redes	Si	Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación				
A.11.5.1	Evitar acceso no autorizado a los sistemas operativos.	Procedimientos de registro en el terminal	Si	Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2		Identificacion y autenticacion del usuario	Si	Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
A.11.5.3		Sistema de gestion de claves	Si	Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4		Uso de utilidades del sistema	Si	Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5		Sesion inactiva	Si	Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6		Limitacion de tiempo de conexión	Si	Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e informacion				

A.11.6.1	Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.	Restriccion al acceso a la informacion	Si	Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2		Aislamiento del sistema sensible	Si	Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computacion movil y tele-trabajo				
A.11.7.1	Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.	Computacion movil y comunicaciones	Si	Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2		Tele-trabajo	Si	Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 Adquisicion, desarrollo y mantenimiento de los sistemas de informacion				
A.12.1 Requerimientos de sguridad de los sistemas				
A.12.1.1	Asegurar que la seguridad sea una parte integral de los sistemas de información.	Analisis y especificaciones de los requerimientos de seguridad	Si	Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones				
A.12.2.1	Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.	Validacion de data de insumo	Si	El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2		Control de procesamiento interno	Si	Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de 34 procesamiento o actos deliberados.
A.12.2.3		Integridad del mensaje	Si	Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4		Validacion de data de output	Si	Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptograficos				
A.12.3.1	Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.	Politica sobre el uso de controles criptograficos	Si	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2		Gestion clave	Si	Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
A.12.4 Seguridad de los archivos del sistema				
A.12.4.1	Garantizar la seguridad de los archivos	Control de software operacional	Si	Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.

A.12.4.2	del sistema	Proteccion de la data de prueba del sistema	Si	Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3		Control de acceso al codigo fuente del programa	Si	Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte				
A.12.5.1	Mantener la seguridad del software e información del sistema de aplicación	Procedimientos de control de cambios	Si	La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2		Revison tecnica de las aplicaciones despues de cambios en el sistema operativo	Si	Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3		Restricciones sobre los cambios en los paquetes de software	Si	No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4		Filtracion de informacion	Si	Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5		Desarrollo de outsourced software	Si	El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.
A.12.6 Gestion de vulnerabilidad tecnica				
A.12.6.1	Reducir los riesgos resultantes de la explotación de vulnerabilidad es técnicas publicadas.	Control de vulnerabilidades tecnicas	Si	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A.13 Gestion de incidentes en la seguridad de la informacion				
A.13.1 Reporte de eventos y debilidades en a seguridad de la informacion				
A.13.1.1	Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva	Reporte de eventos en la seguridad de la informacion	Si	Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2		Reporte de debilidades en la seguridad	Si	Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.

	oportuna.			
A.13.2 Gestion de inicidentes y mejoras en la seguridad de la informacion				
A.13.2.1	Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.	Responsabilidades y procedimientos	Si	Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2		Aprendizaje de los incidentes en la seguridad de la informacion	Si	Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3		Recoleccion de evidencia	Si	Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14 Gestion de la continuidad comercial				
A.14.1 Aspectos de la seguridad de la informacion de la gestion de la continuidad comercial				
A.14.1.1	Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o esastres en los sistemas de información y asegurar su reanudación oportuna.	Incluir seguridad de la informacion en el proceso de gestion de la continuidad del negocio	Si	Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2		Continuidad del negocio y evaluacion del riesgo	Si	Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3		Desarrollar e implementar planes de continuidad incluyendo seguridad de la informacion	Si	Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4		Marco referencial para la planeacion de la continuidad del negocio	Si	Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5		Prueba, mantenimiento y re-evaluacion de planes de continuidad comerciales	Si	Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15 Cumplimiento				
A.15.1 Cumplimiento con requerimientos legales				

A.15.1.1	Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad	Identificacion de legislacion aplicable	Si	Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2		Derechos de propiedad intelectual (IPR)	Si	Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3		Proteccion de los registros organizacionales	Si	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4		Proteccion de la data y privacidad de la informacion personal	Si	Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
A.15.1.5		Prevencion del mal uso de los medios de procesamiento de la informacion	Si	Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6		Regulacion de controles criptograficos	Si	Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento de las politicas y estandares de seguridad y el cumplimento tecnico				
A.15.2.1	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional .	Cumplimiento con las politicas y estandares de seguridad	Si	Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2		Chequeo de cumplimiento tecnico	Si	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoria de los sistemas de informacion				
A.15.3.1	Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría de los sistemas de información.	Controles de auditoria de sistemas de informacion	Si	Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2		Proteccion de las herramientas de auditoria de los sistemas de informacion	Si	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Tabla 6.2 Declaración de aplicabilidad. Fuente: Autor

6.2 POLÍTICAS

6.2.1 POLÍTICAS GENERALES

- Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
- Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
- Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
- El ingreso de las personas a la oficina será restringido con el uso de un mecanismo electrónico de control de accesos basado en lector de huellas dactilares y el software respectivo que validará el ingreso al personal enrolado en el sistema y que se encuentre autorizado para su ingreso.
- El acceso al cuarto de servidores estará limitado al responsable del área de Tecnología y Sistemas de Información, y en su ausencia, a la persona que se delegue. Para el ingreso se contará con un mecanismo electrónico de control de accesos basado en lector de huellas dactilares.
- Las contraseñas contendrán al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.
- Se debe mantener el escritorio del computador (Windows) limpio de información confidencial para la empresa.
- En caso de que necesite alejarse del computador inmediatamente, bloquear la sesión activa.

- Se debe usar un protector de pantalla ante inactividad del computador, el mismo que se establecerá para activarse luego de 2 minutos de inactividad.
- Los archivos creados deberán ser almacenados en la carpeta “Mis Documentos” la cual mantiene una copia sincronizada en el recurso “Documentos” del servidor.

6.2.2 POLÍTICAS DE SEGURIDAD A NIVEL FÍSICO

- El ingreso de las personas a la oficina será restringido con el uso de un mecanismo electrónico de control de accesos basado en lector de huellas dactilares y el software respectivo que validará el ingreso al personal enrolado en el sistema y que se encuentre autorizado para su ingreso.
- El ingreso a la segunda puerta de oficina se concederá sin restricción de días, al igual que al cuarto de servidores a las personas respectivamente autorizadas. Se utilizarán dos políticas de acceso 1) Acceso general y 2) Acceso a cuarto de servidores; se establecerán dos grupos de usuarios: General y Sistemas para controlar los accesos a los puntos de control.
- Todo el personal debe contar con su respectiva tarjeta de identificación. En estas tarjetas debe estar anotado la política de gestión integrada.
- El personal externo deberá recibir una tarjeta de visita. En estas tarjetas debe estar anotado la política de seguridad de la información y mecanismo para reportar incidentes de seguridad.

- Al ingresar o salir de la Oficina, todo el personal deberá registrar en el lector biométrico su ingreso o salida. En el evento de que un grupo de colaboradores llegue o salga de la Oficina, cada uno de ellos deberá registrar individualmente su ingreso o salida.
- El ingreso y salida de Files del cuarto de archivo deberá ser registrado en una bitácora por una persona del departamento de Administración. Solamente el personal de A&CGroup está autorizado a ingresar a esta área. El cuarto de archivo debe permanecer cerrado y luego de la jornada laboral cerrado con llave. El custodio de la llave será el Responsable del área de Administración.
- El acceso al cuarto de servidores estará limitado al responsable del área de Tecnología y Sistemas de Información, y en su ausencia, a la persona que se delegue. Para el ingreso se contará con un mecanismo electrónico de control de accesos basado en lector de huellas dactilares.
- Se deberá contar con un sistema de detección de intrusos a efectos de controlar el acceso físico en horas no laborables.
- Se deberá mantener extintores contra fuego cerca del cuarto de servidores, del cuarto de archivo y área de trabajo de auditores y revisarse anualmente para su respectivo mantenimiento.
- Con el objetivo de proteger los activos de información físicos, se prohíbe el consumo de comidas y bebidas en los escritorios de trabajo donde se encuentren equipos de computación y/o documentos físicos.
- Se prohíbe el consumo de cigarrillos dentro de las áreas de trabajo de la oficina.

- Se designa al área de Recepción como punto de entrega y carga. El acceso a la oficina estará restringido al personal registrado en el sistema biométrico de control de accesos. Si un proveedor necesita ingresar para entregar suministros debe ser acompañado por un funcionario de la Firma.

6.2.3 POLÍTICAS DE SEGURIDAD A NIVEL LÓGICO

- Todo equipo con sistema operativo Windows tiene activo el firewall de comunicaciones para evitar infección y posibles ataques al computador.
- Todos los equipos con Windows cuentan con software antivirus.
- Todo archivo de dudosa procedencia se debe rechazar.
- Verificar que las definiciones (bases de datos) del software antivirus se mantengan actualizadas.
- No usar contraseñas similares para el acceso a sistemas abiertos, como por ejemplo: el de correo electrónico, foros, etc., a las que usa para la administración o acceso a equipos de la empresa.
- No conectarse a redes inalámbricas inseguras si se va a trabajar con información confidencial de la empresa.
- Las contraseñas contendrán al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.
- Al finalizar el primer semestre de cada año se solicitara el cambio de la contraseña de acceso al computador.

- No abrir el case del equipo. Esta actividad está reservada solo al personal de Soporte Técnico.

6.2.4 POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

- Las copias de respaldo de la información se realizaran dos veces en el día a intervalos definidos.
- Los respaldos se harán mediante la herramienta correspondiente y serán almacenados en una unidad de almacenamiento externo.
- Se deben realizar pruebas de restauración, al menos una vez al año.

6.2.5 POLÍTICAS DE MANTENIMIENTO DE EQUIPOS

- Antes de encender el computador asegúrese que se cuente con condiciones ambientales adecuadas.
- Al finalizar la jornada laboral se debe apagar el sistema haciendo uso de la opción “Apagar” y esperar hasta que el proceso finalice normalmente.
- Evitar tocar la pantalla de los computadores o laptops con los dedos, uñas u otro objeto.
- Cuando el laptop se encuentre cerrado evitar colocar carpetas o elementos encima del mismo.

- No consumir bebidas en los escritorios de trabajo donde se encuentren equipos de computación y/o documentos físicos.
- El equipo deber estar ubicado y protegido para reducir los riesgos de las amenazas y las oportunidades para el acceso no autorizado.
- Se deberá contar con protección ante fallas o interrupciones de energía mediante la utilización de UPS.
- Se debe contar con mantenimiento preventivo físico para los equipos que almacenan información en medio electrónico para permitir su disponibilidad e integridad.
- Los mantenimientos físicos programados a los equipos, se realizaran dentro de la oficina y bajo supervisión de una persona del departamento de TI.

6.2.6 POLÍTICAS DE USO DE SOFTWARE

- Los usuarios no deben instalar o intentar instalar programas, utilitarios o complementos para navegadores de internet. Esta actividad está reservada solo al personal de Soporte Técnico de la empresa.
- Está prohibido el uso de programas sin licencias no autorizadas por la empresa.
- Todo equipo de computación debe mantener en forma residente un antivirus instalado y las actualizaciones de las nuevas versiones, deben realizarse en línea.

CAPÍTULO 7

ANÁLISIS DE RESULTADOS

7.1 ESTRATEGIAS DE DIFUSIÓN

La última fase de un Sistema de Gestión de Seguridad de la Información consiste en la concientización y formación del personal, con el fin de crear en la empresa una cultura de seguridad mostrando la importancia de sus actividades y como ellos pueden contribuir al logro de los objetivos establecidos en el sistema.

La concientización y divulgación consiguen que el personal conozca qué actividades se están llevando a cabo y por qué se están realizando. Con ello se concede transparencia al proceso y se involucra a todo el personal.

Las estrategias utilizadas por A&CGroup para lograr esto son:

- Programa de capacitación en seguridad de la información.
- Campaña de concientización.

7.1.1 PROGRAMA DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El programa de capacitación consiste en un grupo de videos, divididos en cinco módulos que tratan los temas:

- Conceptos generales.
- Gestión de eventos e incidentes de seguridad.
- Documentación del sistema.
- Gestión de riesgos.
- Plan de evacuación.

Debajo de cada módulo, se encuentra una sección que contiene el acceso a una autoevaluación en línea referente al video visto previamente. Ver figura 7.1.

Una vez culminada la autoevaluación, los resultados serán enviados automáticamente por correo electrónico a la persona responsable de registrar los resultados obtenidos por los usuarios en cada prueba.

Figura 7.1 Programa de capacitación. Fuente: A&CGroup

7.1.2 CAMPAÑA DE CONCIENTIZACIÓN PARA EL PERSONAL

Otra estrategia de concientización utilizada es la campaña de concientización para el personal, la cual consiste en un grupo de fondos y protectores de pantalla, los cuales han sido configurados en cada equipo del personal.

Estos fondos contienen las políticas más relevantes, que deben tener muy en cuenta los usuarios para lograr mantener la seguridad de la información. Ver figura 7.2

Figura 7.2 Campaña de concientización. Fuente: A&CGroup

7.2 REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El reporte de incidentes tiene como finalidad asegurar que la información de los eventos y debilidades en la seguridad de la información, asociados con los sistemas de información, sea comunicada para así poder tomar una acción correctiva oportuna.

El objetivo de esta actividad es proveer un canal de comunicación para que el personal pueda dar a conocer los eventos o incidentes y asegurar el tratamiento de los mismos.

A continuación se indica cómo realizar esta actividad:

- Ingresar al sistema de reporte de incidentes, con el usuario y clave previamente establecido, ver figura 7.3.

Figura 7.3 Reporte de incidentes 1

- Dar clic en la pestaña Servicio al cliente, y seleccionar la opción Incidencias, como se muestra en la figura 7.4.

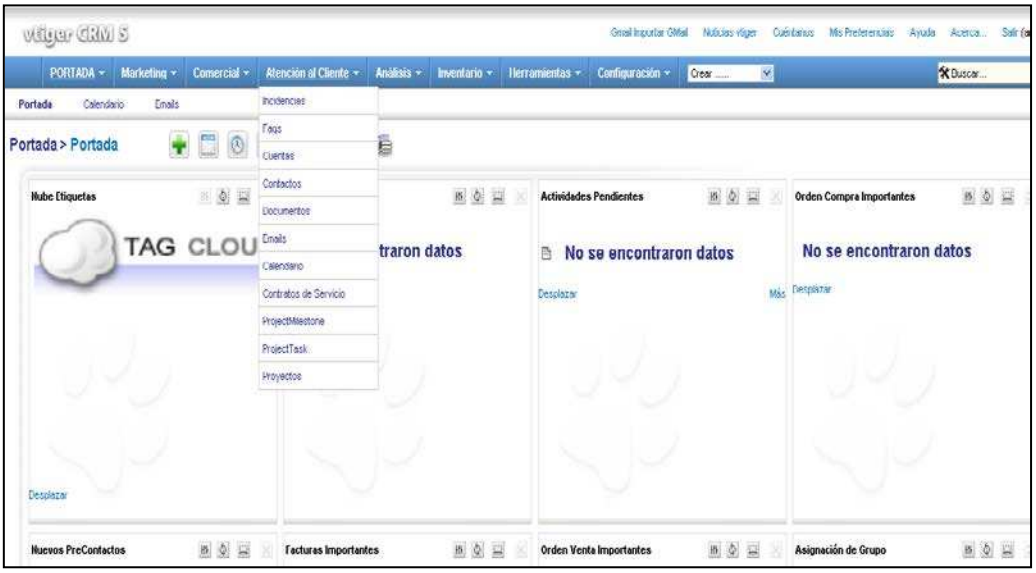


Figura 7.4 Reporte de incidentes 2

- Aparecerá una pantalla, seleccionamos el icono “Nuevo incidente”, ver figura 7.5.

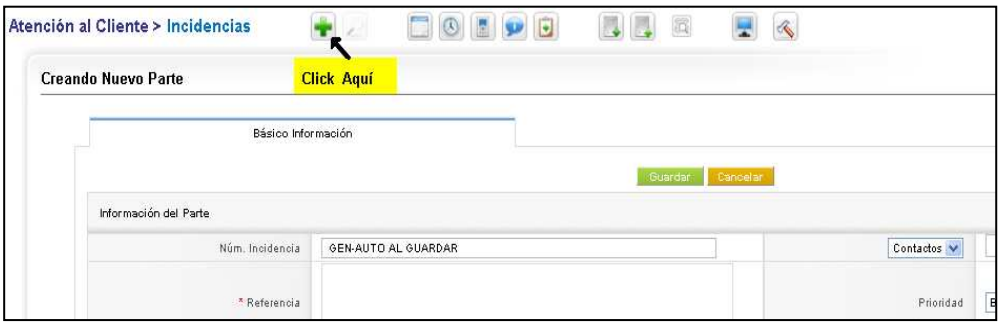


Figura 7.5 Reporte de incidentes 3

- Llenamos el formulario con las especificaciones del incidente a reportar y damos clic en guardar, como se muestra en la figura 7.6.

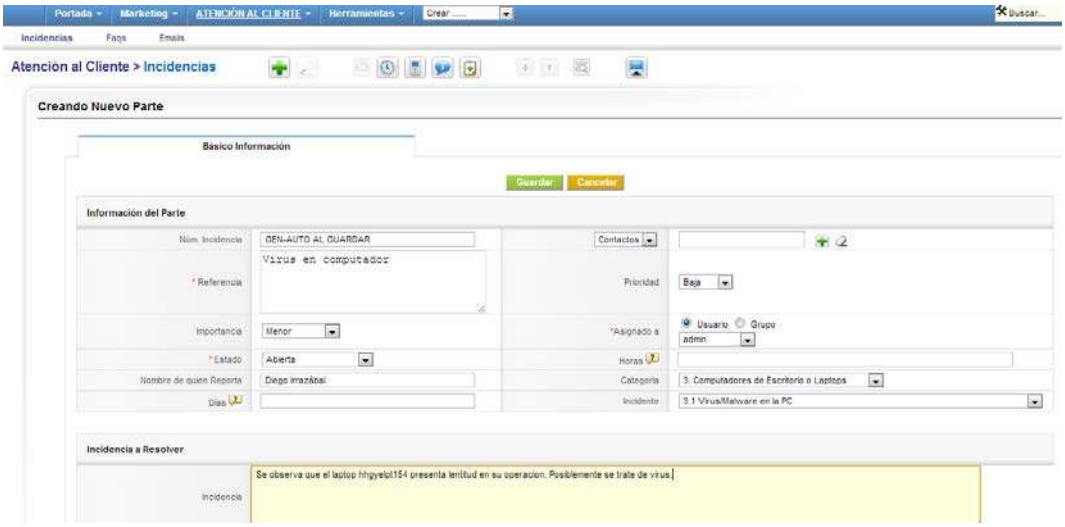


Figura 7.6 Reporte de incidentes 4

Este procedimiento se debe realizar cada vez que se presente algún tipo de incidente de seguridad, de esta manera se podrá tener un mayor control de la cantidad de incidentes que se reportan y la cantidad a los que se les da el respectivo tratamiento.

CONCLUSIONES

1. Debido a que en las organizaciones es primordial la optimización de recursos, el establecimiento del alcance del sistema de gestión de seguridad de la información se convierte en una actividad muy importante ya que delimita el campo de acción y el uso de recursos.
2. Es importante establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia.
3. La adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que

se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos.

4. Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.
5. Una vez identificados los riesgos a los que están expuestos los activos de información, es necesario implementar controles o salvaguardas, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización. Es importante considerar que al momento de seleccionar los controles se debe realizar un análisis de costo beneficio ya que el costo de la implementación de un control no debe exceder la posible pérdida económica de no tener implementado el control.
6. Dentro del ciclo de un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001, se encuentra la mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales. Estos elementos aportan retroalimentación al Sistema posibilitando conocer el estado del mismo y aplicar acciones correctivas, si fuera el caso, que permitan el cumplimiento de los planes y objetivos

RECOMENDACIONES

1. La concientización de la compañía es un pilar fundamental de esta norma, por lo cual la organización debe poner mucho empeño en despertar el interés y compromiso de todos sus empleados.
2. Contar con personal clave dentro de la empresa y con las competencias exigidas por la Norma ISO 27001:2005 para evitar la contratación de consultorías externas, cuyo costo suele ser alto.
3. La organización debe tratar de facilitar las tareas operativas del sistema SGSI, para lo cual necesita utilizar herramientas tecnológicas que automaticen ciertas tareas.

4. Se debe buscar el compromiso y soporte gerencial, de manera que el proyecto venga patrocinado desde arriba en la dirección, y sea esta la primera en dar ejemplo a la hora de aplicar aquellas medidas necesarias para definir, aplicar y mantener la seguridad en la empresa.
5. Es importante que se establezca un sistema de medición, que permita valorar la marcha del SGSI de modo global y particular, detectando desviaciones y cambios en la empresa que deban ser tratados para que el SGSI se mantenga operativo.

BIBLIOGRAFÍA

[1] Organización Internacional para la Estandarización (ISO).

http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm

[2] Norma ISO27001.

http://www.iso27000.es/iso27000.html

[3] Alberto G. Alexander. Diseño de un Sistema de Gestión de Seguridad de Información- Óptica ISO 27001:2005. Alfaomega, 2007

[4] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.