# DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BONOS Y DESCUENTOS S.A.S, A PARTIR DE LA NORMA ISO 27001:2013

SANDRA PAOLA MOLINA BRAVO
JACK DENNIS QUINTERO TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

# DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BONOS Y DESCUENTOS S.A.S, A PARTIR DE LA NORMA ISO 27001:2013

SANDRA PAOLA MOLINA BRAVO
JACK DENNIS QUINTERO TORRES

Proyecto de Grado – Proyecto aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Director de proyecto
Yolima Esther Mercado
Ingeniera de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

**CONTENIDO**

pág.

## LISTA DE CUADROS

pág.

## LISTA DE FIGURAS

pág.

## LISTA DE ANEXOS

pág.

## GLOSARIO

**Amenaza:** acción delictiva que atenta contra la seguridad de la información de una compañía y son consecuencia de la existencia de vulnerabilidades a nivel de hardware y software.

**APT "Advance Persistent Threat":** está enfocado a realizar ataques a redes corporativas o grandes compañías, estos ataques consisten en la extracción de datos de servidor, usuarios y contraseñas, y lo más grave, obtener accesos a las bases de datos, usuarios de clientes, contraseñas, dependiendo del tipo de negocio de la compañía las consecuencias podrían ser catastróficas.

**Black hackers:** son expertos informáticos con la capacidad de vulnerar un gran número de sistemas, estos se dedican e su gran mayoría a trabajar para empresas que buscan mitigar los huecos de seguridad que puedan vulnerar de alguna manera los delincuentes informáticos.

**Confidencialidad:** esta define que la información que pueda tener una compañía no puede ser revelada a terceros, es única y exclusivamente de uso corporativo o de los empleados de la compañía. Para lograr cumplir con este pilar, las compañías deben seguir estrictas normas de seguridad, dentro de ellas podemos encontrar restricciones de correos electrónicos, restricción de puertos USB en las estaciones de trabajo, ingreso exclusivo de bases de datos o información, solo a personal estrictamente necesario o autorizado.

**Control de Acceso:** Es un sistema de seguridad que permite el ingreso a diversos ambientes físicos, digitales, software, web, etc. Básicamente es un control a usuarios que se encuentran en una lista blanca y que permitirá o denegará su ingreso.

Actualmente existen diversos tipos de control de acceso, los podemos encontrar para sistemas de seguridad de ingreso, lectores de huella, lectores de proximidad, teclados de control, reconocimiento facial. También podemos encontrar controles de acceso en dispositivos de comunicación, estos últimos se encuentran sectorizados por perfiles o privilegios. (ACL).

**Cracker:** son expertos de la informática dedicados a cometer delitos informáticos, a la creación de programas, virus, malware que pueden vulnerar a las compañías, su objetivo en la mayoría de los casos es dañar los sistemas para de esta forma cobrar rescates o sumas cuantiosas de dinero para liberar los sistemas, también simplemente no buscan nada a cambio aparte de causar daños en los sistemas.

**Disponibilidad:** dentro de este pilar es prioritario que la información esté disponible durante los tiempos que sea necesario, relativamente 7x24 en caso que así se requiera, debe existir una constante comunicación entre las aplicaciones y los motores de bases de datos o lugares donde se resguarda la información. Para ellos es importante que la información o las bases de datos estén protegidas para que sea accesible todo el tiempo, para ellos es importante implementar restricciones y protecciones de seguridad, estas permitirán que la información esté disponible cuando los usuarios así lo requieran.

**Firewall:** herramienta de seguridad enfocada a proteger hardware y software dentro de una red privada, realiza filtrado de tráfico entrante y saliente a nivel de protocolo, usuarios, contenido, filtrado por geolocalización a nivel mundial, controles de acceso, entre otros. Previniendo de esta forma cualquier tipo de ataque informático.

**Hacker:** un Hacker es una persona con muy avanzados conocimientos de casi todos los frentes de la informática, desarrollo, comunicaciones, sistemas operativos, estas personas bien podrían vulnerar innumerables sistemas, muchos son conocidos como Hacker Éticos y son contratados por las compañías, otros como hemos visto anteriormente enfocan sus conocimientos a los delitos informáticos, de allí parten los términos para individualizar a cada uno como vimos en los términos anteriores.

**Integridad:** esta se refiere a que la información de una compañía en ningún caso debe ser modificada o alterada en ningún aspecto, debe ser estrictamente protegida y contar con implementaciones de seguridad que la resguardaran, para ello las compañías deben invertir es la protección de la misma, antivirus, firewall, restricción de usuarios, etc.

**Lammers:** son personas que, al contrario de los mencionados anteriormente, carecen de buenos conocimientos en la informática pero que presumen del mismo sin tenerlo, básicamente son individuos que tienen cierto conocimiento, pero no les interesa tener aprendizaje.

**Malware:** software malicioso, tiene múltiples objetivos, uno de ellos robar información personal, usuarios y contraseñas. Pueden ser descargados de alguna web no segura y con fines delincuenciales.

**Prehacker:** estos son individuos que se dedican al estudio de los dispositivos telefónicos, a partir de allí y con su gran conocimiento son capaces de construir dispositivos electrónicos que podrían interceptar comunicaciones o realizar llamadas prohibidas o simplemente utilizando saldos de otras personas para su beneficio propio.

**Ransomware**: es un tipo de Malware, su objetivo principal es impedir que un usuario pueda ingresar a sus archivos, una vez infectada la máquina, todos sus archivos

aparecerán encriptados y no será posible acceder. Esto se hace con el fin de pedir un rescate y liberar los archivos mencionados, estos pagos se piden en criptomonedas, de esta forma no podrán rastrear al atacante. Su contagio comúnmente es por medio de Spam que llega a nuestros correos electrónicos, al abrirlo el ransomware se descarga en la máquina.

**Riesgo:** es la posibilidad existente de que se presente un ataque a los sistemas de seguridad con efectos negativos a nivel informático y financiero.

**Spear Phishing:** esta es una modalidad de estafa muy común, consiste en que un delincuente informático crea una página idéntica a la de un banco con un dominio muy similar, de esta forma los usuarios a simple vista no la diferencian e ingresan a la página web, al ingresar sus datos de usuario y contraseña en la web falsa, estos son tomados inmediatamente por el delincuente y procede a ingresar a la real para sustraer su saldo o realizando compras, o transferencias. Esto también se ve en páginas de recargas virtuales donde las consecuencias también son altamente graves.

**Virus Informático:** un virus es un software malicioso cuyo objetivo es infectar y dañar archivos mediante un código malicioso, para que el virus sea efectivo, el usuario debe abrir estos ficheros, de esta manera el virus actuará según su fin.

**Vishing**: esta modalidad de delito consiste en que el delincuente informático genera una llamada a través de Vo/IP, es una grabación similar a la de las entidades bancarias, esto seguido de una persona hablando y suplantando a un funcionario de una entidad bancaria, esto con el fin de robar los datos de tarjetas de crédito y realizar de esta forma compras no autorizadas.

**Vulnerabilidad:** son fallas o brechas de seguridad existentes en un sistema de seguridad, estas son aprovechadas y explotadas por los delincuentes informáticos para causar daños a una compañía.

**White hackers:** similar a los anteriores, estos se dedican a estudiar y encontrar vulnerabilidades a los desarrollos, programas o sistemas operativos de las compañías, finalmente el objetivo es dar a conocer las fallas y dar sus posibles soluciones para que las compañías realicen las implementaciones correspondientes.

## RESUMEN

La empresa Bonos y Descuentos S.A.S ha sido creada el 4 de enero de 2021, se dedica al Marketing y publicidad de productos turísticos en general, paquetes turísticos y otros servicios en específico es una de sus principales funciones. Bonos y Descuentos S.A.S. por ser una empresa nueva a un no cuenta con SGSI en donde se establezcan políticas, procedimientos y controles con el fin de disminuir los riesgos a los que está expuesta la información de la empresa.

Para mitigar los riesgos de la seguridad de información se presentará el diseño de un SGSI basado en la norma ISO 27001:2013. Dentro del proceso se realizará un análisis de los activos de información, se encontrarán los riesgos, amenazas, vulnerabilidades y estado de seguridad en que se encuentren estos activos, se garantizará la selección de manera sistemática y adecuada de las políticas, controles y procedimientos necesarios para preservar la confidencialidad, integridad y disponibilidad de los activos de información de la empresa Bonos y Descuentos S.A.S.

La recolección de datos se realizará a través de visitas a la empresa, posteriormente se aplicará la metodología Margerit, controles del “SOA-Política de aplicabilidad”, anexo A de la Norma Internacional ISO 27001:2013 y finalmente se entregará el diseño del SGSI a Bonos y Descuentos S.A.S



**Palabras claves:** Confidencialidad, Disponibilidad, Integridad, ISO 27001:2013

## ABSTRACT

The company Bonos y Descuentos S.A.S has been created on January 4, 2021, it is dedicated to Marketing and advertising of tourist products in general, tourist packages and other specific services is one of its main functions. Bonos y Descuentos S.A.S Since it is a new company, it does not have an ISMS where policies, procedures and controls are established in order to reduce the risks to which the company's information is exposed.

To mitigate the risks of information security, the design of an ISMS based on the ISO 27001: 2013 standard will be presented. Within the process, an analysis of the information assets will be carried out, the risks, threats, vulnerabilities and security status will be found. in which these assets are located, the systematic and adequate selection of the policies, controls and procedures necessary to preserve the confidentiality, integrity and availability of the company's information assets will be guaranteed.

The data collection will be carried out through visits to the company, subsequently the Margerit methodology will be applied, controls of the "SOA-Applicability Policy", annex A of the International Standard ISO 27001: 2013 and finally the design of the ISMS will be delivered to Bonos y Descuentos S.A.S.



**Keywords:** confidentiality, availability, integrity, ISO 27001: 2013

# INTRODUCCIÓN

Las organizaciones actuales dependen en gran medida de los sistemas de información para gestionar el negocio y ofrecer productos / servicios. Dependen de TI para el desarrollo, la producción y la entrega en diversas aplicaciones internas. La aplicación incluye bases de datos financieras, reserva de tiempo para empleados, asistencia técnica y otros servicios, acceso remoto a clientes / empleados, acceso remoto a sistemas de clientes, interacciones con el mundo exterior a través del correo electrónico, Internet, uso de terceros y proveedores subcontratados.

La seguridad de la información es necesaria como parte del contrato entre cliente y cliente. El marketing quiere una ventaja competitiva y puede generar confianza en el cliente. La alta dirección desea conocer el estado de las interrupciones de la infraestructura de TI o las infracciones de la información o los incidentes de información dentro de la organización. Los requisitos legales como la Ley de Protección de Datos, los derechos de autor, los diseños y la regulación de patentes y los requisitos reglamentarios de una organización deben cumplirse y protegerse adecuadamente. La protección de la información y los sistemas de información para cumplir con los requisitos comerciales y legales mediante la provisión y demostración de un entorno seguro a los clientes, la gestión de la seguridad entre proyectos de clientes competidores y la prevención de la fuga de información confidencial son los mayores desafíos para los sistemas de información

La información es un activo que, al igual que otros activos comerciales importantes, es valioso para una organización y, en consecuencia, debe protegerse adecuadamente. Cualquiera que sea la forma que adopte la información o los medios por los que se comparta o almacene, siempre se debe proteger adecuadamente, la información se puede almacenar electrónicamente, puede transmitirse a través de la red, puede mostrarse en videos y puede ser verbal, los ciberdelincuentes, los piratas informáticos, el software malicioso, los troyanos, los phishing y los spammers son las principales amenazas para nuestro sistema de información.

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

La empresa Bonos y Descuentos S.A.S., presenta diversas fallas de seguridad en varios de sus sistemas de hardware y software, pérdida de información, robo de información confidencial, interoperabilidad por ransomware, pérdida de prestigio, confidencialidad en las bases de datos de clientes y personal interno entre otros activos de información que se encuentran vulnerables a diversos ataques o fallas de los sistemas.

En una era de globalización, en la que la tecnología ha permitido impulsar el desarrollo de empresas, los datos y la información se convierten en activos esenciales en las organizaciones, que están expuestos a piratas informáticos, virus informáticos, ciberespionaje y fallas de infraestructura son algunos de los problemas que se enfrentan a diario, es por ello que el diseño de un SGSI es de vital importancia para Bonos y Descuentos S.A.S.

La ciberseguridad es una preocupación creciente para las empresas de todos los tamaños, ya que las tácticas cada vez más sofisticadas de los ciberdelincuentes continúan perturbando las organizaciones. El conocimiento de Gartner proyectó que las empresas gastarán más de $123 mil millones en seguridad en 2020 y calculan que crecerán a $170,4 mil millones para 2022.

Sin embargo, los piratas informáticos aún logran comprometer los datos y sistemas corporativos con relativa facilidad y de forma regular. Esto se debe a que las organizaciones continúan sin tener conciencia de la seguridad cibernética y utilizan prácticas deficientes que hacen que sus datos estén desprotegidos y sean vulnerables a robos y violaciones.

El problema al que se enfrentan las organizaciones se ha agravado aún más por la operación de fuerzas de trabajo remotas, la creciente brecha de habilidades de ciberseguridad y el crecimiento de dispositivos conectados y de Internet de las cosas (IoT) que son particularmente vulnerables a los ciberataques.

La pandemia de COVID-19 en curso también ha tenido un impacto importante en la seguridad cibernética. Las estafas en línea aumentaron más del 400% en marzo de 2020 en comparación con los meses anteriores, según el bufete de abogados internacional Reed Smith, mientras que Google reveló que estaba bloqueando más de 18 millones de correos electrónicos de malware y phishing relacionados con COVID-19 todos los días.

Las estadísticas de ciberseguridad como estas son importantes para ayudar a las personas y organizaciones a comprender los desafíos y riesgos que enfrentan. Los conocimientos sobre ciberseguridad también son vitales para comprender los errores de seguridad comunes, como dejar datos desprotegidos y usar contraseñas débiles, que hacen que las organizaciones sean vulnerables a las infracciones. Es importante que los usuarios y los líderes empresariales tomen nota de las estadísticas de ciberseguridad, mientras que las organizaciones deben implementar procesos de capacitación que generen conciencia, prevención y mejores prácticas en su cultura.

En 2020, los investigadores de ESET observaron varios ataques dirigidos exclusivamente a entidades colombianas, que en conjunto han sido denominadas Operación Spalax. Estos ataques continúan y se centran tanto en instituciones gubernamentales como en empresas privadas, especialmente en las industrias energética y metalúrgica. Los atacantes dependen del uso de troyanos de acceso remoto, lo más probable es que realicen actividades de ciberespionaje.

ESET observó al menos 24 direcciones IP diferentes en uso durante la segunda mitad de 2020. Estos probablemente son dispositivos comprometidos que actúan como proxies para sus servidores C&C. Esto, combinado con el uso de servicios DNS dinámicos, significa que su infraestructura nunca se queda quieta. Hemos visto al menos 70 nombres de dominio activos en este período de tiempo, y registran nuevos de forma regular, dice Matías Porolli, investigador de ESET que investigó a Spalax[1].

Colombia ha acelerado su proceso de digitalización en los últimos años. La transformación digital brinda a Colombia la oportunidad de diversificar sus actividades desde una economía basada en productos básicos a una economía de servicios de alto valor agregado. La seguridad digital se ha convertido en un desafío en el país debido al rápido ritmo del proceso de transformación digital. La pandemia ha afectado a una gran cantidad de sectores e industrias en Colombia. Como consecuencia de las drásticas medidas tomadas por el gobierno local para frenar la propagación del virus, incluidas las medidas de permanencia en casa, la adopción del trabajo a distancia aumentó casi un 400% en el primer semestre de 2020 en comparación con los dos años anteriores. Como resultado, las empresas y las personas ahora están más expuestas y son más vulnerables a los ciberataques.

Si bien las empresas colombianas han realizado importantes inversiones en ciberseguridad en los últimos años, la demanda de ciberseguridad adicional aumentó con la llegada de la pandemia COVID-19. Al cierre del primer trimestre de 2020, la demanda de servicios de ciberseguridad había aumentado en un 40% en

[1] ESET SECURITY REPORT. Latinoamérica 2018. [Sitio web]. [Consulta: 14 de abril 2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Colombia (según la Cámara Colombiana de Informática y Telecomunicaciones). Según informó el Centro Cibernético de la Policía Nacional de Colombia, el primer semestre de 2020 registró un aumento del 59% en las denuncias de delitos informáticos en comparación con el mismo período del año anterior. Esta amenaza animó a las empresas del sector tecnológico a incrementar su integración de la ciberseguridad en el proceso de digitalización.

En 2019, Colombia se encontraba entre los países de América Latina más atacados por los ciberdelincuentes. La ciberseguridad se ha convertido en un tema frecuente de preocupación política para Colombia. El gobierno propuso a través del documento CONPES 3701, buscar los lineamientos nacionales en políticas de ciberseguridad. Con el objetivo principal del desarrollo de una estrategia nacional que contrarreste el aumento de amenazas informáticas al proceso de digitalización en Colombia.

Las entidades colombianas están implementando sus propias políticas de seguridad de TI para prevenir ciberataques. Colombia fue el más alto en la región para empresas con políticas de ciberseguridad implementadas en 2019, para Bonos y Descuentos S.A.S. es apremiante el diseño de un Sistema de Gestión de la seguridad de la información para eliminar o minimizar el impacto de las amenazas y vulnerabilidades relacionadas con la seguridad de los activos de información de la empresa. Al hacerlo, el Sistema de Gestión de Seguridad de la Información (SGSI) protegerá la capacidad para su funcionamiento, permitirá que las aplicaciones implementadas en los sistemas de TI tengan un funcionamiento seguro, protegerá los datos que la empresa recopila y utiliza, por último, salvaguardar los activos tecnológicos usados en Bonos y Descuentos S.A.S[2].

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo un SGSI basado en la Norma internacional ISO 27001:2013 puede ayudar en la seguridad de la información a la empresa Bonos y Descuentos S.A.S.?

[2] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional de Confianza y Seguridad Digital. [Sitio Web]. Colombia (2020). pp. 16-26, 34– 44. [Consulta: 14 de abril 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

# 2 JUSTIFICACIÓN

La información se encuentra entre los activos más importantes de una empresa, la información es valiosa y debe protegerse adecuadamente, mucha gente todavía no tiene idea de la importancia de la seguridad de la información para las empresas, muchos gerentes tienen la idea errónea de que su información es completamente segura y está libre de amenazas, por mucho que una empresa tome medidas para proteger su propiedad intelectual, es importante dejar de lado la creencia de que es imposible que alguien acceda a sus datos.

Con el avance de las tecnologías, los ciberataques se están renovando rápidamente, e incluso antes de que se den cuenta, es posible que una empresa ya esté en riesgo, es por eso que se debe tener mucho cuidado con la información confidencial.

Un ciberataque puede causar problemas graves y daños incalculables a una empresa pequeña o grande, muchas empresas pequeñas y medianas tienden a descubrir que no son un objetivo potencial y, por lo tanto, no necesitan invertir en la industria de la seguridad de datos. Debido a la falta de protección de estos sistemas, muchos de los ataques exitosos fueron dirigidos a empresas de estos tamaños.

Las pérdidas en las grandes empresas debido a los ataques suelen tener una conmoción más impactante incluso por la cantidad de material robado, pero en las empresas más pequeñas, esta acción puede significar más que unas pocas pérdidas: puede declarar el fin del negocio, la filtración o el robo de información importante puede generar problemas financieros que lleven a la quiebra de la empresa.

La seguridad cibernética sólida requiere un SGSI construido sobre tres pilares: personas, procesos y tecnología, al diseñar un SGSI, se puede proteger la información, aumentar la resistencia a los ataques cibernéticos y reducir los costos asociados con la seguridad de la información, gracias al enfoque de análisis y evaluación de riesgos de un SGSI, las empresas pueden reducir los costos invertidos en agregar indiscriminadamente capas de tecnología defensiva que podrían no funcionar.

Es por ello que la empresa Bonos y Descuentos S.A.S. requiere el diseño de un SGSI basado en la norma ISO 27001:2013, para proteger y gestionar la información de la empresa a través de una gestión de riesgos eficaz[3].

[3] ISO/CEI 27001:2013. [Sitio web]. Information technology — Security techniques — Information security management systems — Requirements. [Consulta: 25 de mayo 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

# 3 OBJETIVOS

## 3.1 OBJETIVOS GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Bonos y Descuentos SAS, a partir de los lineamientos de la norma ISO 27001:2013, para el aseguramiento de los activos de información.

## 3.2 OBJETIVOS ESPECÍFICOS

- Evaluar la brecha de seguridad, comparando los controles existentes de la empresa frente a los controles del “SOA - Declaración de aplicabilidad” de la Norma Internacional ISO 27001:2013, para la identificación del nivel de madurez de los controles que tiene la empresa respecto al cumplimiento que exige la norma.

- Elaborar un inventario, análisis y valoración de riesgos de los activos de información de la empresa Bonos y Descuentos SAS, a través de la Metodología Magerit, para la valoración de los riesgos e identificación de las amenazas y vulnerabilidades de los activos de información.

- Construir la declaración de controles a aplicar dentro de la empresa, por medio del “SOA – Declaración de aplicabilidad” de la Norma Internacional ISO 27001:2013, para generar el plan de tratamiento de riesgos.

- Proponer las políticas y controles de seguridad a los activos de información a partir de los dominios de seguridad propuestos en el anexo A de la Norma Internacional ISO 27001:2013, para el mejoramiento en la seguridad de la información.

.

# 4 MARCO REFERENCIAL

## 4.1 MARCO TEÓRICO

4.1.1 Dominio de los sistemas de información. Los sistemas de información se han definido como un término colectivo que se refiere a una serie de áreas de aplicación, incluida la integración empresarial, la traducción al lenguaje natural, la información geográfica. El conjunto central de fenómenos que define el campo de los sistemas de información se ha definido como que incluye capacidades de tecnología de la información (TI), el artefacto de TI, las prácticas de TI, el uso y el impacto, en el nivel más amplio, se ha definido y explicado el dominio de los sistemas de información como un sistema compuesto por personas y computadoras que procesa o interpreta información.

- **Enfoque ontológico**

La teoría se entiende dentro de los sistemas de información como de naturaleza amplia, para abarcar marcos, modelos, o el cuerpo de conocimiento. El carácter ontológico de los tipos de teoría ha sido articulado en cinco categorizaciones: análisis, explicación, predicción, explicación y predicción y diseño y acción, estas categorizaciones brindan a los investigadores un lenguaje para describir los diversos componentes de la teoría.

- **Enfoque epistemológico**

Para explorar cómo se puede construir la teoría y qué métodos de investigación se pueden utilizar, observamos que la discusión en esta área a menudo contrasta los puntos de vista positivista e interpretivista, o los puntos de vista cuantitativo y puntos de vista cualitativos.

- **Enfoque sociopolítico**

Explorando dónde se ha desarrollado la teoría hasta la fecha, encontramos que ha habido un sorprendentemente bajo número de teorías (es decir, menos de media docena) que, cuando se desarrollaron, se originaron únicamente en el área de los sistemas de información. Otras teorías tienen áreas de origen que incluyen tanto sistemas de información como una disciplina de referencia, mientras que el resto se origina únicamente de otra disciplina[4].

[4] GREGOR, Shirley. La naturaleza de la teoría en los sistemas de información. Universidad Nacional de Australia. Canberra. 2006, vol. 30, nro. 3, pp. 611-642

La seguridad de la información es un fenómeno dentro del dominio de los sistemas de información porque involucra personas que protegen la información que reside en las computadoras, que son todos elementos comunes consistentes con sistemas de información. Desde el punto de vista de los sistemas de información, la seguridad de la información se refiere con la protección de la información.

La seguridad de la información solía ser puramente técnica, sin embargo, ha evolucionado con el tiempo para mantenerse al día con cambios en computadoras y redes. El objetivo de la información la seguridad implica preservar la confidencialidad, integridad y disponibilidad de la información comercial, además, el objetivo de la seguridad de la información es salvaguardar la continuidad del negocio y reducir el deterioro del negocio al limitar el efecto de la seguridad incidentes. En otra contribución, se afirmó que el objetivo de la seguridad de la información era confidencialidad, integridad, disponibilidad y no repudio de la información.

La seguridad cibernética es diferente a la seguridad de la información, aunque ellos son muy diferentes, el término seguridad cibernética parece usarse indistintamente con el término información seguridad en la literatura académica. La seguridad cibernética trasciende los límites de la seguridad de la información para incluir la defensa de la información y también a las personas, la meta y los objetivos generales de seguridad de la ciberseguridad son la disponibilidad, integridad y confidencialidad de los activos de una organización, incluidas las redes, la infraestructura, la información y personal.

La seguridad de la información es un proceso consciente o subconsciente en el que las personas y las organizaciones intentan para crear recursos viables de forma sostenible, a partir de la información. Lo hacen aplicando controles adecuados a proteger la información de amenazas, de acuerdo con los objetivos para el uso de esa información. Esto entonces resulta en recursos sostenibles. La seguridad de la información se centra en qué protección se brinda a información y qué uso puede ofrecer esa información protegida a las organizaciones[5].

[5] VON SOLMS, Rossouw. Gestión de la seguridad de la información versión 3 el código de prácticas para la gestión de la seguridad de la información. *Gestión de la información y seguridad informática*. 1998, nro 80, pp. 224-225.

## 4.2 MARCO CONCEPTUAL

4.2.1 Pilares de la seguridad de la información. La información es un recurso valioso para cualquier empresa en este mundo digital. Debido a la dura competencia en los negocios, debe proporcionar su información con la mayor seguridad posible para no ofrecer a sus competidores ninguna forma de ventaja. La seguridad de la información es, por lo tanto, primordial para su negocio para garantizar que ninguna cantidad de información se vea comprometida.

La información enviada a través de redes en línea es vulnerable a ataques maliciosos. Por lo tanto, es necesario crear un sistema de información seguro para salvaguardar los datos vitales. La construcción de un sistema seguro sigue cinco pilares esenciales.

4.2.2 Cinco pilares a considerar al proteger la información. Confidencialidad, Integridad de datos e información, Disponibilidad, Autenticidad y No repudio.

- **Confidencialidad**

La confidencialidad es la parte más vital de la seguridad de la información. Si la información o la transmisión de datos es a través de la red, debe usar un lenguaje codificado que solo pueda ser descifrado por el remitente y el receptor de la información. Los terceros no deberían poder descifrar los datos de ninguna manera. Las personas adecuadas solo deben ver información muy confidencial.

- **Integridad de datos e información**

Se supone que la información enviada debe permanecer siempre en su naturaleza original. No debe modificarse durante el proceso de transmisión. La manipulación o modificación por parte de agentes no autorizados no es algo que deba permitirse. Un sistema de seguridad de la información eficiente proporciona un método para garantizar que los datos no se manipulen. Por ejemplo, muchas empresas y negocios utilizan firmas hash, lo que permite verificar la no manipulación de la información recibida.

- **Disponibilidad**

La disponibilidad de información significa que solo las personas calificadas que tienen acceso al sistema pueden obtener la información en cualquier momento que lo deseen sin fallas. Puede habilitarse teniendo un marco sólido que componga la infraestructura de TI. Asegura que el sistema permanezca completamente funcional incluso durante situaciones adversas como la caída de la base de datos. Tener excelentes recursos asegura que se pueda acceder a la información de manera cómoda y oportuna. La forma típica de garantizar la disponibilidad de los datos es

tener equilibradores de carga que proporcionen una ausencia de fallas en los recursos del servidor.

- **Autenticidad**

Las medidas de autenticación evitan la suplantación de identidad y requieren que los usuarios proporcionen pruebas de que están autorizados para acceder al sistema y a los recursos. Es fundamental ya que establece la validez del tránsito de la información y su origen. La forma convencional de garantizar la autenticidad incluye el uso de contraseñas, nombres de usuario y datos biométricos confiables, entre otros.

- **No repudio**

Es un elemento crítico en la seguridad de la información, ya que confirma la entrega de datos al remitente. El receptor también puede verificar la identidad del remitente de la información. Entre los dos agentes, nadie puede negar el envío o la recepción de los datos. Significa que debería haber alguna forma de audibilidad. El sistema de seguridad de la información proporciona registros que se pueden abrir para proporcionar pruebas de quién envió y recibió los datos.

Las medidas adicionales no incluidas en los cinco pilares pero que también son esenciales incluyen:

- **Recuperación:** en escenarios en los que el sistema se vea comprometido, debe haber medidas para restaurar los datos a su forma original. Los recursos de respaldo lo hacen mejor

- **Auditabilidad**: proporciona un sistema en el que se detectan posibles amenazas a la seguridad y se toman las acciones de respuesta adecuadas. Se hace monitoreando el sistema para confirmar y registrar a todos aquellos que acceden a la información.

4.2.3 ¿Qué es un activo informático?. Casi todas las organizaciones poseen información que no les gustaría que se compartiera o publicitara. Ya sea que estos datos se mantengan en formato digital o físico, la disciplina de la Gestión de la seguridad de la información es fundamental para proteger los datos contra el acceso no autorizado o el robo.

4.2.4 Tipos de activos de información:

- **Documentación estratégica**: las empresas y las organizaciones de TI desarrollan y documentan objetivos estratégicos a largo plazo y tácticos a corto plazo que establecen sus metas y visión para el futuro. Estos valiosos documentos internos contienen secretos y conocimientos a los que los competidores pueden querer acceder.

- **Información de productos / servicios:** la información crítica sobre productos y servicios, incluidos los ofrecidos por la empresa y por TI, debe protegerse mediante la gestión de seguridad de la información. Esto incluye el código fuente de la aplicación desarrollada internamente, así como los datos o productos informativos que se venden a los clientes. Si su empresa vende un producto digital, necesitará seguridad de la información para garantizar que los piratas informáticos no puedan robar su producto y distribuirlo sin su consentimiento o conocimiento.

- **Propiedad intelectual / Patentes**: si su empresa genera propiedad intelectual, incluido el desarrollo de software, es posible que necesite controles de seguridad de la información para protegerla. Es posible que sus competidores quieran robar su código fuente y usarlo para realizar ingeniería inversa en un producto para competir con el suyo. Algunos países no hacen cumplir las leyes de derechos de autor o propiedad intelectual, por lo que es posible que no tenga ningún recurso si se permite que esto suceda.

- **Conocimientos patentados / secretos comerciales:** todas las organizaciones generan conocimientos patentados a lo largo del curso de sus actividades comerciales. Para las organizaciones de TI, ese conocimiento puede almacenarse en una base de conocimiento interna que sea accesible para los operadores de TI y el personal de soporte. Los secretos comerciales son conocimientos y conocimientos únicos que le dan a su empresa una ventaja competitiva. Si no los comparte abiertamente con su competencia, debe proteger los secretos comerciales y el conocimiento de propiedad mediante controles de administración de seguridad de la información.

- **Documentación del proyecto en curso**: la documentación del proyecto en curso consiste en los detalles documentados de los productos o servicios que están en proceso de lanzamiento. Si sus competidores descubren lo que está haciendo, es posible que intenten lanzar un producto o característica de la competencia más rápido de lo previsto e incluso podrían compararlo con su nuevo producto en un esfuerzo por excluirlo del mercado.

- **Datos de los empleados:** los departamentos de recursos humanos recopilan y conservan datos sobre sus empleados, incluidas revisiones de desempeño, historial de empleo, salarios y otra información. Estos registros

pueden contener información confidencial que un atacante cibernético podría utilizar para chantajear a sus empleados. Una organización de la competencia podría usar estos datos para identificar objetivos antes de intentar robar a sus empleados[6].

[6] PORTAL DE ISO 27000 EN ESPAÑOL. [Sitio web]. Glosario. [Consulta: 14 de abril 2021]. Disponible en:: http://www.iso27000.es/glosario.html#section10c

# 5 DISEÑO METODOLÓGICO

## 5.1 MODELO DE PROCESOS PHVA

Para el diseño del SGSI de Bonos y Descuentos S.A.S se fundó en la norma ISO 27001:2013, en donde la metodología que se adoptó fue el modelo de procesos (Planear – Hacer – Verificar – Actuar) PHVA.

Hoy en día es mejor adoptar un enfoque de procesos porque introduce una gestión horizontal que atraviesa las barreras entre las diferentes unidades funcionales y garantiza la eficacia de los SGSI al organizar, gestionar y controlar las actividades y las interacciones entre los procesos y entre las jerarquías funcionales de una organización.

- **Requisitos genéricos en todo el PHVA**

  - Requisitos de documentación
  - Responsabilidad de la administración - Revisión de la administración del SGSI
  - Mejora del SGSI

### 5.1.1 Fases del modelo de procesos PHVA

- **Planear: establecimiento del SGSI**

Esta fase de la ISO 27001 ayuda a una organización a establecer el alcance de los objetivos y controles del SGSI. Muchas empresas de todo el mundo se están hundiendo en los ciberataques. En la norma ISO 27001, la cláusula 4.2 determina el contexto de la organización. Al implementar la fase de planificación, debe analizar los problemas externos e internos de la empresa. La identificación de estos problemas realmente podría ayudar a su organización a implementar los procedimientos del SGSI ISO 27001 y eliminar los obstáculos. Los problemas externos son la lista de amenazas que podrían ser la parte externa de la organización, como los requisitos legales, económicos y políticos. Las cuestiones internas son la parte interna, como estructura organizativa, valores, culturas, infraestructura TIC, recursos disponibles, etc.

- **Hacer: implementar el SGSI**

Esta fase es donde una organización implementa y explota la política, los controles, el proceso y los procedimientos del SGSI. En la fase hacer, una organización crea

una evaluación de riesgos y evalúa las razones detrás de cada estructura. Deben preparar una serie de procedimientos indicando los riesgos y su tratamiento. Deben asegurarse de que los documentos de procedimientos y políticas estén disponibles y adecuadamente protegidos, distribuidos y almacenados en el sistema administrado. Los documentos de origen externo deben cubrir el alcance de SGSI 27001. Así es como se llevará a cabo la fase hacer.

- **Verificar: seguimiento y revisión del SGSI**

Esta fase cubre los controles de seguimiento, medición, análisis y evaluación dentro de la organización. Las personas responsables deben medir el desempeño de los procesos contra las políticas, objetivos y experiencia práctica en un procedimiento documentado establecido en la fase anterior. Los líderes responsables deberán presentar cualquier resultado, seguido de la aplicación de estos resultados de las políticas. Es la mejor manera de verificar dónde se han identificado, tratado, eliminado los problemas y dónde se requiere revisar y mejorar.

- **Actuar: actualizaciones y mejoras del SGSI**

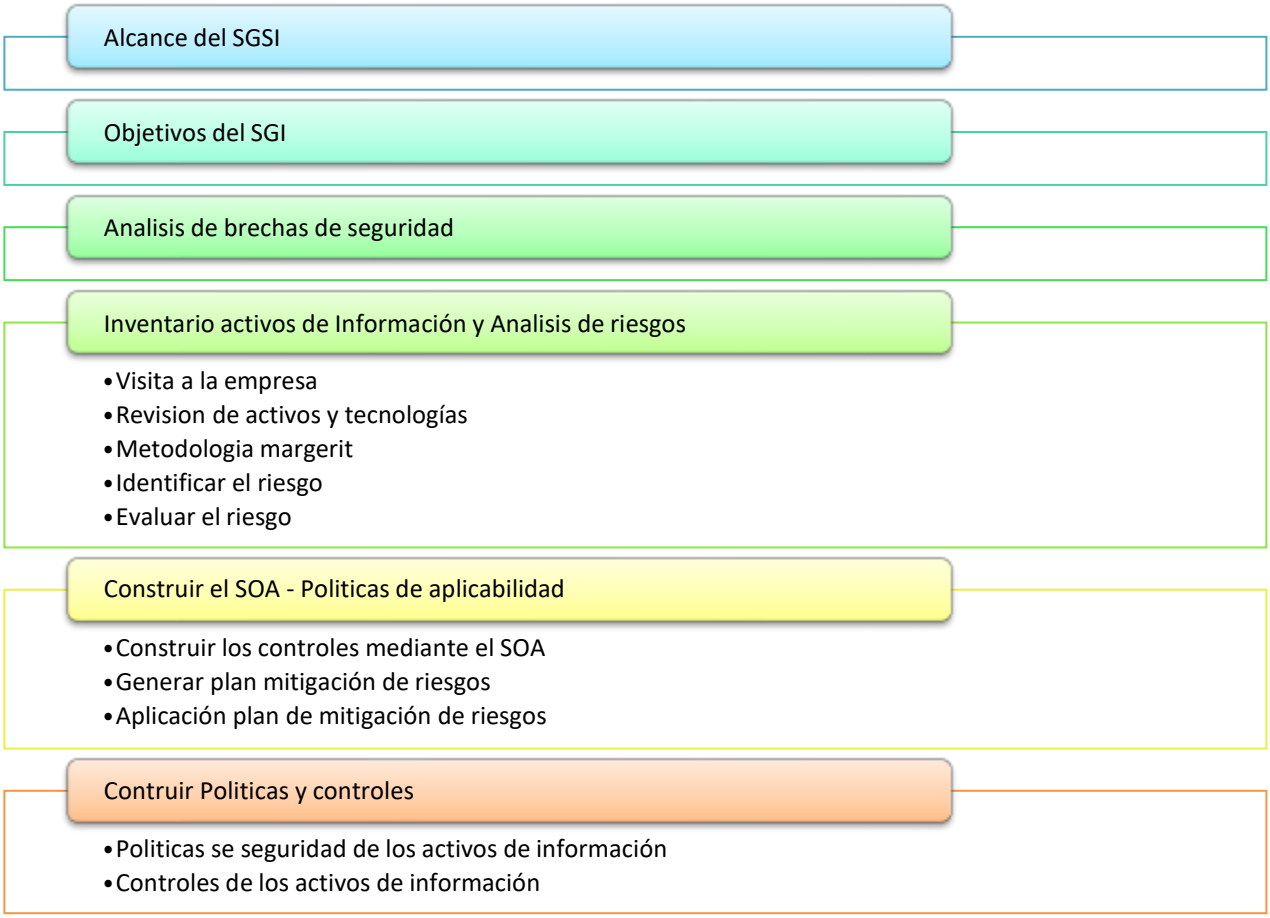
Una organización debe emprender acciones correctivas y preventivas basadas en los resultados de la auditoría interna y la revisión por la dirección del SGSI. Se puede nombrar un Director de Información que será responsable de monitorear y medir la seguridad de la información. El CIO debe actuar sobre cualquier hallazgo que se relacione con la violación de la seguridad de la información. La mejora continua es una parte integral de ISO 27001. La norma requiere que las organizaciones mejoren continuamente para eliminar más amenazas.

Ahora hemos reconocido los elementos PHVA y su aplicabilidad al SGSI ISO 27001. También comunica que todos los responsables deben participar en la implementación de ISO 27001. Todas las mejoras requieren actualización y documentación, respectivamente.[7]

Para este proyecto se realizará las dos primeras etapas (Planear – Hacer) como se indica en la Figura 1, en la fase de Planificación, de define el alcance y se identifican los objetivos del SGSI. Se realiza el análisis de brecha, métodos de análisis de riesgo y se produce un inventario apropiado de activos en riesgo con evaluaciones de riesgo clasificadas. La fase hacer se gestiona los riesgos mediante la generación de un plan de tratamiento de los riesgos, la construcción de los controles mediante el SOA, la creación de políticas y controles.

[7] UNIVERSIDAD NACIONAL DE COLOMBIA. [Sitio web]. Ciclo de control P.H.V.A. [Consulta: 14 de abril 2021]. Disponible en: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4010014/Contenidos/Capitulo1/Pages/1.4/148Ciclo_Control_PHVA.htm

Figura 1. Metodología para el diseño del SGSI




Fuente: “Elaboración propia”.

## 5.2 HERRAMIENTA METODOLÓGICA MARGERIT V3

Para el análisis y gestión de riesgos se utilizará la herramienta metodológica de MAGERIT V3. Este Manual ha sido concebido como un simple manual de referencia para identificar los Activos de una organización, evaluar las vulnerabilidades, las amenazas, los impactos de los activos de información y proponer decisiones de salvaguardas basadas sobre la identificación de Riesgos.

### 5.2.1 Objetivos de MAGERIT. La metodología tiene dos objetivos inmediatos:

- Examinar los riesgos que afectan a un sistema de información específico y su entorno relacionado.

- Sugerir las medidas que deban utilizar para prevenir, descubrir, reducir, Impedir o vigilar los riesgos investigados.

Como objetivo a más largo plazo, MAGERIT está preparando mecanismos de evaluación y certificación para seguridad de los sistemas de información.

### 5.2.2 Pasos para la implementación de MARGERIT

1. Identificación de activos. Son los activos propiedad de la Organización clasificados según su función.

2. Valoración de activos. Esta es la valoración asignada al activo según su criticidad y teniendo en cuenta las cinco dimensiones de la seguridad.

3. Identificación de amenazas. Estos son eventos que degradarían el valor de los activos.

4. Frecuencia. Se refiere a eventos que ocurren en un tiempo determinado.

5. Degradación. Así de gravemente se dañaría el activo si se materializan las amenazas.

6. Impacto. Este es un indicador de lo que puede suceder cuando ocurren amenazas.

7. Cálculo de riesgos. Esta es la probabilidad de que se materialicen amenazas al activo.

8. Identificación y evaluación de salvaguardas. Estas son las medidas precisas que se deben tomar para reducir el riesgo.

9. Cálculo de riesgo residual. Este es el riesgo que queda después de que se hayan aplicado las salvaguardias[8].

[8] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. [Sitio web]. MAGERIT versión 3 (versión español): Metodología de Análisis y gestión de riesgos de los sistemas de información. [Consulta: 14 de abril 2021]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

# 6 DESARROLLO DE LOS OBJETIVOS

## 6.1 DESARROLLAR UN ANÁLISIS DE BRECHA DE SEGURIDAD - DESARROLLO DE OBJETIVO 1

Un análisis de brechas de seguridad de la información es un paso crítico en el proceso de planificación de la continuidad del negocio y es una forma de Evaluación de riesgos. Un análisis de brechas está diseñado para determinar las diferencias entre el estado actual de la información seguridad dentro de una empresa y su estado ideal u óptimo. Estándares existentes, incluidos los desarrollados por el Organización Internacional de Normalización (ISO), Asociación de Control y Auditoría de Sistemas de Información (ISACA) y el Instituto Nacional de Estándares y Tecnología (NIST), representan pautas para el proceso de análisis de brechas, pero debe usarse como parte de un plan de seguridad empresarial integral. Este informe define un Análisis de brechas de seguridad de la información, analiza las posibles fallas y proporciona un plan de implementación paso a paso.

Un análisis de brechas relacionadas con la seguridad de la información identifica las brechas de seguridad de la información que pueden existir dentro de una organización mediante el examen de la postura actual de seguridad de la información de acuerdo con las mejores prácticas o estándares de la industria y regulaciones. Sin embargo, el análisis de brechas no es un proceso independiente. Es un paso, aunque estratégico, en el desarrollo de un Plan de continuidad del negocio (BCP) es un programa general para la seguridad organizacional.

Si bien existe una tendencia natural a centrarse en la seguridad de la red, garantizando una protección adecuada contra virus, gusanos, y otras formas de malware que se propagan a través de Internet, un análisis de brechas de seguridad de la información no está completo sin considerar otras exposiciones comunes, pero a menudo pasadas por alto, como la seguridad de las computadoras portátiles, la seguridad física, y seguridad del personal.

Una fuente de fallas de seguridad desde la invención de los dispositivos y su adopción en el interior empresas, las computadoras portátiles continúan siendo la fuente de importantes filtraciones de información que utilizan personas malintencionadas para robar identidades personales, hacer uso de información patentada o descubrir contraseñas para la red comercial interna

En casi todos los casos, se podría haber utilizado un análisis de brechas de seguridad de la información para revelar:

- La falta de protección de archivos con contraseña.

- La falta de cifrado de datos sensibles.
- No almacenar las computadoras portátiles en un lugar seguro.
- Uso no autorizado de laptops que contienen datos críticos para la empresa en redes no seguras y en redes no seguras.

De acuerdo al análisis de brecha de la empresa Bonos y Descuentos S.A.S, se evidenció que no cuenta con un nivel de madurez del modelo de seguridad y privacidad de la información aceptable, lo anterior debido que es una empresa nueva en el mercado y se encuentra implementando las respectivas políticas y controles de seguridad de la información[9].

En la Figura 2, se encuentran relacionados los valores de nivel de madurez con su respectivo puntaje y criterios.

Figura 2. Valoración de nivel de madurez

| NIVEL | PORCENTAJE | CRITERIO |
|---|---|---|
| INEXISTENTE | 0 | Requisito no implementado ni planeado; |
| INICIAL | 1-25 | El requisito está planeado pero no implementado; |
| REPETIBLE | 26-50 | El requisito se implementa solo parcialmente, por lo que no se pueden esperar efectos completos; |
| ADMINISTRADO | 51-75 | Se implementa el requisito, pero no se realizan mediciones, revisiones y mejoras; y |
| OPTIMIZADO | 76-100 | El requisito se implementa y la medición, revisión y mejora se realizan con regularidad. |

Fuente: Autoría propia

Según los controles del “SOA - Política de aplicabilidad” de la Norma Internacional ISO 27001:2013 en el Cuadro 1, se puede observar el Nivel de madurez con el que cuenta actualmente los controles de la empresa Bonos y Descuentos S.A.S. Para obtener el nivel de madurez se realizó dos visitas a las instalaciones de la empresa, donde se tuvo contacto con el gerente general llevando a cabo dos entrevistas para el levantamiento de la información, levantamiento de sus activos de información y el grado de cumplimiento actualmente de los controles y políticas de seguridad establecidas por la empresa.

[9] GUIJARRO, Hanna. IT GOVERNANCE EUROPEAN BLOG. [Sitio web]. 9 razones para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). [Consulta 25 de mayo 2021]. Disponible en: https://www.itgovernance.eu/blog/es/9-razones-para-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi

Cuadro 1. Porcentaje del cumplimiento de los controles y su Nivel de Madurez

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| **A.5** | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** | 0 | 0 - requisito no implementado ni planeado; |
| **A.5.1** | **Orientación de la dirección para la gestión de la seguridad de la información** | 0 | |
| A.5.1.1 | Políticas para la seguridad de la información | 0 | |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información | 0 | |
| **A.6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | 12,5 | 1-25 - el requisito está planeado pero no implementado; |
| **A.6.1** | **Organización interna** | 0 | |
| A.6.1.1 | Roles y responsabilidades para la seguridad de la información | 0 | |
| A.6.1.2 | Separación de deberes | 0 | |
| A.6.1.3 | Contacto con las autoridades | 0 | |
| A.6.1.4 | Contacto con grupos de interés especial | 0 | |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | 0 | |
| **A.6.2** | **Dispositivos Móviles y teletrabajo** | 25 | |
| A.6.2.1 | Política para dispositivos móviles | 0 | |
| A.6.2.2 | Teletrabajo | 50 | |
| **A.7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | 70 | 51-75 - se implementa el requisito, pero no se realizan mediciones, revisiones y mejoras; y |
| **A.7.1** | **Antes de asumir el empleo** | 80 | |
| A.7.1.1 | Selección | 80 | |
| A.7.1.2 | Términos y condiciones del empleo | 80 | |
| **A.7.2** | **Durante la ejecución del empleo** | 50 | |
| A.7.2.1 | Responsabilidades de la dirección | 70 | |
| A.7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | 0 | |
| A.7.2.3 | Proceso disciplinario | 80 | |

Cuadro 1. (Continuación)

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| **A.7.3** | **Terminación y cambio de empleo** | 80 | |
| A.7.3.1 | Terminación o cambio de responsabilidades de empleo | 80 | |
| **A.8** | **GESTIÓN DE ACTIVOS** | 48,7 | 26-50 - el requisito se implementa solo parcialmente, por lo que no se pueden esperar efectos completos; |
| **A.8.1** | **Responsabilidad por los activos** | 92,5 | |
| A.8.1.1 | Inventario de activos | 100 | |
| A.8.1.2 | Propiedad de los activos | 100 | |
| A.8.1.3 | Uso aceptable de los activos | 70 | |
| A.8.1.4 | Devolución de activos | 100 | |
| **A.8.2** | **Clasificación de la información** | 36,6 | |
| A.8.2.1 | Clasificación de la información | 30 | |
| A.8.2.2 | Etiquetado de la información | 40 | |
| A.8.2.3 | Manejo de activos | 40 | |
| **A.8.3** | **Manejo de medios** | 20 | |
| A.8.3.1 | Gestión de medios removibles | 20 | |
| A.8.3.2 | Disposición de los medios | 20 | |
| A.8.3.3 | Transferencia de medios físicos | 20 | |
| **A.9** | **CONTROL DE ACCESOS** | 13,5 | 1-25 - el requisito está planeado pero no implementado |
| **A.9.1** | **Requisitos del negocio para control de accesos** | 50 | |
| A.9.1.1 | Política de control de acceso | 0 | |
| A.9.1.2 | Acceso a redes y a servicios en red | 100 | |
| **A.9.2** | **Gestión de acceso de usuarios** | 0 | |
| A.9.2.1 | Registro y cancelación del registro de usuarios | 0 | |
| A.9.2.2 | Suministro de acceso de usuarios | 0 | |
| A.9.2.3 | Gestión de derechos de acceso privilegiado | 0 | |
| A.9.2.4 | Gestión de información de autenticación secreta de usuarios | 0 | |
| A.9.2.5 | Revisión de los derechos de acceso de usuarios | 0 | |
| A.9.2.6 | Retiro o ajuste de los derechos de acceso | 0 | |

Cuadro 1. (Continuación)

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| **A.9.3** | **Responsabilidades de los usuarios** | 0 | 1-25 - el requisito está planeado pero no implementado |
| A.9.3.1 | Uso de información de autenticación secreta | 0 | |
| **A.9.4** | **Control de acceso a sistemas y aplicaciones** | 4 | |
| A.9.4.1 | Restricción de acceso a la información | 10 | |
| A.9.4.2 | Procedimiento de ingreso seguro | 10 | |
| A.9.4.3 | Sistema de gestión de contraseñas | 0 | |
| A.9.4.4 | Uso de programas utilitarios privilegiados | 0 | |
| A.9.4.5 | Control de acceso a códigos fuente de programas | 0 | |
| **A.10** | **CRIPTOGRAFIA** | 0 | 0 - requisito no implementado ni planeado; |
| **A.10.1** | **Controles criptográficos** | 0 | |
| A.10.1.1 | Política sobre el uso de controles criptográficos | 0 | |
| A.10.1.2 | Gestión de llaves | 0 | |
| **A.11** | **SEGURIDAD FÍSICA Y DEL ENTORNO** | 52,15 | 51-75 - se implementa el requisito, pero no se realizan mediciones, revisiones y mejoras |
| **A.11.1** | **Áreas seguras** | 56,6 | |
| A.11.1.1 | Perímetro de seguridad física | 80 | |
| A.11.1.2 | Control de accesos físicos | 80 | |
| A.11.1.3 | Seguridad de oficinas, recintos e instalaciones | 80 | |
| A.11.1.4 | Protección contra amenazas externas y ambientales | 40 | |
| A.11.1.5 | Trabajo en áreas seguras | 40 | |
| A.11.1.6 | Áreas de despacho y carga | 80 | |
| **A.11.2** | **Equipos** | 47,7 | |
| A.11.2.1 | Ubicación y protección de los equipos | 40 | |
| A.11.2.2 | Servicios de suministro | 80 | |
| A.11.2.3 | Seguridad del cableado | 80 | |
| A.11.2.4 | Mantenimiento de equipos | 70 | |
| A.11.2.5 | Retiro de activos | 40 | |

Cuadro 1. (Continuación)

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| A.11.2.6 | Seguridad de activos y equipos fuera de la oficina | 30 | 51-75 - se implementa el requisito, pero no se realizan mediciones, revisiones y mejoras |
| A.11.2.7 | Disposición segura o reutilización de equipos | 0 | |
| A.11.2.8 | Equipos de usuario desatendido | 0 | |
| A.11.2.9 | Políticas de escritorio limpio y pantalla limpia | 90 | |
| **A.12** | **SEGURIDAD DE LAS OPERACIONES** | 10,7 | 1-25 - el requisito está planeado pero no implementado; |
| **A.12.1** | **Procedimientos operacionales y responsabilidades** | 40 | |
| A.12.1.1 | Procedimientos de operación documentados | 50 | |
| A.12.1.2 | Gestión de cambios | 0 | |
| A.12.1.3 | Gestión de capacidad | 50 | |
| A.12.1.4 | Separación de los ambientes de desarrollo, pruebas, y operación | 60 | |
| **A.12.2** | **Protección contra códigos maliciosos** | 20 | |
| A.12.2.1 | Controles contra códigos maliciosos | 20 | |
| **A.12.3** | **Proteger contra la perdida de datos** | 0 | |
| A.12.3.1 | Respaldo de la información | 0 | |
| **A.12.4** | **Registro y seguimiento** | 0 | |
| A.12.4.1 | Registro de eventos | 0 | |
| A.12.4.2 | Protección de la información de registro | 0 | |
| A.12.4.3 | Registros del administrador y del operador | 0 | |
| A.12.4.4 | Sincronización de reloj | 0 | |
| **A.12.5** | **Control de software operacional** | 10 | |
| A.12.5.1 | Instalación de software en sistemas operativos | 10 | |
| **A.12.6** | **Gestión de la vulnerabilidad técnica** | 5 | |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | 10 | |
| A.12.6.2 | Restricciones sobre la instalación de software | 0 | |
| **A.12.7** | **Consideraciones sobre auditorías de sistemas de información** | 0 | |
| A.12.7.1 | Controles de auditorías de sistemas de información | 0 | |

Cuadro 1. (Continuación)

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| **A.13** | **SEGURIDAD DE LAS COMUNICACIONES** | 25 | 1-25 - el requisito está planeado pero no implementado; |
| **A.13.1** | **Gestión de la seguridad de las redes** | 10 | |
| A.13.1.1 | Controles de redes | 20 | |
| A.13.1.2 | Seguridad de los servicios de red | 10 | |
| A.13.1.3 | Separación en las redes | 0 | |
| **A.13.2** | **Transferencia de información** | 40 | |
| A.13.2.1 | Políticas y procedimientos de transferencia de información | 0 | |
| A.13.2.2 | Acuerdos sobre transferencia de información | 0 | |
| A.13.2.3 | Mensajería electrónica | 80 | |
| A.13.2.4 | Acuerdos de confidencialidad o de no divulgación | 80 | |
| **A.14** | **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** | 23,7 | 1-25 - el requisito está planeado pero no implementado |
| **A.14.1** | **Requisitos de seguridad de los sistemas de información** | 40 | |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | 40 | |
| A.14.1.2 | Seguridad de servicio de las aplicaciones en redes publicas | 40 | |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones | 40 | |
| **A.14.2** | **Seguridad en los procesos de desarrollo y soporte** | 11,1 | |
| A.14.2.1 | Políticas de desarrollo seguro | 0 | |
| A.14.2.2 | Procedimiento de control de cambios en sistemas | 0 | |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | 40 | |
| A.14.2.4 | Restricción en los cambios a los paquetes de software | 0 | |
| A.14.2.5 | Principios de construcción de los sistemas seguros | 0 | |
| A.14.2.6 | Ambiente seguro de desarrollo | 0 | |

Cuadro 1. (Continuación)

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| A.14.2.7 | Desarrollo externamente contratado | 60 | 1-25 - el requisito está planeado pero no implementado |
| A.14.2.8 | Pruebas de seguridad de sistemas | 0 | |
| A.14.2.9 | Prueba de aceptación de sistemas | 0 | |
| **A.14.3** | **Datos de pruebas** | 20 | |
| A.14.3.1 | Protección de datos de pruebas | 20 | |
| **A.15** | **RELACIONES CON LOS PROVEEDORES** | 80 | 76-100 - el requisito se implementa y la medición, revisión y mejora se realizan con regularidad. |
| **A.15.1** | **Seguridad de la información en las relaciones con los proveedores** | 90 | |
| A.15.1.1 | Política de seguridad de la información para las relaciones con proveedores | 90 | |
| A.15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | 90 | |
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación | 90 | |
| **A.15.2** | **Gestión de la prestación de servicios de proveedores** | 70 | |
| A.15.2.1 | Seguimiento y revisión a los servicios proveedores | 70 | |
| A.15.2.2 | Gestión de cambios en los servicios de los proveedores | 70 | |
| **A.16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | 14,3 | 1-25 - el requisito está planeado pero no implementado; |
| **A.16.1** | **Gestión de incidentes y mejoras en la seguridad de la información** | 14,3 | |
| A.16.1.1 | Responsabilidades y procedimientos | 40 | |
| A.16.1.2 | Reporte de eventos de seguridad de la información | 10 | |
| A.16.1.3 | Reporte de debilidades de seguridad de la información | 10 | |
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | 10 | |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | 10 | |
| A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | 10 | |
| A.16.1.7 | Recolección de evidencia | 10 | |

Cuadro 1. (Continuación)

| No del Control | Objetivo de control | Porcentaje % | Nivel de madurez |
|---|---|---|---|
| **A.17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO** | 40 | 26-50 - el requisito se implementa solo parcialmente, por lo que no se pueden esperar efectos completos; |
| **A.17.1** | **Continuidad de seguridad de la información** | 0 | |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | 0 | |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | 0 | |
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | 0 | |
| **A.17.2** | **Redundancia** | 80 | |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | 80 | |
| **A.18** | **CUMPLIMIENTO** | 24 | 1-25 - el requisito está planeado, pero no implementado; |
| **A.18.1** | **Cumplimiento de requisitos legales y contractuales** | 48 | |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | 70 | |
| A.18.1.2 | Derechos de propiedad intelectual | 70 | |
| A.18.1.3 | Protección de registros | 50 | |
| A.18.1.4 | Privacidad y protección de información de datos personales | 50 | |
| A.18.1.5 | Reglamentación de controles criptográficos | 0 | |
| A.18.2 | **Revisiones de seguridad de la información** | 0 | |
| A.18.2.1 | Revisión independiente de la seguridad de la información | 0 | |
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad | 0 | |
| A.18.2.3 | Revisión del cumplimiento técnico | 0 | |

Fuente: “Elaboración propia basado en el Anexo A de la ISO 27001:2013”

6.1.1 Informe ejecutivo Análisis de Nivel de Madurez. Con el análisis de Nivel de Madurez de Bonos y Descuentos S.A.S, según lo indicado en el Cuadro 2, la empresa cuenta con un nivel de madurez inicial donde los requisitos están planteados pero no se encuentran implementados.

Cuadro 2. Resumen Nivel de Madurez

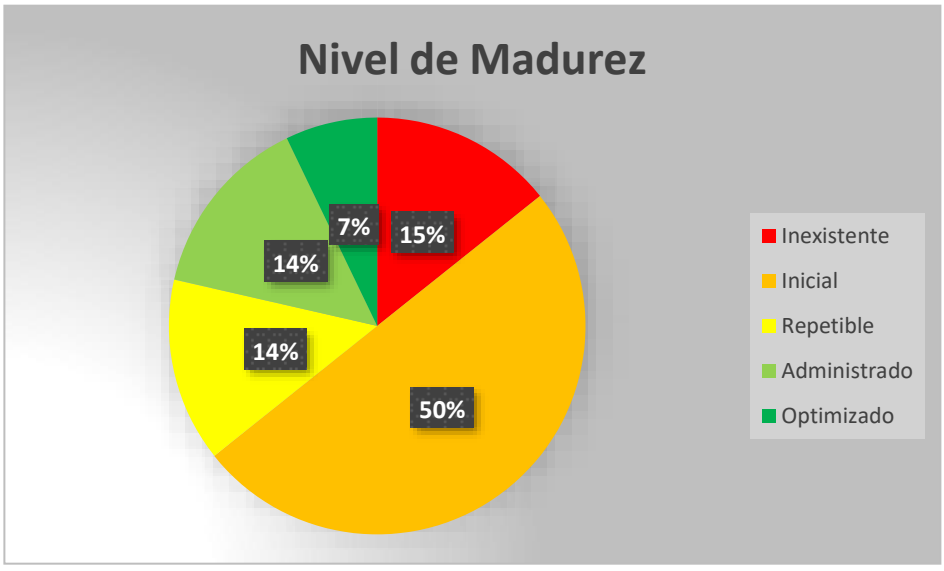
| Resumen de Nivel de madurez MSPI | |
|---|---|
| Inexistente | 2 |
| Inicial | 7 |
| Repetible | 2 |
| Administrado | 2 |
| Optimizado | 1 |
| **TOTAL** | **14** |

Fuente: “Elaboración propia”

En la Figura 3, el estado actual de la seguridad información dentro de la empresa se encuentra en un 50% su nivel de madurez, indicando que la continuidad del negocio está en riesgo.

Los porcentajes fueron calculados utilizando la Matriz_evaluación de riesgos en formato .XLS obtenida mediante el tutor Miguel Andres Avila del curso Administración y Gestión del Riesgo de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia - UNAD.

Figura 3. Nivel de Madurez




Fuente: Autoría propia

## 6.2 ELABORAR UN INVENTARIO, ANÁLISIS Y VALORACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN - DESARROLLO DE OBJETVO 2

Las evaluaciones de riesgos son el núcleo del proyecto de cumplimiento de la norma ISO 27001:2013 de cualquier organización.

Son esenciales para garantizar que un SGSI (sistema de gestión de seguridad de la información), aborde las amenazas de manera integral y adecuada.

Analizar y valorar los riesgos implica proporcionar una lista de activos de información crítica que la organización necesita proteger e identificar sus vulnerabilidades y amenazas potenciales que podrían ser explotadas.

6.2.1 Levantamiento de activos. Estos son entendidos como cualquier información de valor para una organización, por lo tanto, requiere unas medidas de protección. Los activos de información están definidos como: hardware, software, datos e información; personas que apoyan y utilizan el sistema de TI; equipo de comunicaciones; y varios servicios, como los servicios públicos.

Debido a que son una fuente primaria de valor, se considera que los activos de información son una unidad sensible de análisis al realizar.
El primer paso en el proceso del levantamiento de activos es descubrir y seleccionar sistemáticamente todos los activos de información relevantes que tiene la organización.

Se deben identificar todos los activos de información en el sistema delimitado para informar con precisión decisiones en el futuro, cada activo de información en una tiene cierto nivel de valor. Sin embargo, las limitaciones presupuestarias y de tiempo significa que no se pueden evaluar los riesgos para todos ellos, se debe decidir qué activos de información son esenciales o críticos para el diseño del SGSI[10].

Con base en los resultados de la visita realizada a la empresa Bonos y Descuentos S.A.S, se identificaron los siguientes activos:

**[S] Servicios**
- Correo Institucional
- Página WEB
- Asterisk en la nube

[10] FROSDICK, Steve. The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management an International Journal*, 1997, nro 6, pp.165-177

**[SW] Software - Aplicaciones informáticas**

- 15 Sofphone
- 14 S.O. Windows 7 crackeado
- 1 S.O. Windows 10 crackeado
- 1 S.O. Windows 10 licenciado
- Office 2016 licenciado
- Antivirus
- CRM
- Servidor de ficheros

**[HW] Equipamiento informático (hardware)**

- Impresora HP wifi
- Impresora PVC
- 15 PC de escritorio
- Portátil
- Módems
- Routers
- 2 Rack
- 2 Switch de 24
- 2 Switch de 48

**[COM] Redes de comunicaciones**

- LAN

**[AUX] Equipamiento auxiliar**

- DVR
- Cableado de Red

**[L] Instalaciones**

- Bonos y Descuentos S.A.S

**[P] Personal**

- Área administrativa
- Call center
- Proveedores

6.2.2 Análisis de riesgos. Es la actividad de examinar la probabilidad de los riesgos y el impacto que se ha determinado.

Una vez que se han identificado los activos de información críticos, se determina el impacto específico con referencia a los tres estados importantes de la información afectada: su confidencialidad, integridad y disponibilidad.

- **Valoración cuantitativa de activos**

La herramienta permite medir el valor de cada activo en base a las siguientes dimensiones:

- Disponibilidad (representada por [D]): Asegura que los colaboradores autorizados accedan a la información y activos cuando lo requieran.
- Integridad (representada por [I]): protege los datos y la información de modificaciones o eliminaciones no autorizadas.
- Confidencialidad (representada por [C]): Garantiza el acceso a la información / activos solo a los usuarios autorizados.
- Autenticidad (representada por [A]): Identifica a los usuarios que generaron la información y bloquea la posibilidad de suplantación.
- Trazabilidad (representada por [T]): permite rastrear quién hizo qué y cuándo[11].

La Figura 4, muestra la valoración de los activos expuesta por la herramienta, para dar una calificación dependiendo el daño en cada dimensión.

Figura 4. Valoración de activos

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

Fuente: Datos obtenido del Magerit V3 libro 2 Catalogo de elementos

De las dimensiones indicadas anteriormente solo serán evaluadas las siguientes:

[D] disponibilidad
[I] integridad
[C] confidencialidad

[11] 2001 MILCOM COMUNICACIONES DE PROCEDIMIENTOS PARA OPERACIONES CENTRADAS EN LA RED: CREANDO LA FUERZA DE INFORMACIÓN. (1: 28, OCTUBRE, 2001: Vienna, Austria). Revisión de la defensa en profundidad: riesgo cualitativo Metodología de análisis para operaciones complejas centradas en la red. IEEE, 2001, 10 p.

El Cuadro 3, muestra la valoración de los activos de servicios, indicando que las dimensiones más afectadas es la integridad y la confidencialidad

Cuadro 3. Valoración de [S] servicios

| **[S] servicios** | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| Correo Institucional | | 9 | 9 |
| Página WEB | 9 | | |
| Asterisk en la nube | 5 | 3 | 5 |

Fuente: “Elaboración propia, con base en la metodología Magerit V3 libro 2 Catalogo de elementos ”

La valoración cuantitativa de los activos de información de aplicaciones (software), en el Cuadro 4, se evidencia que un gran porcentaje de los activos de información tienen una valoración de 9 (muy alto), en las dimensiones de integridad y confidencialidad.

Cuadro 4. Valoración de [SW] aplicaciones (software)

| **[SW] aplicaciones (software)** | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| 15 Sofphone | | 9 | 9 |
| 14 S.O. Windows 7 crackeado | 9 | 9 | 9 |
| 1 S.O. Windows 10 crackeado | 9 | 9 | 9 |
| 1 S.O. Windows 10 licenciado | 6 | 6 | |
| Office 2016 licenciado | 5 | 5 | |
| Antivirus | 6 | 6 | 6 |
| CRM | 3 | | 3 |
| Servidor de ficheros | 9 | 9 | 9 |

Fuente: “Elaboración propia”

La dimensión más afectada en los activos equipos informáticos (hardware) del Cuadro 5 es la disponibilidad.

Cuadro 5. Valoración de [HW] equipos informáticos (hardware)

| **[HW] equipos informáticos (hardware)** | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| Impresora HP wifi | 5 | | |
| Impresora PVC | 3 | 3 | 3 |
| 15 PC de escritorio | 9 | 9 | 9 |
| Portátil | 9 | | 9 |
| Módems | 9 | 9 | 9 |
| Routers | 9 | 9 | 9 |
| 2 Rack | 6 | | |
| 2 Switch de 24 | 9 | 9 | 9 |
| 2 Switch de 48 | 9 | | 9 |

Fuente: “Elaboración propia”

En el Cuadro 6, la valoración del activo de información LAN el daño es alto en las dimensiones disponibilidad y confidencialidad.

Cuadro 6. Valoración de [COM] redes de comunicaciones

| **[COM] redes de comunicaciones** | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| LAN | 6 | | 6 |

Fuente: “Elaboración propia”

Los activos equipamiento auxiliar, las dimensiones disponibilidad y confidencialidad, son las más afectadas, según el Cuadro 7.

Cuadro 7. Valoración de [AUX] equipamiento auxiliar

| [AUX] equipamiento auxiliar | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| DVR | 9 | 9 | 9 |
| Cableado de Red | 5 | | 5 |

Fuente: “Elaboración propia”

El Cuadro 8, muestra la valoración de los activos de personal, indicando que las dimensiones más afectadas es la disponibilidad y la confidencialidad

Cuadro 8. Valoración de [P] personal

| [P] personal | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| Área administrativa | 9 | | |
| Call center | 9 | | 9 |
| Proveedores | 9 | 9 | 9 |

Fuente: “Elaboración propia”

La valoración cuantitativa del activo de información instalaciones, en el Cuadro 9, se evidencia que en las tres dimensiones a trabajar tienen una valoración de 9 (muy alto), donde indica que este activo se encuentra en daño extremamente grave, lo cual podría afectar la continuidad del negocio.

Cuadro 9. Valoración de [L] instalaciones

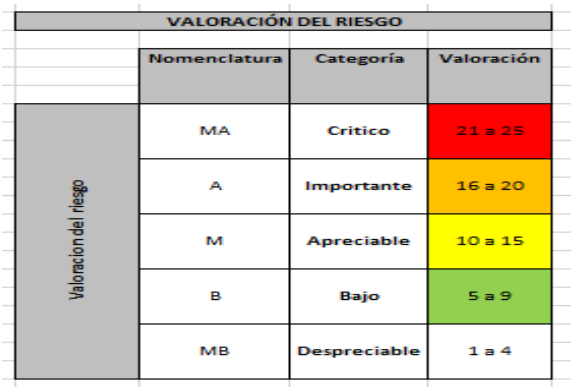
| [L] instalaciones | | | |
|---|---|---|---|
| **Activo** | **Dimensión de seguridad** | | |
| | **[ D ]** | **[ I ]** | **[ C ]** |
| Bonos y Descuentos S.A.S | 9 | 9 | 9 |

Fuente: “Elaboración propia”

- **Valoración del riesgo**

Algunos riesgos son más graves que otros, por lo que se debe determinar cuáles deben preocuparse más en esta etapa. Aquí es donde los criterios de riesgo son útiles. La Figura 5, proporciona una guía que ayuda a comparar los riesgos, al asignar una puntuación a la probabilidad de que ocurra y el daño que causará. Al evaluar los riesgos de esta manera, se obtiene una valoración consistente y comparable de las amenazas que enfrenta la empresa Bonos y Descuentos S.A.S.

Figura 5. Valoración del riesgo



| VALORACIÓN DEL RIESGO | | | |
|---|---|---|---|
| | Nomenclatura | Categoría | Valoración |
| Valoracion del riesgo | MA | Critico | 21 a 25 |
| | A | Importante | 16 a 20 |
| | M | Apreciable | 10 a 15 |
| | B | Bajo | 5 a 9 |
| | MB | Despreciable | 1 a 4 |

Fuente: Datos obtenido del Magerit V3 libro 2 Catalogo de elementos

Con la información de la valoración cuantitativa de activos es posible establecer el impacto, el cual puede definirse como la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en sus diferentes dimensiones), es posible identificar el impacto que estas causarían en el sistema. El impacto se calcula para cada activo de información de acuerdo con las dimensiones relacionadas. En el Cuadro 10, se muestra la lista de los activos con mayor valoración y con los niveles de criticidad más altos.

Cuadro 10. Valoración de riesgo de los activos de información

| Activos de información | Nombre del activo de información | Riesgo | Disponibilidad | Integridad | Confidencialidad | Autenticidad | Trazabilidad | Valor |
|---|---|---|---|---|---|---|---|---|
| [S] Servicios | Correo Institucional | IMPORTANTE | 15 | 25 | 25 | 25 | 9 | 20 |
| | Página WEB | IMPORTANTE | 25 | 15 | 15 | 15 | 15 | 17 |
| | Asterisk en la nube | APRECIABLE | 15 | 9 | 15 | 9 | 9 | 11 |

Cuadro 10. (Continuación)

| Activos de información | Nombre del activo de información | Riesgo | Disponibilidad | Integridad | Confidencialidad | Autenticidad | Trazabilidad | Valor |
|---|---|---|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | 15 Sofphone | CRITICO | 15 | 25 | 25 | 25 | 15 | 21 |
| | 14 S.O. Windows 7 crackeado | CRITICO | 25 | 25 | 25 | 25 | 25 | 25 |
| | 1 S.O. Windows 10 crackeado | CRITICO | 25 | 25 | 25 | 25 | 25 | 25 |
| | 1 S.O. Windows 10 licenciado | APRECIABLE | 15 | 15 | 15 | 9 | 9 | 13 |
| | Office 2016 licenciado | APRECIABLE | 15 | 15 | 9 | 9 | 9 | 11 |
| | Antivirus | IMPORTANTE | 20 | 20 | 20 | 15 | 15 | 18 |
| | CRM | BAJO | 9 | 9 | 9 | 9 | 9 | 9 |
| | Servidor de ficheros | CRITICO | 25 | 25 | 25 | 25 | 25 | 25 |
| **[HW] Equipamiento informático (hardware)** | Impresora HP wifi | APRECIABLE | 15 | 9 | 9 | 9 | 9 | 10 |
| | Impresora PVC | BAJO | 9 | 9 | 9 | 9 | 9 | 9 |
| | 15 PC de escritorio | CRITICO | 25 | 25 | 25 | 20 | 20 | 23 |
| | Portátil | IMPORTANTE | 25 | 15 | 25 | 15 | 15 | 19 |
| | Módems | CRITICO | 25 | 25 | 25 | 20 | 20 | 23 |
| | Routers | CRITICO | 25 | 25 | 25 | 15 | 15 | 21 |
| | 2 Rack | CRITICO | 25 | 20 | 20 | 20 | 20 | 21 |
| | 2 Switch de 24 | CRITICO | 25 | 25 | 25 | 20 | 20 | 23 |
| | 2 Switch de 48 | CRITICO | 25 | 20 | 25 | 20 | 20 | 22 |
| **[COM] Redes de comunicaciones** | LAN | IMPORTANTE | 20 | 15 | 20 | 15 | 15 | 17 |

Cuadro 1. (Continuación)

| Activos de información | Nombre del activo de información | Riesgo | Disponibilidad | Integridad | Confidencialidad | Autenticidad | Trazabilidad | Valor |
|---|---|---|---|---|---|---|---|---|
| **[AUX] Equipamiento auxiliar** | DVR | CRITICO | 25 | 25 | 25 | 20 | 20 | 23 |
| | Cableado de Red | APRECIABLE | 15 | 9 | 15 | 9 | 9 | 11 |
| **[L] Instalaciones** | Bonos y Descuentos S.A.S | CRITICO | 25 | 25 | 25 | 20 | 20 | 23 |
| **[P] Personal** | Área administrativa | CRITICO | 25 | 20 | 20 | 20 | 20 | 21 |
| | Call center | CRITICO | 25 | 20 | 25 | 20 | 20 | 22 |
| | Proveedores | CRITICO | 25 | 25 | 25 | 20 | 20 | 23 |

Fuente: “Elaboración propia”

- **Análisis de riesgos**

Una vez que se ha realizado la valoración del riesgo a los activos de información, se realiza de manera precisa y completa definir las amenazas y vulnerabilidades a cada uno. Aquí, es necesario identificar los resultados de un ataque exitoso a cada activo, como las posibilidades de destrucción, modificación / corrupción, o interrupciones en el acceso u operación.

Esta etapa identifica las amenazas que pueden tener un impacto en los activos de información. La herramienta incluye una biblioteca con las amenazas más comunes, tales como:

- Amenazas de la naturaleza, como terremotos, inundaciones, incendios, entre otras.
- Amenazas ambientales (origen industrial), como contaminación, fallas eléctricas, averías, etc.
- Defectos de aplicaciones / equipos (por defectos en su diseño o su implementación).
- Accidentes provocados por personas. Las personas con acceso al sistema de información pueden causar problemas no intencionales, ya sea por error o por omisión.

- Problemas causados deliberadamente por personas. Las personas con acceso al sistema de información pueden causar problemas de forma intencionada.

El cuadro 11, muestran las principales amenazas y vulnerabilidades a los activos de información más críticos de la empresa.

Cuadro 11. Análisis de riesgos de los activos de información

| **Activos de información** | **Nombre del activo de información** | **Valoración de riesgos de activos de información** | **Amenazas metodología Magerit** | **Vulnerabilidades** |
|---|---|---|---|---|
| **[S] Servicios** | Correo Institucional | 20 | [E19] Fugas de información | Mediante el correo electrónico se puede enviar información confidencial a usuarios externos |
| | | | [A5] Suplantación de la identidad del usuario | Un atacante podría suplantar el dominio realizando Spoofing |
| | Página WEB | 17 | [E24] Caída del sistema por agotamiento de recursos | Deficiencia de recursos cuando la carga de consultas tiene un alto de volumen |
| | | | [A24] Denegación de servicio | Por sobrecarga de ancho de banda y agotamiento de recursos del sistema |
| | Asterisk en la nube | 11 | [A24] Denegación de servicio | Se envía un ataque DoS al servidor, ocasionando que el servicio de llamadas quede indisponible |
| | | | [A5] Suplantación de la identidad del usuario | El atacante interno o externo podría romper la seguridad del servidor para tomar usuario y contraseña de las cuentas VoIP |

Cuadro 11. (Continuación)

| Activos de información | Nombre del activo de información | Valoración de riesgos de activos de información | Amenazas metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | 15 Sofphone | 21 | [E19] Fugas de información | Los empleados podrían divulgar información confidencial de la empresa a través de una llamada telefónica |
| | | | [A5] Suplantación de la identidad del usuario | El atacante interno o externo podría hacerse pasar por otra persona |
| | 14 S.O. Windows 7 crackeado | 25 | [A8] Difusión de software dañino | Al no encontrarse licenciado los S.O se podrán instalar software malicioso |
| | | | [E21] Errores de mantenimiento / actualización de programas (software) | Al ser crackeados no tienen una cuenta legitima, por lo tanto no pueden corregir las fallas de seguridad del S.O |
| | 1 S.O. Windows 10 crackeado | 25 | [E20] Vulnerabilidades de los programas (software) | La integridad de los datos siempre está en riesgo |
| | | | [A6] Abuso de privilegios de acceso | Al no contar con usuarios y contraseñas un atacante interno y externo tendría acceso al equipo |
| | 1 S.O. Windows 10 licenciado | 13 | [E21] Errores de mantenimiento / actualización de programas (software) | Al no tener una periodicidad no se podrán corregir las fallas presentadas |
| | Office 2016 licenciado | 11 | [E21] Errores de mantenimiento / actualización de programas (software) | Al no realizar las actualizaciones se presentan fallos en el funcionamiento de la suite |

Cuadro 11. (Continuación)

| Activos de información | Nombre del activo de información | Valoración de riesgos de activos de información | Amenazas metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | Antivirus | 18 | [E21] Errores de mantenimiento / actualización de programas (software) | Fallas en la protección, se podría infectar la máquina de malware, virus, etc. |
| | | | [E8] Difusión de software dañino | Propagación de virus, spyrawe, troyanos, etc. |
| | CRM | 9 | [E19] Fugas de información | El atacante podría sustraer información de los clientes para obtener ingresos |
| | | | [E18] Destrucción de información | El atacante podría destruir la información comprometiendo la integridad de los datos |
| | Servidor de ficheros | 25 | [I5] Avería de origen físico o lógico | Falla del funcionamiento del hardware y/o en el programa |
| | | | [A11] Acceso no autorizado | Ingreso al servidor sin los privilegios de autorización, lo cual podría modificar o borrar la información allí alojada |
| **[HW] Equipamiento informático (hardware)** | Impresora HP wifi | 10 | [I6] Corte del suministro eléctrico | Podría ocasionar daño permanente al equipo |
| | | | [I5] Avería de origen físico o lógico | Fallo en el equipo que lo podría sacar de funcionamiento |
| | Impresora PVC | 9 | [A7] Uso no previsto | Se podría usar para impresiones de documentos personales y financieros |
| | | | [E24] Caída del sistema por agotamiento de recursos | Presentación de fallas por uso excesivo del equipo |

Cuadro 11. (Continuación)

| Activos de información | Nombre del activo de información | Valoración de riesgos de activos de información | Amenazas metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware)** | 15 PC de escritorio | 23 | [I1] Fuego | Se podría presentar un incendio destruyendo los PC |
| | | | [A7] Uso no previsto | Un atacante interno o externo podría usar los equipos para ejecutar un ataque |
| | | | [A23] Manipulación de los equipos | Los equipos podrían sufrir modificaciones en el hardware causando bajo rendimiento o quedando inservible |
| | Portátil | 19 | [A25] Robo | Podría ocasionar la pérdida total de la información allí guardada exponiendo a la confidencialidad de los clientes |
| | | | [A26] Ataque destructivo | Destrucción del hardware y los respectivos soportes |
| | Módems | 23 | [A6] Abuso de privilegios de acceso | Ingreso como administrador a de la configuración del equipo realizando cambios no determinados |
| | | | [A11] Acceso no autorizado | Modificación de la configuración del equipo dejando sin internet a la empresa |
| | Routers | 21 | [A23] Manipulación de los equipos | Alteración intencionada en el funcionamiento del equipo para un beneficio propio |
| | | | [E2] Errores del administrador | Mala configuración del equipo ocasionando conflicto de red |

Cuadro 11. (Continuación)

| Activos de información | Nombre del activo de información | Valoración de riesgos de activos de información | Amenazas metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware)** | 2 Rack | 21 | [I1] Fuego | Destrucción total del hardware allí alojado |
| | | | [I6] Corte del suministro eléctrico | Perdida de información |
| | 2 Switch de 24 | 23 | [E2] Errores del administrador | Mala configuración de los puertos ocasionando conflictos en la red |
| | | | [E24] Caída del sistema por agotamiento de recursos | Caída del sistema por el alto volumen de tráfico |
| | 2 Switch de 48 | 22 | [A23] Manipulación de los equipos | Alteración intencionada en el funcionamiento del equipo para un beneficio propio |
| | | | [A26] Ataque destructivo | Interrupción de las comunicaciones internas como internet, base de datos, llamadas, etc. |
| **[COM] Redes de comunicaciones** | LAN | 17 | [I8] Fallo de servicios de comunicaciones | Perdida de conexión a los servicios de la empresa |
| | | | [A14] Interceptación de información (escucha) | Acceso a los servicios sin tener una autorización |
| **[AUX] Equipamiento auxiliar** | DVR | 23 | [I6] Corte del suministro eléctrico | Dejaría de grabar, lo cual a un incidente no se tendría como realizar una investigación |
| | | | [A11] Acceso no autorizado | Saturación y divulgación de la información confidencial. |

Cuadro 11. (Continuación)

| Activos de información | Nombre del activo de información | Valoración de riesgos de activos de información | Amenazas metodología Magerit | Vulnerabilidades |
|---|---|---|---|---|
| **[AUX] Equipamiento auxiliar** | Cableado de Red | 11 | [A25] Robo | Interrupción de las comunicaciones internas. |
| | | | [A26] Ataque destructivo | Perdida de conexión a los servicios de la empresa |
| **[L] Instalaciones** | Bonos y Descuentos S.A.S | 23 | [N*] Desastres naturales | Destrucción parcial o total de las instalaciones dejando en riesgo todos los activos de información |
| | | | [A11] Acceso no autorizado | Ingreso de personal no autorizado para realizar un ataque delictivo |
| **[P] Personal** | Área administrativa | 21 | [E7] Deficiencias en la organización | Falta de organización en los procesos afectando el negocio |
| | | | [E28] Indisponibilidad del personal | Interrupción del negocio |
| | Call center | 22 | [E19] Fugas de información | Suministro de información confidencial a internos y externos. |
| | | | [A28] Indisponibilidad del personal | Afectación al negocio y sus instalaciones |
| | Proveedores | 23 | [A29] Extorsión | Obtener ingresos con la información de la empresa |
| | | | [A30] Ingeniería social (picaresca) | Exposición de la confidencialidad, integridad y disponibilidad de la empresa |
| | | | [E19] Fugas de información | Sustraer información de la empresa para obtener un beneficio afectando la confidencialidad del negocio. |

Fuente: “Elaboración propia basado en magerit v3 libro 2 catálogo de elementos”

6.2.3 Informe ejecutivo Análisis de riesgos. La empresa Bonos y Descuentos cuenta con 27 activos de información, según la Clasificación general y Número de activos Cuadro 12 se catalogan por tipo de activo.

Cuadro 12. Clasificación general y Número de activos

| Tipo de activo | Cantidad |
|---|---|
| Tipo Dato | 0 |
| Tipo Claves Criptograficas | 0 |
| Tipo Servicio | 2 |
| Tipo Software | 9 |
| Tipo Hardware | 9 |
| Tipo Comunicaciones | 1 |
| Tipo Soporte de Información | 0 |
| Tipo Equipamento Auxiliar | 2 |
| Tipo Instalaciones | 1 |
| Tipo Personal | 3 |
| **Total de Activos** | **27** |

Fuente: “Elaboración propia”

Con el análisis de los activos de información se identificó el nivel del riesgo, las amenazas y las vulnerabilidades de estos, en el Cuadro 13, sé evidencia que de los 27 activos 15 se encuentran en un riesgo extremo.

Cuadro 13. Resumen de nivel de riesgo en los activos

| RIESGO | CANTIDAD DE ACTIVOS |
|---|---|
| **Extremo** | 15 |
| **Alto** | 5 |
| **Medio** | 1 |
| **Bajo** | 6 |

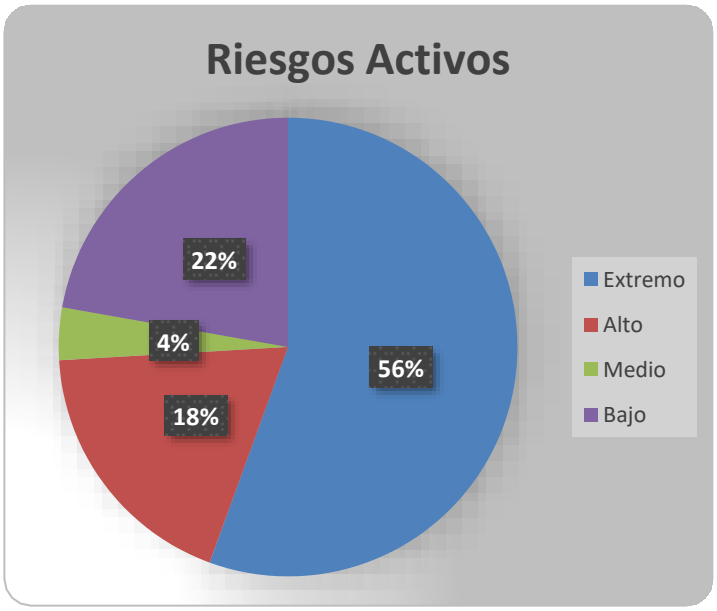
Fuente: “Elaboración propia”

En la Figura 6, el 56% de los activos de información se encuentran en riesgo extremo y un 18% de estos en riesgo alto, indicando que la empresa Bonos y Descuentos S.A.S se encuentra en alto riesgo de que estos se materialicen y sufra un ciberataque, en donde podría afectar la continuidad del negocio, también como

podría proteger activamente sus activos de información y, por lo tanto, intentar minimizar pérdidas tangibles e intangibles

.

Figura 6. Riesgos activos




Fuente: Autoría propia

## 6.3 CONSTRUIR LA DECLARACIÓN DE CONTROLES A APLICAR DENTRO DE LA EMPRESA, POR MEDIO DEL "SOA - POLÍTICA DE APLICABILIDAD" PARA GENERAR EL PLAN DE TRATAMIENTO DE RIESGOS - DESARROLLO DE OBJETVO 3

6.3.1 SOA - política de aplicabilidad. El SoA es un documento útil para el uso operativo diario porque proporciona una cobertura completa de las medidas de seguridad de la información de la organización.

Un SoA resume la posición de la organización en cada uno de los 114 controles de seguridad de la información descritos en el Anexo A de ISO 27001.

La cláusula 6.1.3 del Estándar establece que un SoA debe:

- Identificar qué controles ha seleccionado una organización para abordar los riesgos identificados;
- Explicar por qué se han seleccionado;
- Indicar si la organización ha implementado los controles o no; y
- Explicar por qué se han omitido los controles.

Cada control debe tener su propia entrada y, en los casos en que se haya seleccionado el control, el SoA debe vincularse a la documentación relevante sobre su implementación.

Esto es especialmente importante para garantizar la mejora continua dentro de la organización. Se Puede evaluar si los controles que se han implementado funcionan según lo previsto y evaluar si otros controles podrían ser más adecuados.

Del mismo modo, se puede revisar por qué se decidió aceptar los riesgos y determinar si el panorama de amenazas ha aumentado lo suficiente como para justificar un cambio.

Las organizaciones solo están obligadas a implementar controles que sean apropiados para los riesgos que enfrentan. Deben determinar qué controles se les aplican mediante la realización de un análisis de brechas y una evaluación de riesgos de la norma ISO 27001.

Estos procesos ayudan a las organizaciones a identificar los riesgos a los que se enfrentan, que pueden hacer coincidir con el control relevante[12].

En el ANEXO A de este documento**,** se proporciona un esquema útil de cada control en la empresa Bonos y Descuentos S.A.S.

6.3.2 Plan de tratamiento de riesgo. Es una parte esencial del proceso de implementación de ISO 27001 de una organización, ya que documenta la forma en que se responderá a las amenazas identificadas.

Es uno de los documentos obligatorios que se debe completar como parte de un SGSI y constituye la etapa final del proceso de evaluación de riesgos de ISO 27001.

En la Figura 7, muestra la valoración del riesgo inherente de los activos expuesta por la herramienta, para dar una calificación dependiendo de la mitigación del riesgo.

[12] ISO/CEI 27001:2013. [Sitio web]. Information technology — Security techniques — Information security management systems — Requirements. [Consulta: 25 de mayo 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Figura 7. Valoración de riesgo inherente

| | Nomenclatura | Categoría | Valoración | | Nomenclatura | Categoría | Valoración |
|---|---|---|---|---|---|---|---|
| Probabilidad | MA | Prácticamente seguro | 5 | Impacto | MA | Muy Alto | 5 |
| | A | Probable | 4 | | A | Alto | 4 |
| | M | Posible | 3 | | M | Medio | 3 |
| | B | Poco probable | 2 | | B | Bajo | 2 |
| | MB | muy raro | 1 | | MB | Muy Bajo | 1 |

Fuente: Datos obtenido del Magerit V3 libro 2 Catalogo de elementos

Una vez que se haya completado la evaluación de riesgos y se hayan definido los niveles de riesgo, se generara una lista de amenazas "inaceptables" que deben abordarse.

- ISO 27001 recomienda que las organizaciones tomen una de cuatro acciones:

  - Modificar el riesgo implementando un control para reducir la probabilidad de que ocurra. Por ejemplo, puede abordar el riesgo de que le roben una computadora portátil del trabajo mediante la creación de una política que indique a los empleados que mantengan los dispositivos con ellos y los almacenen de manera segura.

  - Evitar el riesgo cesando cualquier actividad que lo genere. Esta respuesta es adecuada si el riesgo es demasiado importante para gestionarlo con un control de seguridad. Por ejemplo, si no está dispuesto a correr el riesgo de que le roben una computadora portátil, puede optar por prohibir a los empleados que la utilicen fuera de las instalaciones. Esta opción hará que las cosas sean menos convenientes para sus empleados, pero mejorará drásticamente su postura de seguridad.

  - Compartir el riesgo con un tercero. Hay dos formas de hacer esto: subcontratando los esfuerzos de seguridad a otra organización o comprando un seguro cibernético para asegurarse de tener los fondos para responder adecuadamente en caso de un desastre. Ninguna de las opciones es ideal porque, en última instancia, usted es el responsable de la seguridad de su organización, pero podrían ser las mejores soluciones si carece de los recursos para abordar el riesgo.

Conservar el riesgo. Esta opción significa que su organización acepta el riesgo y cree que el costo de tratarlo es mayor que el daño que causaría. La opción de tratamiento de riesgo más común es modificar el riesgo porque generalmente ofrece la mejor combinación de seguridad y costo.

Las organizaciones pueden determinar la mejor manera de modificar un riesgo observando los controles enumerados en el Anexo A de ISO 27001. Enumera 114 controles, que se dividen en 14 secciones (o 'conjuntos de control'), cada uno adaptado a un aspecto específico de la seguridad de la información.

Por lo consiguiente para el diseño del SGSI de la empresa Bonos y Descuentos S.A.S se optó por la opción de “Modificar el riesgo” por temas se seguridad y costo como lo indica la Cuadro 15.

Los resultados obtenidos con la herramienta PILAR indican el nivel de cumplimiento de los dominios de la norma ISO / IEC 27001:2013. Es importante considerar que las salvaguardas o controles a aplicar están asociados con los controles de la norma ISO / IEC. El cumplimiento e implementación de las recomendaciones fortalecerá la seguridad de la Compañía[13].

Cuadro 14. Mitigación del riesgo

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[S] Servicios** | Correo Institucional | [E19] Fugas de información | Mediante el correo electrónico se puede enviar información confidencial a usuarios externos | A.7.2.1 A.7.2.2 A.7.2.3 | Probable | Alto |
| | | [A5] Suplantación de la identidad del usuario | Un atacante podría suplantar el dominio realizando Spoofing | A.9.4.1 A.9.4.2 | Posible | Medio |
| | Página WEB | [E24] Caída del sistema por agotamiento de recursos | Deficiencia de recursos cuando la carga de consultas tiene un alto de volumen | A.12.1.3 | Posible | Medio |

[13] CALDER, Alan. Information Security Based on ISO 27001/ISO 27002: A Management Guide. 2 ed. Bolduque.: Van Haren, 2009. p.85.(Best Practice). ISBN 908-75-3540-6

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[S] Servicios** | Página WEB | [A24] Denegación de servicio | Por sobrecarga de ancho de banda y agotamiento de recursos del sistema | A.12.2.1 | Prácticamente seguro | Muy alto |
| | Asterisk en la nube | [A24] Denegación de servicio | Se envía un ataque DoS al servidor, ocasionando que el servicio de llamadas quede indisponible | A.12.2.1 | Probable | Alto |
| | | [A5] Suplantación de la identidad del usuario | El atacante interno o externo podría romper la seguridad del servidor para tomar usuario y contraseña de las cuentas VoIP | A.9.2.1<br>A.9.2.2<br>A.9.2.3<br>A.9.4.2 | Posible | Medio |
| **[SW] Software - Aplicaciones informáticas** | 15 Sofphone | [E19] Fugas de información | Los empleados podrían divulgar información confidencial de la empresa a través de una llamada telefónica | A.7.1.2<br>A.7.2.1<br>A.7.2.2<br>A.7.2.3 | Probable | Alto |
| | | [A5] Suplantación de la identidad del usuario | El atacante interno o externo podría hacerse pasar por otra persona | A.9.2.1<br>A.9.2.2<br>A.9.2.3<br>A.9.4.2 | Posible | Medio |
| | 14 S.O. Windows 7 crackeado | [A8] Difusión de software dañino | Al no encontrarse licenciado los S.O se podrán instalar software malicioso | A.9.4.4<br>A.12.2.1<br>A.12.5.1 | Prácticamente seguro | Muy alto |
| | | [E21] Errores de mantenimiento / actualización de programas (software) | Al ser crackeados no tienen una cuenta legitima, por lo tanto no pueden corregir las fallas de seguridad del S.O | A.12.5.1<br>A.12.6.2 | Prácticamente seguro | Muy alto |

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | 1 S.O. Windows 10 crackeado | [E20] Vulnerabilidades de los programas (software) | La integridad de los datos siempre está en riesgo | A.12.6.1 A.12.6.2 | Prácticamente seguro | Muy alto |
| | | [A6] Abuso de privilegios de acceso | Al no contar con usuarios y contraseñas un atacante interno y externo tendría acceso al equipo | A.9.4.2 A.9.4.3 A.9.4.4 | Prácticamente seguro | Muy alto |
| | 1 S.O. Windows 10 licenciado | [E21] Errores de mantenimiento / actualización de programas (software) | Al no tener una periodicidad no se podrán corregir las fallas presentadas | A.12.5.1 A.12.6.2 | Poco probable | Bajo |
| | Office 2016 licenciado | [E21] Errores de mantenimiento / actualización de programas (software) | Al no realizar las actualizaciones se presentan fallos en el funcionamiento de la suite | A.12.5.1 A.12.6.2 | Poco probable | Bajo |
| | Antivirus | [E21] Errores de mantenimiento / actualización de programas (software) | Fallas en la protección, se podría infectar la máquina de malware, virus, etc. | A.12.5.1 A.12.6.2 | Prácticamente seguro | Muy alto |
| | | [E8] Difusión de software dañino | Propagación de virus, spyrawe, troyanos, etc. | A.12.2.1 | Prácticamente seguro | Muy alto |
| | CRM | [E19] Fugas de información | El atacante podría sustraer información de los clientes para obtener ingresos | A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 | Poco probable | Bajo |
| | | [E18] Destrucción de información | El atacante podría destruir la información comprometiendo la integridad de los datos | A.12.3.1 A.12.4.1 A.12.4.2 A.12.4.3 | Poco probable | Bajo |

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | Servidor de ficheros | [I5] Avería de origen físico o lógico | Falla del funcionamiento del hardware y/o en el programa | A.11.2.2<br>A.11.2.4<br>A.11.2.8 | Prácticamente seguro | Muy alto |
| | | [A11] Acceso no autorizado | Ingreso al servidor sin los privilegios de autorización, lo cual podría modificar o borrar la información allí alojada | A.9.1.1<br>A.9.2.2<br>A.9.2.3<br>A.9.4.1<br>A.12.3.1 | Prácticamente seguro | Muy alto |
| **[HW] Equipamiento informático (hardware)** | Impresora HP wifi | [I6] Corte del suministro eléctrico | Podría ocasionar daño permanente al equipo | A.11.2.2<br>A.11.2.3 | Poco probable | Bajo |
| | | [I5] Avería de origen físico o lógico | Fallo en el equipo que lo podría sacar de funcionamiento | A.11.2.2<br>A.11.2.4<br>A.11.2.8 | Poco probable | Bajo |
| | Impresora PVC | [A7] Uso no previsto | Se podría usar para impresiones de documentos personales y financieros | A.11.2.1 | Posible | Medio |
| | | [E24] Caída del sistema por agotamiento de recursos | Presentación de fallas por uso excesivo del equipo | A.12.1.3 | Posible | Medio |
| | 15 PC de escritorio | [I1] Fuego | Se podría presentar un incendio destruyendo los PC | A.11.1.1<br>A.11.1.3<br>A.11.1.4 | Probable | Alto |
| | | [A7] Uso no previsto | Un atacante interno o externo podría usar los equipos para ejecutar un ataque | A.11.2.1 | Prácticamente seguro | Muy alto |

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware** | 15 PC de escritorio | [A23] Manipulación de los equipos | Los equipos podrían sufrir modificaciones en el hardware causando bajo rendimiento o quedando inservible | A.11.2.1<br>A.11.2.4<br>A.11.2.5 | Prácticamente seguro | Muy alto |
| | Portátil | [A25] Robo | Podría ocasionar la pérdida total de la información allí guardada exponiendo a la confidencialidad de los clientes | A.11.2.5<br>A.11.2.6<br>A.12.3.1 | Probable | Alto |
| | | [A26] Ataque destructivo | Destrucción del hardware y los respectivos soportes | A.11.2.1<br>A.11.2.4<br>A.11.2.5<br>A.11.2.8 | Posible | Medio |
| | Módems | [A6] Abuso de privilegios de acceso | Ingreso como administrador de la configuración del equipo realizando cambios no determinados | A.9.1.1<br>A.9.1.2<br>A.9.2.1<br>A.9.2.2<br>A.9.2.3<br>A.9.2.4<br>A.9.2.5<br>A.9.2.6 | Probable | Alto |
| | | [A11] Acceso no autorizado | Modificación de la configuración del equipo dejando sin internet a la empresa | A.9.4.4<br>A.12.4.1 | Probable | Alto |
| | Routers | [A23] Manipulación de los equipos | Alteración intencionada en el funcionamiento del equipo para un beneficio propio | A.11.2.1<br>A.11.2.4<br>A.11.2.5 | Probable | Alto |

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware** | Routers | [E2] Errores del administrador | Mala configuración del equipo ocasionando conflicto de red | A.13.1.1<br>A.13.1.2<br>A.13.1.3 | Prácticamente seguro | Muy alto |
| | 2 Rack | [I1] Fuego | Destrucción total del hardware allí alojado | A.11.1.1<br>A.11.1.3<br>A.11.1.4 | Posible | Medio |
| | | [I6] Corte del suministro eléctrico | Perdida de información | A.11.2.2<br>A.11.2.3 | Posible | Medio |
| | 2 Switch de 24 | [E2] Errores del administrador | Mala configuración de los puertos ocasionando conflictos en la red | A.13.1.1<br>A.13.1.2<br>A.13.1.3 | Posible | Medio |
| | | [E24] Caída del sistema por agotamiento de recursos | Caída del sistema por el alto volumen de tráfico | A.12.1.3 | Posible | Medio |
| | 2 Switch de 48 | [A23] Manipulación de los equipos | Alteración intencionada en el funcionamiento del equipo para un beneficio propio | A.11.2.1<br>A.11.2.4<br>A.11.2.5 | Posible | Medio |
| | | [A26] Ataque destructivo | Interrupción de las comunicaciones internas como internet, base de datos, llamadas, etc. | A.11.1.1<br>A.11.1.2<br>A.11.1.4 | Posible | Medio |
| **[COM] Redes de comunicaciones** | LAN | [I8] Fallo de servicios de comunicaciones | Perdida de conexión a los servicios de la empresa | A.11.2.2<br>A.11.2.3 | Poco probable | Bajo |

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[COM] Redes de comunicaciones** | LAN | [A14] Interceptación de información (escucha) | Acceso a los servicios sin tener una autorización | A.9.1.1<br>A.9.2.2<br>A.9.2.3<br>A.9.4.1<br>A.12.4.1<br>A.12.4.2 | Poco probable | Bajo |
| **[AUX] Equipamiento auxiliar** | DVR | [I6] Corte del suministro eléctrico | Dejaría de grabar, lo cual a un incidente no se tendría como realizar una investigación | A.11.2.2<br>A.11.2.3 | Probable | Alto |
| | | [A11] Acceso no autorizado | Sustracción y divulgación de la información confidencial. | A.9.1.1<br>A.9.2.2<br>A.9.2.3<br>A.9.4.1<br>A.12.4.1<br>A.12.4.2 | Prácticamente seguro | Muy alto |
| | Cableado de Red | [A25] Robo | Interrupción de las comunicaciones internas. | A.11.2.3 | Poco probable | Bajo |
| | | [A26] Ataque destructivo | Perdida de conexión a los servicios de la empresa | A.11.2.3 | Poco probable | Bajo |
| **[L] Instalaciones** | Bonos y Descuentos S.A.S | [N*] Desastres naturales | Destrucción parcial o total de las instalaciones dejando en riesgo todos los activos de información | A.11.1.4 | Posible | Medio |
| | | [A11] Acceso no autorizado | Ingreso de personal no autorizado para realizar un ataque delictivo | A.11.1.1<br>A.11.1.2<br>A.11.1.3 | Probable | Alto |

Cuadro 15. (Continuación)

| Activos de información | Nombre del activo de información | Amenazas metodología Magerit | Vulnerabilidades | Control | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| **[P] Personal** | Área administrativa | [E7] Deficiencias en la organización | Falta de organización en los procesos afectando el negocio | A.12.1.1 | Poco probable | Bajo |
| | | [E28] Indisponibilidad del personal | Interrupción del negocio | A.7.1.2 | Poco probable | Bajo |
| | Call center | [E19] Fugas de información | Suministro de información confidencial a internos y externos. | A.7.1.2<br>A.7.2.1<br>A.7.2.2<br>A.7.2.3 | Probable | Alto |
| | | [A28] Indisponibilidad del personal | Afectación al negocio y sus instalaciones | A.7.1.2 | Posible | Medio |
| | Proveedores | [A29] Extorsión | Obtener ingresos con la información de la empresa | A.15.1.1<br>A.15.1.2<br>A.15.1.3<br>A.15.2.1<br>A.15.2.2 | Probable | Alto |
| | | [A30] Ingeniería social (picaresca) | Exposición de la confidencialidad, integridad y disponibilidad de la empresa | A.15.1.1<br>A.15.1.2<br>A.15.1.3<br>A.15.2.1<br>A.15.2.2 | Probable | Alto |
| | | [E19] Fugas de información | Sustraer información de la empresa para obtener un beneficio afectando la confidencialidad del negocio. | A.7.1.2<br>A.7.2.1<br>A.7.2.2<br>A.7.2.3 | Probable | Alto |

Fuente: “Elaboración propia”

### 6.3.3 Aplicación plan de mitigación de riesgos.

- **Aplicación de salvaguardas**

En esta fase, es necesario considerar los siguientes aspectos para la identificación y valoración de salvaguardas.

- El tipo de activos a proteger, cada tipo está protegido de forma diferente.
- Amenazas para las que el activo requiere protección.
- Si existen salvaguardias alternativas o adicionales.
- Céntrese en los riesgos más importantes.

Cabe señalar que las salvaguardas brindan diferentes tipos de protección:

- [PR] Preventiva: cuando se reducen las posibilidades de que ocurra un incidente, por ejemplo: pruebas de preproducción.

- [CR] Correctiva: Ejecutado después del daño. El daño se repara y reduce, por ejemplo: administración de incidentes.

- [DC] Detectado: El evento se informa cuando ocurre un ataque, por ejemplo: antivirus.

Las salvaguardas se aplicarán a aquellos dominios con menor porcentaje de cumplimiento de la norma ISO / IEC ya que tienen mayores riesgos[14].

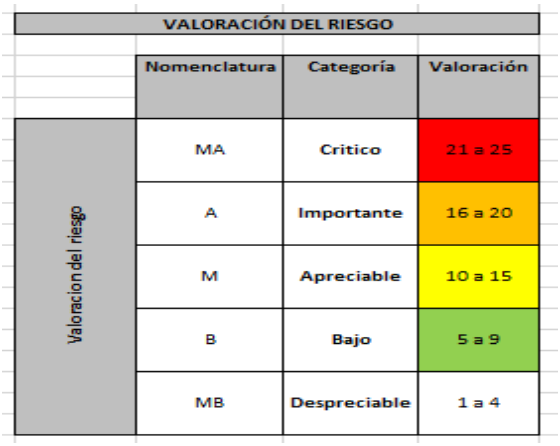
**Análisis de impacto y riesgo residual**

Esta es la última etapa y permite el análisis de resultados luego de la implementación de las salvaguardas. Permite medir la modificación del impacto y el riesgo de un valor potencial a un valor residual.

La Figura 8, muestra la valoración de los activos expuesta por la herramienta, para dar una calificación dependiendo del resultado de impacto y riesgo residual una vez aplicados lo controles

[14] SUAREZ GONZÁLEZ, Rafael. Análisis de activos de información para un sistema misional basados en la metodología MAGERIT V3 y la norma ISO 27001:2013 [en línea]. Trabajo de grado. Universidad Nacional Abierta y a Distancia UNAD CEAD Jose Acevedo y Gomez, 2018. [Consultado 25 de mayo 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/19571/80803746.pdf?sequence=3&isAllowed=y

Figura 8. Valoración del riesgo



| VALORACIÓN DEL RIESGO | | | |
|---|---|---|---|
| | Nomenclatura | Categoría | Valoración |
| Valoracion del riesgo | MA | Critico | 21 a 25 |
| | A | Importante | 16 a 20 |
| | M | Apreciable | 10 a 15 |
| | B | Bajo | 5 a 9 |
| | MB | Despreciable | 1 a 4 |

Fuente: Datos obtenido del Magerit V3 libro 2 Catalogo de elementos

El Cuadro 16, muestra los objetivos esperados a alcanzar mediante la aplicación de las salvaguardas, los resultados de impacto y riesgo residual después de aplicar las recomendaciones de protección.

Cuadro 15. Aplicación plan de mitigación

| Activos de informaci ón | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[S] Servicios** | Correo Institucional | A.7.2.1 | Se deben establecer las políticas y los procedimientos en la seguridad de la información, para que esta sea exigida por la dirección | BAJO | 9 |
| | | A.7.2.2 | Es necesario realizar capacitaciones de forma periódica de acuerdo a las actualizaciones de seguridad establecida por la empresa. | | |
| | | A.7.2.3 | De acuerdo a la gravedad de la falta o de la violación de seguridad esta será tratada bajo los reglamentos de la empresa o será informada a las autoridades competentes de ser necesario. | | |
| | | A.9.4.1 | Se debe contar con un formato de solicitud donde realicen estos tipos de requerimientos dependiendo del rol y las funciones realizadas, el formato será diligenciado por el superior | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[S] Servicios** | Correo Institucional | A.9.4.2 | Implementación de un Directorio Activo (DA) que permita brindar seguridad con contraseñas complejas a los sistemas de información. | BAJO | 9 |
| | Página WEB | A.12.2.1 | Es necesario la implementación de licencias de antivirus, antimalware, antispyware, etc. | BAJO | 9 |
| | | A.12.1.3 | Los equipos deben tener mantenimiento preventivo de ser necesario reacondicionamiento dentro de su vigencia | | |
| | Asterisk en la nube | A.12.2.1 | Es necesario la implementación de licencias de antivirus, antimalware, antispyware, etc. | BAJO | 9 |
| | | A.9.2.1 | Se debe crear un formato en donde se realice la solicitud y cancelación de Roles, el formato debe ser diligenciado por el jefe inmediato. | | |
| | | A.9.2.2 | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. | | |
| | | A.9.2.3 | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. | | |
| | | A.9.4.2 | Implementación de un Directorio Activo (DA) que permita brindar seguridad con contraseñas complejas a los sistemas de información. | | |
| **[SW] Software - Aplicaciones informáticas** | 15 Sofphone | A.7.1.2 | Se debe dar cumplimiento a las políticas de confidencialidad establecidas para personal de la empresa. | BAJO | 9 |
| | | A.7.2.1 | Se deben establecer las políticas y los procedimientos en la seguridad de la información, para que esta sea exigida por la dirección | | |
| | | A.7.2.2 | Es necesario realizar capacitaciones de forma periódica de acuerdo a las actualizaciones de seguridad establecida por la empresa. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | 15 Sofphone | A.7.2.3 | De acuerdo a la gravedad de la falta o de la violación de seguridad esta será tratada bajo los reglamentos de la empresa o será informada a las autoridades competentes de ser necesario. | BAJO | 9 |
| | | A.9.2.1 | Se debe crear un formato en donde se realice la solicitud y cancelación de Roles, el formato debe ser diligenciado por el jefe inmediato. | | |
| | | A.9.2.2 | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. | | |
| | | A.9.2.3 | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. | | |
| | | A.9.4.2 | Implementación de un Directorio Activo (DA) que permita brindar seguridad con contraseñas complejas a los sistemas de información. | | |
| | 14 S.O. Windows 7 crackeado | A.9.4.4 | Con las políticas del Directorio Activo se restringen la instalación de aplicaciones a todos los usuarios de la empresa. | BAJO | 9 |
| | | A.11.2.1 | La ubicación de los equipos debe estar aislada de las personas externas | | |
| | | A.12.2.1 | Es necesario la implementación de licencias de antivirus, antimalware, antispyware, etc. | | |
| | | A.12.5.1 | Se deben implementar un formato para instalación y desinstalación de software. | | |
| | | A.12.6.2 | A través del Directorio Activo ejecutar las restricciones para realizar cualquier tipo de instalación. | | |
| | 1 S.O. Windows 10 crackeado | A.9.4.2 | Implementación de un Directorio Activo (DA) que permita brindar seguridad con contraseñas complejas a los sistemas de información. | BAJO | 9 |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | 1 S.O. Windows 10 crackeado | A.9.4.3 | Establecer políticas a través del Directorio Activo y por un portal WEB para asegurar las contraseñas. | BAJO | 9 |
| | | A.9.4.4 | Con las políticas del Directorio Activo se restringen la instalación de aplicaciones a todos los usuarios de la empresa. | | |
| | | A.12.6.1 | Es necesario realizar periódicamente en los distintos sistemas de información el análisis de vulnerabilidades para mitigar los riesgos. | | |
| | | A.12.6.2 | A través del Directorio Activo ejecutar las restricciones para realizar cualquier tipo de instalación. | | |
| | 1 S.O. Windows 10 licenciado | A.12.5.1 | Se deben implementar un formato para instalación y desinstalación de software. | BAJO | 9 |
| | | A.12.6.2 | A través del Directorio Activo ejecutar las restricciones para realizar cualquier tipo de instalación. | | |
| | Office 2016 licenciado | A.12.5.1 | Se deben implementar un formato para instalación y desinstalación de software. | BAJO | 9 |
| | | A.12.6.2 | A través del Directorio Activo ejecutar las restricciones para realizar cualquier tipo de instalación. | | |
| | Antivirus | A.12.2.1 | Es necesario la implementación de licencias de antivirus, antimalware, antispyware, etc. | BAJO | 9 |
| | | A.12.5.1 | Se deben implementar un formato para instalación y desinstalación de software. | | |
| | | A.12.6.2 | A través del Directorio Activo ejecutar las restricciones para realizar cualquier tipo de instalación. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | CRM | A.7.1.2 | Se debe dar cumplimiento a las políticas de confidencialidad establecidas para personal de la empresa. | BAJO | 9 |
| | | A.7.2.1 | Se deben establecer las políticas y los procedimientos en la seguridad de la información, para que esta sea exigida por la dirección | | |
| | | A.7.2.2 | Es necesario realizar capacitaciones de forma periódica de acuerdo a las actualizaciones de seguridad establecida por la empresa. | | |
| | | A.7.2.3 | De acuerdo a la gravedad de la falta o de la violación de seguridad esta será tratada bajo los reglamentos de la empresa o será informada a las autoridades competentes de ser necesario. | | |
| | | A.12.3.1 | Las copias de respaldo se deben realizar periódicamente de acuerdo a la criticidad. | | |
| | | A.12.4.1 | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias | | |
| | | A.12.4.2 | Se deben establecer controles de acceso y vigilancia privada | | |
| | | A.12.4.3 | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias | | |
| | Servidor de ficheros | A.9.1.1 | De acuerdo con el perfil y el rol de las funciones se establecen las políticas de acceso a las aplicaciones, información confidencial, etc. | BAJO | 9 |
| | | A.9.2.2 | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[SW] Software - Aplicaciones informáticas** | Servidor de ficheros | A.9.2.3 | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. | BAJO | 9 |
| | | A.9.4.1 | Se debe contar con un formato de solicitud donde realicen estos tipos de requerimientos dependiendo del rol y las funciones realizadas, el formato será diligenciado por el superior | | |
| | | A.11.2.2 | Se debe contar con reguladores de energía y una UPS | | |
| | | A.11.2.4 | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica | | |
| | | A.11.2.8 | Los equipos que se encuentran en desuso deben ser almacenados para posterior disposición final. | | |
| | | A.12.3.1 | Las copias de respaldo se deben realizar periódicamente de acuerdo a la criticidad. | | |
| **[HW] Equipamiento informático (hardware)** | Impresora HP wifi | A.11.2.2 | Se debe contar con reguladores de energía y una UPS | BAJO | 9 |
| | | A.11.2.3 | Es necesario que el cableado este protegido con canaletas seguras. | | |
| | | A.11.2.4 | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica | | |
| | | A.11.2.8 | Los equipos que se encuentran en desuso deben ser almacenados para posterior disposición final. | | |
| | Impresora PVC | A.11.2.1 | La ubicación de los equipos debe estar aislada de las personas externas | BAJO | 9 |
| | | A.12.1.3 | Los equipos deben tener mantenimiento preventivo de ser necesario reacondicionamiento dentro de su vigencia | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware)** | 15 PC de escritorio | A.11.1.1 | Se debe crear un centro de datos aislado del personal y con un control de acceso como tarjetas de proximidad, lectores biométricos y/o cctv. | BAJO | 9 |
| | | A.11.1.3 | Implentación de alarmas y contratación de seguridad privada | | |
| | | A.11.1.4 | Se debe contar con una póliza sistema contraincendios un datacenter alterno que se encuentre geográficamente en otro lugar. | | |
| | | A.11.2.1 | La ubicación de los equipos debe estar aislada de las personas externas | | |
| | | A.11.2.4 | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica | | |
| | | A.11.2.5 | Es necesario la creación de un procedimiento para retiro los equipos y un formato que será autorizado por el jefe inmediato. | | |
| | Portátil | A.11.2.1 | La ubicación de los equipos debe estar aislada de las personas externas | BAJO | 9 |
| | | A.11.2.4 | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica | | |
| | | A.11.2.5 | Es necesario la creación de un procedimiento para retiro los equipos y un formato que será autorizado por el jefe inmediato. | | |
| | | A.11.2.6 | Se debe adquirir una póliza que proteja los equipos contra robo o daño. | | |
| | | A.11.2.8 | Los equipos que se encuentran en desuso deben ser almacenados para posterior disposición final. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware)** | Portátil | A.12.3.1 | Las copias de respaldo se deben realizar periódicamente de acuerdo a la criticidad. | BAJO | 9 |
| | Módems | A.9.1.1 | De acuerdo con el perfil y el rol de las funciones se establecen las políticas de acceso a las aplicaciones, información confidencial, etc. | BAJO | 9 |
| | | A.9.1.2 | La red debe estar diseñada por VLAN que permita el acceso seguro a la infraestructura según los roles y funciones de los usuarios. | | |
| | | A.9.2.1 | Se debe crear un formato en donde se realice la solicitud y cancelación de Roles, el formato debe ser diligenciado por el jefe inmediato. | | |
| | | A.9.2.2 | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. | | |
| | | A.9.2.3 | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. | | |
| | | A.9.2.4 | Este es controlado mediante el acuerdo de confidencialidad suscrito por el empleador y empleado. | | |
| | | A.9.2.5 | El control de acceso de los usuarios debe ser revisado cada seis meses por parte del jefe inmediato | | |
| | | A.9.2.6 | La solicitud debe ser diligenciada por el jefe inmediato en el formato predeterminado. | | |
| | | A.9.4.4 | Con las políticas del Directorio Activo se restringen la instalación de aplicaciones a todos los usuarios de la empresa. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware)** | Módems | A.12.4.1 | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias | BAJO | 9 |
| | Routers | A.11.2.1 | La ubicación de los equipos debe estar aislada de las personas externas | BAJO | 9 |
| | | A.11.2.4 | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica | | |
| | | A.11.2.5 | Es necesario la creación de un procedimiento para retiro los equipos y un formato que será autorizado por el jefe inmediato. | | |
| | | A.13.1.1 | Para prevenir fuga de información se deben crear distintas Vlan. | | |
| | | A.13.1.2 | Se deben identificar las configuraciones y restricciones de la red que permitan brindar la seguridad necesaria | | |
| | | A.13.1.3 | Es necesario que la red y sus dispositivos como switch, router, sean configurados con Vlan para separación de los diversos grupos de red | | |
| | 2 Rack | A.11.1.1 | Se debe crear un centro de datos aislado del personal y con un control de acceso como tarjetas de proximidad, lectores biométricos y/o cctv. | BAJO | 9 |
| | | A.11.1.3 | Implentación de alarmas y contratación de seguridad privada | | |
| | | A.11.1.4 | Se debe contar con una póliza sistema contraincendios un datacenter alterno que se encuentre geográficamente en otro lugar. | | |
| | | A.11.2.2 | Se debe contar con reguladores de energía y una UPS | | |
| | | A.11.2.3 | Es necesario que el cableado este protegido con canaletas seguras. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[HW] Equipamiento informático (hardware)** | 2 Switch de 24 | A.12.1.3 | Los equipos deben tener mantenimiento preventivo de ser necesario reacondicionamiento dentro de su vigencia | BAJO | 9 |
| | | A.13.1.1 | Para prevenir fuga de información se deben crear distintas Vlan. | | |
| | | A.13.1.2 | Se deben identificar las configuraciones y restricciones de la red que permitan brindar la seguridad necesaria | | |
| | | A.13.1.3 | Es necesario que la red y sus dispositivos como switch, router, sean configurados con Vlan para separación de los diversos grupos de red | | |
| | 2 Switch de 48 | A.11.1.1 | Se debe crear un centro de datos aislado del personal y con un control de acceso como tarjetas de proximidad, lectores biométricos y/o cctv. | BAJO | 9 |
| | | A.11.1.2 | Mediante lectores biométricos a doble autenticación. | | |
| | | A.11.1.4 | Se debe contar con una póliza sistema contraincendios un datacenter alterno que se encuentre geográficamente en otro lugar. | | |
| | | A.11.2.1 | La ubicación de los equipos debe estar aislada de las personas externas | | |
| | | A.11.2.4 | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica | | |
| | | A.11.2.5 | Es necesario la creación de un procedimiento para retiro los equipos y un formato que será autorizado por el jefe inmediato. | | |
| **[COM] Redes de comunicaciones** | LAN | A.9.1.1 | De acuerdo con el perfil y el rol de las funciones se establecen las políticas de acceso a las aplicaciones, información confidencial, etc. | BAJO | 9 |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[COM] Redes de comunicaciones** | LAN | A.9.2.2 | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. | BAJO | 9 |
| | | A.9.2.3 | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. | | |
| | | A.9.4.1 | Se debe contar con un formato de solicitud donde realicen estos tipos de requerimientos dependiendo del rol y las funciones realizadas, el formato será diligenciado por el superior | | |
| | | A.11.2.2 | Se debe contar con reguladores de energía y una UPS | | |
| | | A.11.2.3 | Es necesario que el cableado este protegido con canaletas seguras. | | |
| | | A.12.4.1 | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias | | |
| | | A.12.4.2 | Se deben establecer controles de acceso y vigilancia privada | | |
| **[AUX] Equipamiento auxiliar** | DVR | A.9.1.1 | De acuerdo con el perfil y el rol de las funciones se establecen las políticas de acceso a las aplicaciones, información confidencial, etc. | BAJO | 9 |
| | | A.9.2.2 | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. | | |
| | | A.9.2.3 | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[AUX] Equipamiento auxiliar** | DVR | A.9.4.1 | Se debe contar con un formato de solicitud donde realicen estos tipos de requerimientos dependiendo del rol y las funciones realizadas, el formato será diligenciado por el superior | BAJO | 9 |
| | | A.11.2.2 | Se debe contar con reguladores de energía y una UPS | | |
| | | A.11.2.3 | Es necesario que el cableado este protegido con canaletas seguras. | | |
| | | A.12.4.1 | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias | | |
| | | A.12.4.2 | Se deben establecer controles de acceso y vigilancia privada | | |
| | Cableado de Red | A.11.2.3 | Es necesario que el cableado este protegido con canaletas seguras. | BAJO | 9 |
| **[L] Instalaciones** | Bonos y Descuentos S.A.S | A.11.1.1 | Se debe crear un centro de datos aislado del personal y con un control de acceso como tarjetas de proximidad, lectores biométricos y/o cctv. | BAJO | 9 |
| | | A.11.1.2 | Mediante lectores biométricos a doble autenticación. | | |
| | | A.11.1.3 | Implentación de alarmas y contratación de seguridad privada | | |
| | | A.11.1.4 | Se debe contar con una póliza sistema contraincendios un datacenter alterno que se encuentre geográficamente en otro lugar. | | |
| **[P] Personal** | Área administrativa | A.7.1.2 | Se debe dar cumplimiento a las políticas de confidencialidad establecidas para personal de la empresa. | BAJO | 9 |
| | | A.12.1.1 | Los procedimientos deben ser divulgados y publicados internamente para que los empleados tengan acceso a la información. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[P] Personal** | Call center | A.7.1.2 | Se debe dar cumplimiento a las políticas de confidencialidad establecidas para personal de la empresa. | BAJO | 9 |
| | | A.7.2.1 | Se deben establecer las políticas y los procedimientos en la seguridad de la información, para que esta sea exigida por la dirección | | |
| | | A.7.2.2 | Es necesario realizar capacitaciones de forma periódica de acuerdo a las actualizaciones de seguridad establecida por la empresa. | | |
| | | A.7.2.3 | De acuerdo a la gravedad de la falta o de la violación de seguridad esta será tratada bajo los reglamentos de la empresa o será informada a las autoridades competentes de ser necesario. | | |
| | Proveedores | A.7.1.2 | Se debe dar cumplimiento a las políticas de confidencialidad establecidas para personal de la empresa. | BAJO | 9 |
| | | A.7.2.1 | Se deben establecer las políticas y los procedimientos en la seguridad de la información, para que esta sea exigida por la dirección | | |
| | | A.7.2.2 | Es necesario realizar capacitaciones de forma periódica de acuerdo a las actualizaciones de seguridad establecida por la empresa. | | |
| | | A.7.2.3 | De acuerdo a la gravedad de la falta o de la violación de seguridad esta será tratada bajo los reglamentos de la empresa o será informada a las autoridades competentes de ser necesario. | | |
| | | A.15.1.1 | Se deben establecer contratos de prestación de servicios y acuerdos de confidencialidad. | | |

Cuadro 16. (Continuación)

| Activos de información | Nombre del activo de información | Control | Aplicación del Control | Riesgo | Valor |
|---|---|---|---|---|---|
| **[P] Personal** | Proveedores | A.15.1.2 | Es necesario que en los contratos realizados se detallen los requisitos necesarios en la seguridad de la información | BAJO | 9 |
| | | A.15.1.3 | Es necesario solicitar a los proveedores acuerdos para proteger la empresa de los riesgos ocurridos por la operación de un proveedor. | | |
| | | A.15.2.1 | Periódicamente se debe realizar seguimiento y auditorías a los servicios prestados. | | |
| | | A.15.2.2 | Si mediante los contratos por prestación de servicios ya establecidos debe ir un ítem que diga servicios conexos el cual incluye la parte de suministros. | | |

Fuente: “Elaboración propia”

## 6.4 PROPONER LAS POLÍTICAS Y CONTROLES DE SEGURIDAD A LOS ACTIVOS DE INFORMACIÓN - DESARROLLO DE OBJETVO 4

6.4.1 Acceso de usuarios. Debe proporcionarse de acuerdo con los principios de "privilegio y necesidad" para lograr la función deseada. El propósito de esta política es para establecer las reglas bajo las cuales el ingreso a la información de la empresa se proporciona, controlan y gestionan los sistemas.

6.4.1.1 Control de acceso.

1. Por servicio y cuando sea posible, el acceso a los sistemas de información de la debe estar controlado por un sistema centralizado de autenticación, autorización y contabilidad (es decir, para la infraestructura de red o dominios de Windows de Active Directory).

2. No se permiten cuentas autenticadas localmente a menos que se haya evaluado y aprobado una justificación académica, comercial o técnica válida a través del proceso de gestión de riesgos.

3. De acuerdo con este estándar, se deben desarrollar procesos y procedimientos de requisitos de control de acceso para administrar cuentas autenticadas localmente.

6.4.1.2 Aprovisionamiento y desaprovisionamiento de acceso general

1. Todas las cuentas deben estar asociadas con un propietario, es decir, una relación de uno a uno y, cuando sea posible, asignarse a un grupo.

2. Las solicitudes de acceso son aprobadas por una autoridad apropiada (el gerente de la persona) antes de que los administradores de aplicaciones y sistemas de TI las implementen.

3. Siempre que sea posible, se deben considerar e implementar los siguientes modelos de control de acceso para la autenticación de usuarios. Por ejemplo: Control de acceso basado en roles (RBAC) para permitir que los usuarios accedan a los sistemas de información según su rol heredando un conjunto predefinido de derechos de acceso.

4. Los derechos de cuenta y de acceso relativo deben eliminarse o deshabilitarse cuando un usuario ya no necesita acceso debido a cambios de roles o retiro de la empresa.

5. Las cuentas de los contratistas siempre deben tener una fecha de vencimiento alineada con el período del contrato.

6. En caso de una emergencia (es decir, un proveedor externo requiere acceso durante una situación de gravedad 1), las solicitudes de acceso se aprueban y documentan retrospectivamente.

7. Para los sistemas aplicables, los propietarios o delegados deben realizar una revalidación anual de la cuenta para validar la necesidad comercial continua con la autoridad que lo autoriza.

8. Los sistemas de autenticación (es decir, Active Directory) deben reflejar la lista actual de personas aprobadas.

6.4.1.3 Acceso de usuario remoto

1. Todas las solicitudes de acceso remoto utilizadas para conectarse a los sistemas de información deben ser aprobadas por una autoridad apropiada (por ejemplo, el jefe de la persona). El acceso remoto a los sistemas de información de debe ser estrictamente controlado e implementado de acuerdo con el Estándar de Seguridad de Red. El acceso remoto está sujeto a las siguientes restricciones:

a) Los usuarios se autentican de forma segura (a través de un par de nombre de usuario / contraseña o, cuando corresponda, mediante un segundo método de autenticación adicional, como un PIN o una tarjeta inteligente) antes del establecimiento de una conexión remota.

b) Los datos “altamente sensibles” y “privados” deben estar encriptados cuando los datos se transfieren a través de redes públicas (es decir, Internet).

c) Las cuentas de acceso remoto con derechos privilegiados para uso administrativo deben estar limitadas al personal autorizado y estrictamente controladas a través de:

- Autenticación de dos factores, es decir, tarjeta inteligente, token de software o PIN.
- Monitoreo regular de registros de eventos.
- Revisiones periódicas, al menos una vez al año, de los derechos de acceso para verificar la adecuación continua de los derechos de acceso.

2. Los usuarios no deben intentar eludir los controles de seguridad de acceso remoto (VPN). Cualquier desviación debe abordarse desde una perspectiva de riesgo y debe ser aprobada por el propietario de la empresa del sistema de punto final y acceso remoto.

6.4.1.4 Responsabilidad del usuario

1. Todos los usuarios de UNSW son personalmente responsables del uso de su cuenta y deben:

- Seleccionar y usar contraseñas seguras.
- Cambiar su contraseña si sabe o sospecha que su cuenta ha sido comprometida.
- Mantener las contraseñas seguras y no revelarlas bajo ninguna circunstancia.
- No intentar utilizar ninguna cuenta que no sea la suya, a menos que sea con fines de apoyo legítimo o incidentes de seguridad.
- No compartir su cuenta de usuario con otras personas.

6.4.2 Gestión de activos de TI. La gestión adecuada de los activos de TI es un requisito fundamental de cualquier SGSI. La empresa debe emplear procesos robustos para garantizar que los activos de TI estén identificados, inventariados y en continuo mantenimiento.

#### 6.4.2.1 Gestión de activos de TI

1. Los propietarios del sistema deben identificar y mantener detalles precisos de los activos en un Inventario de activos central (Base de datos de gestión de la configuración). El inventario de activos debe incluir, si corresponde:

    - El propietario del sistema.
    - Propietario de la empresa.
    - Identificador de activo único (por ejemplo, código de barras) y ubicación, por ejemplo, centro de datos seguro.
    - Información como nombre del proveedor, número de modelo, número de serie, código / versión de firmware, nombre de host / aplicación, dirección IP, referencia de circuito, número de licencia.
    - Clasificación de riesgo, es decir, alto según los cálculos de clasificación

2. El inventario de activos de TI debe actualizarse cuando:

    - Se encarga un activo, por ejemplo, se pone en producción.
    - Una situación de reparación o actualización que implique el reemplazo de un activo, es decir, el reemplazo del módulo de infraestructura donde el hardware y, por lo tanto, el número de serie ha cambiado.
    - Cambio de código o versión debido a actualización o parche.
    - Un activo se da de baja, es decir, se retira de la producción.

3. El inventario de activos de TI debe conciliarse al menos una vez al año.

4. El acceso al inventario de activos de TI está limitado al personal autorizado que tenga una necesidad comercial válida.

#### 6.4.2.2 Responsabilidades del propietario del sistema y del negocio de activos de TI

1. Se deben asignar propietarios de negocios y sistemas para todos los activos bajo administración.

2. Los propietarios de negocios son, en última instancia, responsables de todos los activos y deben nominar, definir y documentar las responsabilidades del propietario del sistema designado.

3. Los propietarios del sistema deben asegurarse de que se abordan los controles del alcance detallados en los estándares del SGSI, específicamente:

    - Documentar y gestionar el activo

- Identificar, implementar, monitorear e informar la efectividad de los controles de seguridad de la información asociados con los activos en todos los estándares de seguridad de la información dentro del alcance.
- Identificar, evaluar, tratar y revisar los riesgos de sus activos.
- Informar los incidentes de seguridad y los riesgos percibidos que afectan a los activos a través de la mesa de servicio de TI.

4. Los propietarios de sistemas deben proteger los activos de TI de acuerdo con los requisitos especificados por los propietarios de empresas.

6.4.3 Seguridad de aplicaciones web. La protección web es fundamental para la seguridad general de la empresa. Los protocolos basados en web son objeto de nuevas y continuas amenazas, y si se explotan puede exponer información confidencial. El propósito de esta política establece los requisitos básicos para el diseño, construcción y prueba de aplicaciones web con el fin de reducir el riesgo para Bonos y Descuentos S.A.S de cualquier compromiso de las aplicaciones web, la información almacenada, redes y sistemas informáticos conectados.

6.4.3.1 Principios de seguridad para aplicaciones web

1. Para lograr un diseño 'seguro' para las aplicaciones web, se deben abordar controles de seguridad específicos en las fases de diseño, construcción y prueba de los procesos de desarrollo de aplicaciones web.

6.4.3.2 Diseño: segregación de la función de la aplicación web para crear una defensa en profundidad

1. Un requisito importante que debe abordarse para proteger la información dentro de los servicios conectados a redes no confiables es aplicar una estrategia de "defensa en profundidad". La defensa en profundidad se puede lograr mediante la implementación de zonas de seguridad de diferente confianza. Esto asegura que la información importante nunca sea directamente accesible desde zonas donde no hay confianza o es mínima, por ejemplo, Internet u otras redes externas fuera del control de la empresa.

2. La arquitectura de las soluciones debe estar separada en zonas de seguridad. El número y la clasificación de las zonas deben definirse en función de la clasificación de la información almacenada dentro de la zona de seguridad y los tipos de red de origen que accederán a esta información

6.4.4 Copia de seguridad de datos. El backup es de vital importancia ya que es la última línea de defensa en el caso de pérdida o modificación accidental o maliciosa de configuraciones de información, aplicaciones e infraestructura. El propósito de esta política es establecer los requisitos básicos para la copia de seguridad de la empresa en sistemas de información y datos. La información de debe ser respaldada regularmente, protegida de acceso no autorizado o modificación durante el almacenamiento, y disponible para recuperación de una manera oportuna. Dado que los backups pueden contener información confidencial en altos volúmenes, es decir, transacciones financieras, identificación personal, etc. Los medios de copia de seguridad deben estar protegidos, durante todo el ciclo de vida de la información

6.4.4.1 Programación de copias de seguridad

1. Las copias de seguridad deben programarse de acuerdo con los requisitos de disponibilidad de la información que se está respaldando. Se debe documentar y mantener un cronograma de respaldo para todos los sistemas.

2. Los requisitos de respaldo para los sistemas de información y los datos deben documentarse y comunicarse a los equipos de implementación y soporte para su inclusión en los procedimientos operativos antes de que los sistemas entren en producción.

6.4.4.2 Verificación de procesos de respaldo e investigación de fallas

1. Se debe verificar una muestra de trabajos como parte del proceso para mantener la integridad de la información que se respalda, de manera acorde con la confiabilidad de los medios de respaldo.

2. Los informes de fallas de respaldo se deben producir, revisar y actuar dentro de un período de tiempo razonable para garantizar que se completen con éxito.

6.4.4.3 Validación de medios de respaldo y procesos de recuperación

1. Existe el riesgo de que los medios ópticos y de cinta se degraden con el tiempo, corrompiendo o destruyendo cualquier información de la que se haya realizado una copia de seguridad en este medio.

2. Para protegerse contra la corrupción de datos, los medios ópticos y de cinta no deben exceder las recomendaciones de uso del fabricante.

3. El proceso de validación y recuperación debe documentarse de manera auditable y probarse de manera regular para ser determinado por el Plan de Recuperación de TI.

6.4.4.4 Protección de copias de seguridad y medios de copia de seguridad

1. Los medios de respaldo deben tratarse como si tuvieran un nivel de clasificación equivalente al del sistema de información fuente. Por ejemplo, los datos confidenciales, como la información de identificación personal regulada, deben estar debidamente cifrados (p. Ej., A nivel de base de datos o archivo) cuando se almacenan en medios de copia de seguridad.

2. El acceso a los medios de respaldo debe estar restringido únicamente al personal autorizado.

6.4.4.5 Retención y eliminación de copias de seguridad y medios de copia de seguridad

1. Los medios de respaldo deben conservarse de acuerdo con los requisitos de recuperación de TI, retención de datos y administración de registros cuando corresponda.

2. Los medios de respaldo deben eliminarse de acuerdo con los requisitos de eliminación apropiados descritos en el Estándar de clasificación de datos y las Pautas de manejo de datos, por ejemplo, sobrescribiendo los medios o destruyéndolos físicamente mediante un proceso verificado y auditable.

6.4.4.6 Ubicaciones de los medios de respaldo y transporte fuera del sitio de los medios de respaldo

1. Los medios de respaldo que contienen información sensible solo deben transportarse fuera del sitio con la protección física adecuada, en un contenedor seguro, dentro de un vehículo seguro, siguiendo un proceso auditable y verificable.

2. La frecuencia de envío de medios de respaldo fuera del sitio debe documentarse y justificarse en el programa de respaldo. La consideración de la frecuencia debe tener en cuenta la importancia y los requisitos de recuperación de los datos.

3. Los medios de copia de seguridad deben almacenarse en una ubicación física segura para garantizar que los medios estén protegidos contra el acceso, la modificación o la destrucción no autorizados. Esto incluye:

    - Fuera del sitio en relación con y almacenado en un lugar con estricta seguridad física.

- En un ambiente de temperatura controlada empleando mecanismos de extinción de incendios.

- En cajas fuertes contra incendios designadas dentro del campus de la, para el almacenamiento local de medios de respaldo.

6.4.5 Seguridad física. Deben existir controles físicos y ambientales sólidos para proteger los activos de información y sistemas contra el acceso no autorizado, y protegerse contra amenazas ambientales. Esta política garantizar la confidencialidad, integridad y disponibilidad de los datos contenidos en el entorno físico.

6.4.5.1 Seguridad del cableado

1. De acuerdo con los estándares eléctricos / de cableado de la industria, se deben tomar precauciones para mitigar el riesgo de interceptación de datos no autorizada / maliciosa y daños accidentales / maliciosos a las instalaciones de TIC.

2. El cableado eléctrico está físicamente separado del cableado de datos para evitar interferencias y reducir el riesgo de lesiones y daños al equipo.

3. Todas las líneas eléctricas y de telecomunicaciones de las instalaciones de procesamiento de información son subterráneas o están sujetas a una protección alternativa adecuada.

4. Todo el equipo de cableado y redes está claramente etiquetado utilizando una convención documentada para minimizar los errores de manejo.

5. Cualquier equipo de comunicaciones o redes (enrutadores, conmutadores, concentradores y paneles de conexión) está protegido contra el acceso físico no autorizado colocándolo dentro de un centro de datos seguro o en un gabinete o sala con llave.

6.4.5.2 Remoción de equipo y seguridad de equipo externo

1. Los empleados y contratistas no deben retirar propiedad (excepto dispositivos móviles) de las instalaciones sin autorización previa.

2. Se debe mantener un inventario de todos los activos de TI, que enumera los equipos que se han retirado de las instalaciones.
3. Todos los medios de almacenamiento extraídos del sitio por los proveedores de servicios (como unidades de disco y cintas defectuosas) requieren

procedimientos de destrucción y gestión física específicos, como se describe en el Estándar de clasificación de datos.

6.4.5.3 Controlar el acceso a los edificios

1. Todos los empleados, contratistas, proveedores y visitantes deben estar autorizados por el Gerente de la empresa equivalente o una autoridad de aprobación apropiada para la entrada física a las instalaciones seguras.

2. Los empleados, contratistas internos deben portar las credenciales y los visitantes o contratistas externos deben mostrarlas. Las insignias deben estar diseñadas para distinguir claramente a visitantes y empleados. Las insignias temporales deben caducar después de un período de tiempo predeterminado.

3. Todos los empleados, contratistas, proveedores y visitantes deben informar inmediatamente a las instalaciones de cualquier tarjeta de identificación perdida e informar al servicio de atención de TI.

4. Los empleados deben notificar a Seguridad de la empresa de cualquier personal sospechoso dentro de las áreas seguras.

5. Los derechos de acceso físico deben eliminarse o desactivarse tan pronto como sea posible cuando un empleado, contratista o visitante ya no necesite acceso debido a cambios de roles o abandono.

6. Los derechos de acceso físico deben ser revisados regularmente por el Gerente de la empresa o el delegado que inicialmente aprobó el acceso a las instalaciones. Esta revisión debe realizarse anualmente.

6.4.6 Seguridad de red. La red proporciona conectividad básica entre todos los usuarios finales, dispositivos de computación y almacenamiento. También proporciona acceso entre la empresa y redes externas, incluidas las redes de socios e Internet. Los controles de seguridad de la información que se implementan en la red son fundamentales para la postura de seguridad general y la falla de estos controles puede exponer la información confidencial y sensible que se maneja.

6.4.6.1 Diagramas de red

1. Se deben crear y mantener diagramas de redes lógicas para las redes de la empresa. El formato de estos diagramas se puede almacenar como copia impresa (por ejemplo, papel), copia electrónica (por ejemplo, diagrama de MS Visio) o lógico (por ejemplo, creado dinámicamente a través de aplicaciones de gestión de red).

2. Para varios sitios o varios dispositivos con el mismo diseño o un diseño similar, se debe documentar y hacer referencia a una plantilla de sitio / dispositivo para cada sitio o grupo de sistemas.
3. Los diagramas de topología de red deben mantenerse protegidos y el acceso limitado solo al personal de TI autorizado; ya que los diagramas de topología de red suelen contener direcciones IP privadas y otra información confidencial.

6.4.6.2 Flujos de tráfico entre zonas de seguridad

1. El flujo de información entre las diferentes zonas de seguridad debe realizarse a través de un punto de control apropiado. Las siguientes tecnologías de seguridad pueden proporcionar esta funcionalidad (NB: una o más de las siguientes tecnologías se pueden utilizar como punto de aplicación):

    - Cortafuegos para reforzar el flujo de información entre zonas según el puerto, el protocolo y / o la aplicación (cortafuegos de próxima generación).

    - Sistemas de detección / prevención de intrusiones para inspeccionar el tráfico en busca de actividad maliciosa y anómala.

    - Tecnología de proxy, por ejemplo, filtrado de contenido para monitorear y controlar el uso de servicios específicos, por ejemplo, correo electrónico (SMTP) y tráfico de navegación web (HTTP / S).

    - Cortafuegos de aplicaciones web (WAF) para proteger las aplicaciones web orientadas a Internet.

6.4.7 Seguridad de recursos humanos. Esta seguridad es uno de los elementos más importantes que contribuyen a la protección general de la información de Bonos y Descuentos S.A.S. La seguridad de la información es responsabilidad de todo el personal, las expectativas de seguridad de la información deben estar claramente definidas y comunicadas a todo el personal. El propósito de esta política es establecer reglas que se apliquen antes, durante y después de la terminación del empleo

6.4.7.1 Antes del empleo

1. Bonos y Descuentos S.A.S debe llevar a cabo un proceso de selección previa al empleo antes de ofrecerlo a un nuevo empleado.

2. Si el empleado está siendo contratado a través de un tercero o una agencia de personal, esa agencia debe implementar controles de detección en línea con los indicados anteriormente.

3. La información recopilada sobre empleados potenciales debe estar protegida por todas las leyes y regulaciones aplicables. El acceso debe limitarse a la "necesidad de saber".

4. Todo el personal debe estar de acuerdo en cumplir con la Política y los Estándares de Seguridad de TI de la empresa antes de que se les otorgue acceso a los sistemas de Información, Comunicación y Tecnología. Además, se le solicita al personal que firme un Acuerdo de confidencialidad.

6.4.7.2 Durante el empleo

1. La empresa debe crear y entregar un programa de concientización sobre seguridad que promueva la importancia de la seguridad para todos los empleados.

2. El programa de concientización sobre seguridad de la información debe crearse en dos partes distintas:

   - Conciencia general sobre seguridad de la información.
   - Concienciación sobre políticas y estándares de seguridad de la información.

3. Se deben mantener registros de las campañas de concientización detallando el tipo de concientización sobre seguridad de la información entregada.

4. El incumplimiento de la Política y los Estándares de Seguridad de TI puede resultar en una acción disciplinaria, consistente con los procesos y procedimientos disciplinarios de la empresa.

6.4.7.3 Terminación o cambio de empleo

1. El jefe inmediato de un empleado debe notificar inmediatamente a la empresa a través de un proceso apropiado sobre la renuncia o despido de cualquier empleado.

2. Los derechos de acceso de los empleados se modifican de manera apropiada tras el cambio o la terminación del empleo de acuerdo con el Estándar de gestión de acceso de usuarios.

3. Los derechos de acceso de los usuarios se revisan cada vez que un empleado cambia de función dentro de la empresa. La dirección es responsable de la revisión. La revisión incluye la cancelación de los derechos de acceso que ya no son necesarios a menos que haya sido explícitamente autorizado por el propietario del sistema de información o los delegados autorizados.

4. Tras la terminación del empleo, los derechos de acceso del empleado deben eliminarse de todos los sistemas. Todos los activos de TI, como el hardware, las llaves, las tarjetas de identificación y de acceso físico, el software, los datos y la documentación, los manuales deben devolverse al jefe inmediato. Los jefes son responsables de devolver todos los activos de TI.

El Cuadro 16 asigna los controles con los dominios de seguridad del Anexo A estándar ISO 27001: 2013 que se sugieren aplicar a los activos de información de la empresa Bonos y Descuentos S.A.S.

Cuadro 16. Controles Anexo A ISO 27001:2013 aplicar a Bonos y Descuentos S.A.S

| No. del Control | Objetivo de control |
|---|---|
| **A.5** | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** |
| **A.5.1** | **Orientación de la dirección para la gestión de la seguridad de la información** |
| A.5.1.1 | Políticas para la seguridad de la información |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información |
| **A.6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** |
| **A.6.1** | **Organización interna** |
| A.6.1.1 | Roles y responsabilidades para la seguridad de la información |
| A.6.1.2 | Separación de deberes |
| A.6.1.3 | Contacto con las autoridades |
| A.6.1.4 | Contacto con grupos de interés especial |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos |
| **A.6.2** | **Dispositivos Móviles y teletrabajo** |
| A.6.2.1 | Política para dispositivos móviles |
| A.6.2.2 | Teletrabajo |
| **A.7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** |
| **A.7.1** | **Antes de asumir el empleo** |
| A.7.1.1 | Selección |
| A.7.1.2 | Términos y condiciones del empleo |

Cuadro 17. (Continuación)

| No. del Control | Objetivo de control |
|---|---|
| **A.7.2** | **Durante la ejecución del empleo** |
| A.7.2.1 | Responsabilidades de la dirección |
| A.7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información |
| A.7.2.3 | Proceso disciplinario |
| **A.7.3** | **Terminación y cambio de empleo** |
| A.7.3.1 | Terminación o cambio de responsabilidades de empleo |
| **A.8** | **GESTIÓN DE ACTIVOS** |
| **A.8.1** | **Responsabilidad por los activos** |
| A.8.1.1 | Inventario de activos |
| A.8.1.2 | Propiedad de los activos |
| A.8.1.3 | Uso aceptable de los activos |
| A.8.1.4 | Devolución de activos |
| **A.8.2** | **Clasificación de la información** |
| A.8.2.1 | Clasificación de la información |
| A.8.2.2 | Etiquetado de la información |
| A.8.2.3 | Manejo de activos |
| **A.8.3** | **Manejo de medios** |
| A.8.3.1 | Gestión de medios removibles |
| A.8.3.2 | Disposición de los medios |
| A.8.3.3 | Transferencia de medios físicos |
| **A.9** | **CONTROL DE ACCESOS** |
| **A.9.1** | **Requisitos del negocio para control de accesos** |
| A.9.1.1 | Política de control de acceso |
| A.9.1.2 | Acceso a redes y a servicios en red |
| **A.9.2** | **Gestión de acceso de usuarios** |
| A.9.2.1 | Registro y cancelación del registro de usuarios |
| A.9.2.2 | Suministro de acceso de usuarios |
| A.9.2.3 | Gestión de derechos de acceso privilegiado |
| A.9.2.4 | Gestión de información de autenticación secreta de usuarios |
| A.9.2.5 | Revisión de los derechos de acceso de usuarios |
| A.9.2.6 | Retiro o ajuste de los derechos de acceso |

Cuadro 17. (Continuación)

| No. del Control | Objetivo de control |
|---|---|
| **A.9.3** | **Responsabilidades de los usuarios** |
| A.9.3.1 | Uso de información de autenticación secreta |
| **A.9.4** | **Control de acceso a sistemas y aplicaciones** |
| A.9.4.1 | Restricción de acceso a la información |
| A.9.4.2 | Procedimiento de ingreso seguro |
| A.9.4.3 | Sistema de gestión de contraseñas |
| A.9.4.4 | Uso de programas utilitarios privilegiados |
| A.9.4.5 | Control de acceso a códigos fuente de programas |
| **A.11** | **SEGURIDAD FÍSICA Y DEL ENTORNO** |
| **A.11.1** | **Áreas seguras** |
| A.11.1.1 | Perímetro de seguridad física |
| A.11.1.2 | Control de accesos físicos |
| A.11.1.3 | Seguridad de oficinas, recintos e instalaciones |
| A.11.1.4 | Protección contra amenazas externas y ambientales |
| A.11.1.5 | Trabajo en áreas seguras |
| A.11.1.6 | Áreas de despacho y carga |
| **A.11.2** | **Equipos** |
| A.11.2.1 | Ubicación y protección de los equipos |
| A.11.2.2 | Servicios de suministro |
| A.11.2.3 | Seguridad del cableado |
| A.11.2.4 | Mantenimiento de equipos |
| A.11.2.5 | Retiro de activos |
| A.11.2.6 | Seguridad de activos y equipos fuera de la oficina |
| A.11.2.7 | Disposición segura o reutilización de equipos |
| A.11.2.8 | Equipos de usuario desatendido |
| A.11.2.9 | Políticas de escritorio limpio y pantalla limpia |
| **A.12** | **SEGURIDAD DE LAS OPERACIONES** |
| **A.12.1** | **Procedimientos operacionales y responsabilidades** |
| A.12.1.1 | Procedimientos de operación documentados |
| A.12.1.2 | Gestión de cambios |
| A.12.1.3 | Gestión de capacidad |
| A.12.1.4 | Separación de los ambientes de desarrollo, pruebas, y operación |
| **A.12.2** | **Protección contra códigos maliciosos** |

Cuadro 17. (Continuación)

| No. del Control | Objetivo de control |
|---|---|
| A.12.2.1 | Controles contra códigos maliciosos |
| **A.12.3** | **Proteger contra la perdida de datos** |
| A.12.3.1 | Respaldo de la información |
| **A.12.4** | **Registro y seguimiento** |
| A.12.4.1 | Registro de eventos |
| A.12.4.2 | Protección de la información de registro |
| A.12.4.3 | Registros del administrador y del operador |
| A.12.4.4 | Sincronización de reloj |
| **A.12.5** | **Control de software operacional** |
| A.12.5.1 | Instalación de software en sistemas operativos |
| **A.12.6** | **Gestión de la vulnerabilidad técnica** |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas |
| A.12.6.2 | Restricciones sobre la instalación de software |
| **A.12.7** | **Consideraciones sobre auditorías de sistemas de información** |
| A.12.7.1 | Controles de auditorías de sistemas de información |
| **A.13** | **SEGURIDAD DE LAS COMUNICACIONES** |
| **A.13.1** | **Gestión de la seguridad de las redes** |
| A.13.1.1 | Controles de redes |
| A.13.1.2 | Seguridad de los servicios de red |
| A.13.1.3 | Separación en las redes |
| **A.13.2** | **Transferencia de información** |
| A.13.2.1 | Políticas y procedimientos de transferencia de información |
| A.13.2.2 | Acuerdos sobre transferencia de información |
| A.13.2.3 | Mensajería electrónica |
| A.13.2.4 | Acuerdos de confidencialidad o de no divulgación |
| **A.14** | **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** |
| **A.14.1** | **Requisitos de seguridad de los sistemas de información** |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información |
| A.14.1.2 | Seguridad de servicio de las aplicaciones en redes publicas |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones |
| **A.14.2** | **Seguridad en los procesos de desarrollo y soporte** |
| A.14.2.1 | Políticas de desarrollo seguro |
| A.14.2.2 | Procedimiento de control de cambios en sistemas |

Cuadro 17. (Continuación)

| No. del Control | Objetivo de control |
|---|---|
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación |
| A.14.2.4 | Restricción en los cambios a los paquetes de software |
| A.14.2.5 | Principios de construcción de los sistemas seguros |
| A.14.2.6 | Ambiente seguro de desarrollo |
| A.14.2.7 | Desarrollo externamente contratado |
| A.14.2.8 | Pruebas de seguridad de sistemas |
| A.14.2.9 | Prueba de aceptación de sistemas |
| **A.14.3** | **Datos de pruebas** |
| A.14.3.1 | Protección de datos de pruebas |
| **A.15** | **RELACIONES CON LOS PROVEEDORES** |
| **A.15.1** | **Seguridad de la información en las relaciones con los proveedores** |
| A.15.1.1 | Política de seguridad de la información para las relaciones con proveedores |
| A.15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores |
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación |
| **A.15.2** | **Gestión de la prestación de servicios de proveedores** |
| A.15.2.1 | Seguimiento y revisión a los servicios proveedores |
| A.15.2.2 | Gestión de cambios en los servicios de los proveedores |
| **A.16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** |
| **A.16.1** | **Gestión de incidentes y mejoras en la seguridad de la información** |
| A.16.1.1 | Responsabilidades y procedimientos |
| A.16.1.2 | Reporte de eventos de seguridad de la información |
| A.16.1.3 | Reporte de debilidades de seguridad de la información |
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información |
| A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información |
| A.16.1.7 | Recolección de evidencia |
| **A.17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO** |
| **A.17.1** | **Continuidad de seguridad de la información** |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información |

Cuadro 17. (Continuación)

| No. del Control | Objetivo de control |
|---|---|
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información |
| **A.17.2** | **Redundancia** |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información. |
| **A.18** | **CUMPLIMIENTO** |
| **A.18.1** | **Cumplimiento de requisitos legales y contractuales** |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales |
| A.18.1.2 | Derechos de propiedad intelectual |
| A.18.1.3 | Protección de registros |
| A.18.1.4 | Privacidad y protección de información de datos personales |
| A.18.2 | **Revisiones de seguridad de la información** |
| A.18.2.1 | Revisión independiente de la seguridad de la información |
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad |
| A.18.2.3 | Revisión del cumplimiento técnico |

Fuente: ISO 27001:2013. Anexo A

# 7 CONCLUSIONES

Con base en los resultados del análisis de brechas que se ha realizado en la empresa Bonos y Descuentos SAS, es posible que el nivel de madurez sea aceptable con el diseño del SGSI, la protección de la información se puede implementar sistemáticamente en toda la organización y garantizar que se cumplan todos los estándares requeridos, en forma de descripción de las condiciones actuales, así como la propuesta de mejora de la seguridad en el futuro que se puede utilizar como referencia para elaborar estrategias de planificación del SGSI, de esta forma optimizar el rendimiento y apoyo en el logro de estrategias comerciales, en donde las empresas pueden verificar ante terceros que la información confidencial se maneja de forma segura. Esto contribuye a una mejor imagen externa y a generar confianza, lo que a su vez significa una ventaja competitiva.

Se analizó y se gestionó los riesgos en los activos de información de Bonos y Descuentos S.A.S, con esto se evidencio que es muy importante un aseguramiento de los activos, donde se pueda determinar las vulnerabilidades y amenazas, para establecer una estructura y la planificación de medidas orientada al riesgo, utilizando los recursos de manera eficiente realizando inversiones en los lugares correctos y los gastos generales puedan reducirse a largo plazo.

Aplicando los controles “SOA – Declaración de aplicabilidad” de la Norma Internacional ISO 27001:2013 para la mitigación de riegos de la empresa Bonos y Descuentos S.A.S, se determina la importancia de establecer los controles adecuados para la optimización de la seguridad de la información en la empresa garantizando que los activos patentados (por ejemplo, propiedad intelectual, datos de personal o datos financieros), así como los datos confiados por clientes o terceros, estén adecuadamente protegidos contra todas y cada una de las amenazas y de esta forma, contrarrestar al máximo el riesgo que los incidentes de seguridad interrumpan la continuidad del negocio.

Con las políticas y controles propuestos para Bonos y Descuentos S.A.S, la empresa proporciona a los clientes la garantía de que la seguridad de la información se toma en serio y de que la organización tiene un sistema sólido de procesos para proteger sus datos, así mismo se asegura de cumplir con todos los requisitos regulatorios y contractuales, lo que evitara las violaciones a las normas legales y los acuerdos establecidos donde podrían resultar en fuertes multas, también ofrece a la empresa más seguridad operativa y jurídica.

# 8 RECOMENDACIONES

La empresa debe estar revisando el aseguramiento de los activos de información en donde cada uno de ellos debe estar protegido por las políticas y los controles adecuados determinando sus valores potenciales en las diferentes oportunidades de negocio, evitando la interrupción de las actividades comerciales dentro de la organización y un posible ataque por personas internas y externas.

Se recomienda realizar un pentest periódicamente para identificar amenazas y / o vulnerabilidades nuevas o modificadas, en caso de ser detectadas, se sugiere volver a calcular el riesgo e identificar y documentar los cambios necesarios en las decisiones de tratamiento de riesgos y los controles de seguridad. Estos cambios deben acordarse con la dirección e implementarse.

Es necesario la creación de una bitácora donde se registren los riesgos incluyendo la fecha de la última evaluación, una descripción del riesgo, una estimación del impacto y la probabilidad, los controles de mitigación y una declaración de acción requerida, con la fecha objetivo y el propietario, con el fin de gestionar los cambios en los activos de información en caso de presentarse una nueva función comercial.

Se sugiere monitorear periódicamente por parte de la compañía el funcionamiento y la efectividad de los controles de la declaración de aplicabilidad SOA, para detectar un posible deterioro, así como los aspectos de comportamiento asociados con los procesos del SGSI, con el fin de iniciar una acción correctiva.

La gerencia necesita revisar el SGSI para asegurar su adecuación, utilidad y efectividad continua, esta verificación debe basarse en la información de los usuarios, resultados de análisis previas, informes de auditoría, registros de procedimientos y evaluaciones comparativas internas y externas. El resultado de los datos debe ser específico sobre los cambios, identificando modificaciones a los procedimientos que afectan la seguridad de la información mostrando dónde se pueden realizar mejoras de eficiencia para implementarlas y mantenerlas.

## BIBLIOGRAFÍA


ACADEMIA. [Sitio web]. Norma técnica NTC-ISO/IEC Colombiana 27001 tecnología de la información. técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. requisitos. [Consulta: 31 de mayo 2021]. Disponible en: https://www.academia.edu/40913480/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_REQUISITOS

AVAST. ¿Qué es el Malware?. [Sitio web]. [Consulta: 23 de mayo 2021]. Disponible en: https://www.avast.com/es-es/c-malware

AVAST. ¿Qué es el Phishing?. [Sitio web]. [Consulta: 23 de mayo 2021]. Disponible en: https://www.avast.com/es-es/c-phishing

CALDER, Alan. Information Security Based on ISO 27001/ISO 27002: A Management Guide. 2 ed. Bolduque.: Van Haren, 2009. p.85.(Best Practice). ISBN 908-75-3540-6

CONFERENCE ON EMERGING SECURITY INFORMATION, SYSTEMS AND TECHNOLOGIES. (2: 25-31, AGOSTO, 2008: L'Esterel, France). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. L'Esterel: IEEE, 2008, pp. 224–231

CONFERENCIA INTERNACIONAL CARNAHAN SOBRE TECNOLOGÍA DE SEGURIDAD. (1: 18-21, OCTUBRE, 2011: Barcelona, España). Modelo de organización de la gestión de la Seguridad Física y Lógica basado en las normas ISO 31000 e ISO 27001. Barcelona: IEEE, 2011, 5 p.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional de Confianza y Seguridad Digital. [Sitio Web]. Colombia (2020). pp. 16-26, 34– 44. [Consulta: 14 de abril 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

EcuCERT – AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES. Vulnerabilidad de tipo Zero Day pone en alto riesgo a sus usuarios. [Sitio web]. [Consulta: 31 de mayo 2021]. Disponible en: https://www.ecucert.gob.ec/vulnerabilidades.html

EcuCERT – AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES. Conceptos sobre ciberseguridad. [Sitio web]. [Consulta: 31 de mayo 2021]. Disponible en: https://www.ecured.cu/Confidencialidad

ENISA - EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. Risk Management /Risk Assessment. [Sitio web]. [Consultado 25 de mayo 2021]. Disponible en: http://www.enisa.europa.eu/rmra

ESET SECURITY REPORT. Latinoamérica 2018. [Sitio web]. [Consulta: 14 de abril 2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

FIGUEROA PEREZ, Omaira y MALAGON SAENZ, Nohora Esther. Propuesta De Políticas De Seguridad De La Información Para La Institución Educativa De Educación Básica y Media Del Departamento De Boyacá, Basadas En La Norma ISO 27001:2013 [en línea]. Monografia. Universidad Nacional Abierta y a Distacina – UNAD, 2017. [Consulta: 14 de abril 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/11881

FORBES. [Sitio web]. Information Security and Risk Management, Worldwide, 2018-2024, 1Q20 Update Published. [Consulta: 25 de mayo 2021]. Disponible en: https://www.forbes.com/sites/louiscolumbus/2020/08/09/cybersecurity-spending-to-reach-123b-in-2020/?sh=7fe1d5a6705f

FROSDICK, Steve. The techniques of risk analysis are insufficient in themselves. Disaster Prevention and Management an International Journal, 1997, nro 6, pp.165-177

GÓMEZ FERNÁNDEZ, Luis. y FERNÁNDEZ RIVERO, Pedro Pablo. [Sitio web]. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. [Consulta: 25 de mayo 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=5

GREGOR, Shirley. La naturaleza de la teoría en los sistemas de información. Universidad Nacional de Australia. Canberra. 2006, vol. 30, nro. 3, pp. 611-642

GUIJARRO, Hanna. IT GOVERNANCE EUROPEAN BLOG. [Sitio web]. 9 razones para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). [Consulta 25 de mayo 2021]. Disponible en: https://www.itgovernance.eu/blog/es/9-razones-para-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi

INCIBE-INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. [Consultado 31 de mayo 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

ISO/IEC 27002:2013. [Sitio web]. Information technology — Security Techniques — Code of practice for information security controls. [Consulta: 25 de mayo 2021]. Disponible en: https://www.iso.org/standard/54533.html

ISO/CEI 27001:2013. [Sitio web]. Information technology — Security techniques — Information security management systems — Requirements. [Consulta: 25 de mayo 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

MILCOM COMUNICACIONES DE PROCEDIMIENTOS PARA OPERACIONES CENTRADAS EN LA RED: CREANDO LA FUERZA DE INFORMACIÓN. (1: 28, OCTUBRE, 2001: Vienna, Austria). Revisión de la defensa en profundidad: riesgo cualitativo Metodología de análisis para operaciones complejas centradas en la red. IEEE, 2001, 10 p.

MOLANO ESPINEL, Rafael Antonio. Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa MARKET MIX, [en línea]. Trabajo de grado. Universidad Católica de Colombia, 2017.[Consulta: 25 de mayo 2021]. Disponible en: https://repository.ucatolica.edu.co/jspui/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, manual de Gobierno Digital. [Consulta: 25 de mayo 2021]. Disponible en: https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, modelo de Gestión de Riesgos de Seguridad Digital - MinTIC. [Consulta: 31 de mayo 2021]. Disponible en: https://mintic.gov.co/portal/604/articles-61854_documento.docx

NACIPUCHA CUMBE, Julio Cesar. Análisis y diseño para un modelo de Gestión de Seguridad de la Información basados en normas ISO/IEC 27001:2013 para la empresa Artehogar en la ciudad de Guayaquil [en línea].Trabajo de grado. Universidad de Guayaquil, 2019. [Consulta: 23 de mayo 2021]. Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/44410/1/Tesis%20Nacipucha%20%2802%2009%29%20impresion.pdf

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. [Sitio web]. Framework for Improving Critical Infrastructure Cybersecurity de National Institute of Standards and Technology. [Consulta: 26 de mayo 2021]. Disponible en: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Análisis Forense Digital. [Sitio web]. [Consulta: 31 de mayo 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. [Sitio web]. MAGERIT versión 3 (versión español): Metodología de Análisis y gestión de riesgos de los sistemas de información. [Consulta: 14 de abril 2021]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

PORTAL DE ISO 27000 EN ESPAÑOL. [Sitio web]. Glosario. [Consulta: 14 de abril 2021]. Disponible en:: http://www.iso27000.es/glosario.html#section10c

PROCEEDINGS OF THE FIFTH INTERNATIONAL ENTERPRISE DISTRIBUTED OBJECT COMPUTING CONFERENCE.(5: 17-20, SEPTIEMBRE, 2002: Lausanne, Switzerland). Model-based risk assessment to improve enterprise security. Lausanne: IEEE, 2002, pp.17-20

SUAREZ GONZÁLEZ, Rafael. Análisis de activos de información para un sistema misional basados en la metodología MAGERIT V3 y la norma ISO 27001:2013 [en línea]. Trabajo de grado. Universidad Nacional Abierta y a Distancia UNAD CEAD Jose Acevedo y Gomez, 2018. [Consultado 25 de mayo 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/19571/80803746.pdf?sequence=3&isAllowed=y

THE SECURITY COMMITTEE. [Sitio web]. The implementation programme of the Cyber Security Strategy. [Consulta: 25 de mayo 2021]. Disponible en: http://www.turvallisuuskomitea.fi/index.php/en/kyberturvallisuusstrategia/toimeenpanoohjelma

UNIVERSIDAD NACIONAL DE COLOMBIA. [Sitio web]. Ciclo de control P.H.V.A. [Consulta: 14 de abril 2021]. Disponible en: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4010014/Contenidos/Capitulo1/Pages/1.4/148Ciclo_Control_PHVA.htm

,

VON SOLMS, Rossouw. Gestión de la seguridad de la información versión 3 el código de prácticas para la gestión de la seguridad de la información. *Gestión de la información y seguridad informática*. 1998, nro 80, pp. 224-225.

**ANEXO A**
(Informativo)

Declaración de aplicabilidad “SOA” de la norma de ISO/IEC 27001:2013

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| **A.5** | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** | | | |
| **A.5.1** | **Orientación de la dirección para la gestión de la seguridad de la información** | | | |
| A.5.1.1 | Políticas para la seguridad de la información | Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y las partes externas pertinentes. | SI | Para manejar datos confidenciales de los clientes y de la empresa. |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información | Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. | SI | Estas políticas deben ser revisadas cada seis meses, ya que pueden surgir cambios en la empresa y/o actualizaciones en los estándares o normas. |
| **A.6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| **A.6.1** | **Organización interna** | | | |
| A.6.1.1 | Roles y responsabilidades para la seguridad de la información | Se debe definir y asignar todas las responsabilidades de la seguridad de la información. | SI | Es importante definir los roles y responsabilidades en cada una de las tareas asignadas |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.6.1.2 | Separación de deberes | Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización. | SI | Se deben separar las funciones con el fin de evitar algunos tipos de fraudes al tener acceso a diversas tareas. |
| A.6.1.3 | Contacto con las autoridades | Se deben tener contactos apropiados con las autoridades pertinentes | SI | Al presentarse algún fraude es necesario tener el contacto con las autoridades para lograr un apropiado escalamiento o reporte de los mismos para su manejo. |
| A.6.1.4 | Contacto con grupos de interés especial | Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. | SI | Es necesario para el asesoramiento o implementación del SGSI |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. | SI | Se debe establecer el procedimiento y un líder en la seguridad de la información de los proyectos garantizando su ejecución. |
| **A.6.2** | **Dispositivos Móviles y teletrabajo** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.6.2.1 | Política para dispositivos móviles | Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | SI | Se debe establecer una política en la empresa donde limite el uso de dispositivos móviles en los tiempos laborales con el fin de evitar una fuga de información. |
| A.6.2.2 | Teletrabajo | Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | SI | Se requiere una conexión VPN para la utilización de los aplicativos de la empresa. |
| **A.7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | | | |
| **A.7.1** | **Antes de asumir el empleo** | | | |
| A.7.1.1 | Selección | Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. | SI | Se requiere una persona especializada en selección de personal y gestión de los estudios de seguridad. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.7.1.2 | Términos y condiciones del empleo | Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. | SI | Se debe dar cumplimiento a las políticas de confidencialidad establecidas para personal de la empresa. |
| **A.7.2** | **Durante la ejecución del empleo** | | | |
| A.7.2.1 | Responsabilidades de la dirección | La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | SI | Se deben establecer las políticas y los procedimientos en la seguridad de la información, para que esta sea exigida por la dirección |
| A.7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | SI | Es necesario realizar capacitaciones de forma periódica de acuerdo a las actualizaciones de seguridad establecida por la empresa. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.7.2.3 | Proceso disciplinario | Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | SI | De acuerdo a la gravedad de la falta o de la violación de seguridad esta será tratada bajo los reglamentos de la empresa o será informada a las autoridades competentes de ser necesario. |
| **A.7.3** | **Terminación y cambio de empleo** | | | |
| A.7.3.1 | Terminación o cambio de responsabilidades de empleo | Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir. | SI | Se deben establecer políticas de bloqueo de accesos. |
| **A.8** | **GESTIÓN DE ACTIVOS** | | | |
| **A.8.1** | **Responsabilidad por los activos** | | | |
| A.8.1.1 | Inventario de activos | Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | SI | Es necesario la actualización periódicamente de los activos con el fin de tener control de los cambios realizados en la empresa |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.8.1.2 | Propiedad de los activos | Los activos mantenidos en el inventario deben tener un propietario. | SI | Los empleados deben ser responsables por los activos que les fueron asignados, así la empresa pueda realizar monitoreos y tenga el conocimiento en donde se encuentran. |
| A.8.1.3 | Uso aceptable de los activos | Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | SI | Se debe firmar un acuerdo de buen uso y cuidado adecuado de los activos de información. |
| A.8.1.4 | Devolución de activos | Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se entregan a su cargo, al terminar su empleo, contrato o acuerdo. | SI | Estos activos deben ser devueltos a la empresa en el estado en que fueron entregados para poder salvaguardar estos mismos. |
| **A.8.2** | **Clasificación de la información** | | | |
| A.8.2.1 | Clasificación de la información | La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada. | SI | Se deben crear perfiles de acceso a la información de acuerdo al perfil de sus funciones y/o área de trabajo |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.8.2.2 | Etiquetado de la información | Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización. | SI | Es necesario la creación de procedimientos que permita clasificar la información |
| A.8.2.3 | Manejo de activos | Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización. | SI | Con los procedimientos establecidos se tendrá el control de los activos de acuerdo a su clasificación. |
| **A.8.3** | **Manejo de medios** | | | |
| A.8.3.1 | Gestión de medios removibles | Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización. | SI | Se crean los procedimientos para el uso adecuado de los medios removibles |
| A.8.3.2 | Disposición de los medios | Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. | SI | Se establece el procedimiento para la disposición final de los bienes en desuso u obsoletos. |
| **A.9** | **CONTROL DE ACCESOS** | | | |
| **A.9.1** | **Requisitos del negocio para control de accesos** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.9.1.1 | Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | SI | De acuerdo con el perfil y el rol de las funciones se establecen las políticas de acceso a las aplicaciones, información confidencial, etc. |
| A.9.1.2 | Acceso a redes y a servicios en red | Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. | SI | La red debe estar diseñada por VLAN que permita el acceso seguro a la infraestructura según los roles y funciones de los usuarios. |
| **A.9.2** | **Gestión de acceso de usuarios** | | | |
| A.9.2.1 | Registro y cancelación del registro de usuarios | Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | SI | Se debe crear un formato en donde se realice la solicitud y cancelación de Roles, el formato debe ser diligenciado por el jefe inmediato. |
| A.9.2.2 | Suministro de acceso de usuarios | Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | SI | Con el formato creado se realiza estos requerimientos, esta solicitud debe ser enviada por el superior inmediato. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. | SI | Con el formato creado se realiza estos requerimientos de acuerdo al perfil y rol del usuario, la solicitud es enviada por el superior inmediato. |
| A.9.2.4 | Gestión de información de autenticación secreta de usuarios | La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. | SI | Este es controlado mediante el acuerdo de confidencialidad suscrito por el empleador y empleado. |
| A.9.2.5 | Revisión de los derechos de acceso de usuarios | Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. | SI | El control de acceso de los usuarios debe ser revisado cada seis meses por parte del jefe inmediato |
| A.9.2.6 | Retiro o ajuste de los derechos de acceso | Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. | SI | La solicitud debe ser diligenciada por el jefe inmediato en el formato predeterminado. |
| **A.9.3** | **Responsabilidades de los usuarios** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.9.3.1 | Uso de información de autenticación secreta | Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. | SI | A través de las políticas de confidencialidad de Bonos y Descuentos SAS |
| **A.9.4** | **Control de acceso a sistemas y aplicaciones** | | | |
| A.9.4.1 | Restricción de acceso a la información | El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. | SI | Se debe contar con un formato de solicitud donde realicen estos tipos de requerimientos dependiendo del rol y las funciones realizadas, el formato será diligenciado por el superior |
| A.9.4.2 | Procedimiento de ingreso seguro | Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. | SI | Implementación de un Directorio Activo (DA) que permita brindar seguridad con contraseñas complejas a los sistemas de información. |
| A.9.4.3 | Sistema de gestión de contraseñas | Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. | SI | Establecer políticas a través del Directorio Activo y por un portal WEB para asegurar las contraseñas. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.9.4.4 | Uso de programas utilitarios privilegiados | Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones. | SI | Con las políticas del Directorio Activo se restringen la instalación de aplicaciones a todos los usuarios de la empresa. |
| A.9.4.5 | Control de acceso a códigos fuente de programas | Se debe registrar el acceso a los códigos fuente de los programas. | SI | Se debe crear un repositorio de código fuente donde solo tenga acceso los desarrolladores. |
| **A.10** | **CRIPTOGRAFIA** | | | |
| **A.10.1** | **Controles criptográficos** | | | |
| A.10.1.1 | Política sobre el uso de controles criptográficos | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. | NO | Debido a que no se utilizan algoritmos para la encriptación de la información |
| A.10.1.2 | Gestión de llaves | Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante su ciclo de vida. | NO | Ya que en la organización no se utilizan llaves criptográficas. |
| **A.11** | **SEGURIDAD FÍSICA Y DEL ENTORNO** | | | |
| **A.11.1** | **Áreas seguras** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.11.1.1 | Perímetro de seguridad física | Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. | SI | Se debe crear un centro de datos aislado del personal y con un control de acceso como tarjetas de proximidad, lectores biométricos y/o cctv. |
| A.11.1.2 | Control de accesos físicos | Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite acceso a personal autorizado. | SI | Mediante lectores biométricos a doble autenticación. |
| A.11.1.3 | Seguridad de oficinas, recintos e instalaciones | Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. | SI | Implementación de alarmas y contratación de seguridad privada |
| A.11.1.4 | Protección contra amenazas externas y ambientales | Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | SI | Se debe contar con una póliza sistema contraincendios un datacenter alterno que se encuentre geográficamente en otro lugar. |
| A.11.1.5 | Trabajo en áreas seguras | Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. | SI | Se debe buscar asesorías con una ARL para el diseño del procedimiento de las áreas seguras. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.11.1.6 | Áreas de despacho y carga | Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | SI | Es necesario contar con una zona de parqueo y personal de vigilancia. |
| **A.11.2** | **Equipos** | | | |
| A.11.2.1 | Ubicación y protección de los equipos | Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | SI | La ubicación de los equipos debe estar aislada de las personas externas |
| A.11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | SI | Se debe contar con reguladores de energía y una UPS |
| A.11.2.3 | Seguridad del cableado | El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño. | SI | Es necesario que el cableado este protegido con canaletas seguras. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.11.2.4 | Mantenimiento de equipos | Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. | SI | Se deben contratar servicios para realizar mantenimientos preventivos de manera periódica |
| A.11.2.5 | Retiro de activos | Los equipos, información o software no se deben retirar de su sitio sin autorización previa. | SI | Es necesario la creación de un procedimiento para retiro los equipos y un formato que será autorizado por el jefe inmediato. |
| A.11.2.6 | Seguridad de activos y equipos fuera de la oficina | Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. | SI | Se debe adquirir una póliza que proteja los equipos contra robo o daño. |
| A.11.2.7 | Disposición segura o reutilización de equipos | Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó. | SI | Es necesario la creación de políticas de verificación, de reasignación del hardware y software |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.11.2.8 | Equipos de usuario desatendido | Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. | SI | Los equipos que se encuentran en desuso deben ser almacenados para posterior disposición final. |
| A.11.2.9 | Políticas de escritorio limpio y pantalla limpia | Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. | SI | Se requiere la creación de políticas con restricciones de notas sensibles en los escritorios como contraseñas, direcciones IP, usuarios, entre otros |
| **A.12** | **SEGURIDAD DE LAS OPERACIONES** | | | |
| **A.12.1** | **Procedimientos operacionales y responsabilidades** | | | |
| A.12.1.1 | Procedimientos de operación documentados | Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan. | SI | Los procedimientos deben ser divulgados y publicados internamente para que los empleados tengan acceso a la información. |
| A.12.1.2 | Gestión de cambios | Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. | SI | Los cambios se deben dar a conocer previamente para realizar una planeación sobre los pasos a seguir evitando errores para minimizar los riesgos. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.12.1.3 | Gestión de capacidad | Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | SI | Los equipos deben tener mantenimiento preventivo de ser necesario reacondicionamiento dentro de su vigencia |
| A.12.1.4 | Separación de los ambientes de desarrollo, pruebas, y operación | Se deben separar los ambientes de desarrollo ,prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. | SI | Cada ambiente debe estar en una red distinta, no debe existir una conexión directa entre los ambientes |
| **A.12.2** | **Protección contra códigos maliciosos** | | | |
| A.12.2.1 | Controles contra códigos maliciosos | Se deben implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos. | SI | Es necesario la implementación de licencias de antivirus, antimalware, antispyware, etc. |
| **A.12.3** | **Proteger contra la perdida de datos** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | SI | Las copias de respaldo se deben realizar periódicamente de acuerdo a la criticidad. |
| **A.12.4** | **Registro y seguimiento** | | | |
| A.12.4.1 | Registro de eventos | Se deben elaborar, conservar y revisar regularmente los registros a cerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información | SI | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias |
| A.12.4.2 | Protección de la información de registro | Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado | SI | Se deben establecer controles de acceso y vigilancia privada |
| A.12.4.3 | Registros del administrador y del operador | Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. | SI | Se requieren almacenar estos registros por un tiempo determinado para futuras auditorias |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.12.4.4 | Sincronización de reloj | Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. | SI | Deben sincronizados por medio de un servidor NTP y así manejar un único horario en los sistemas de información. |
| **A.12.5** | **Control de software operacional** | | | |
| A.12.5.1 | Instalación de software en sistemas operativos | Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. | SI | Se deben implementar un formato para instalación y desinstalación de software. |
| **A.12.6** | **Gestión de la vulnerabilidad técnica** | | | |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | SI | Es necesario realizar periódicamente en los distintos sistemas de información el análisis de vulnerabilidades para mitigar los riesgos. |
| A.12.6.2 | Restricciones sobre la instalación de software | Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios. | SI | A través del Directorio Activo ejecutar las restricciones para realizar cualquier tipo de instalación. |
| **A.12.7** | **Consideraciones sobre auditorías de sistemas de información** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.12.7.1 | Controles de auditorías de sistemas de información | Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. | SI | Para verificar cada uno de los controles a los sistemas de información. |
| **A.13** | **SEGURIDAD DE LAS COMUNICACIONES** | | | |
| **A.13.1** | **Gestión de la seguridad de las redes** | | | |
| A.13.1.1 | Controles de redes | Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. | SI | Para prevenir fuga de información se deben crear distintas Vlan. |
| A.13.1.2 | Seguridad de los servicios de red | Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. | SI | Se deben identificar las configuraciones y restricciones de la red que permitan brindar la seguridad necesaria |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.13.1.3 | Separación en las redes | Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. | SI | Es necesario que la red y sus dispositivos como switch, router, sean configurados con Vlan para separación de los diversos grupos de red |
| **A.13.2** | **Transferencia de información** | | | |
| A.13.2.1 | Políticas y procedimientos de transferencia de información | Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. | SI | Se deben implementar las respectivas políticas, procedimientos y formatos para la protección de la transferencia de la información. |
| A.13.2.2 | Acuerdos sobre transferencia de información | Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas. | SI | Los acuerdos de confidencialidad deben estar bien definidos en los contratos externos para la transferencia de la información de forma segura y confiable. |
| A.13.2.3 | Mensajería electrónica | Se debe proteger adecuadamente la información incluida en la mensajería electrónica. | SI | Es necesario la creación de los acuerdos de confidencialidad para el uso de mensajería electrónica. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.13.2.4 | Acuerdos de confidencialidad o de no divulgación | Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | SI | Se debe revisar periódicamente los acuerdos de confidencialidad. |
| **A.14** | **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** | | | |
| **A.14.1** | **Requisitos de seguridad de los sistemas de información** | | | |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. | SI | Es necesario la implementación de procedimientos que contenga los requisitos para la realización de nuevos proyectos. |
| A.14.1.2 | Seguridad de servicio de las aplicaciones en redes publicas | La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. | SI | Se debe realizar la implementación de sistema de protección pública como WAF, certificado SSL, etc. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones | La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado la alteración no autorizada de mensajes, la divulgación no autorizada y la divulgación o reproducción de mensajes no autorizados. | SI | Se debe establecer una política de confidencialidad de la información para salvaguardar las transacciones de servicios. |
| **A.14.2** | **Seguridad en los procesos de desarrollo y soporte** | | | |
| A.14.2.1 | Políticas de desarrollo seguro | Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización. | SI | Los desarrollos deben contar con los parámetros necesarios garantizando su desarrollo seguro |
| A.14.2.2 | Procedimiento de control de cambios en sistemas | Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | SI | Es necesario documentar cada uno de los cambios a realizar en las aplicaciones. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. | SI | Es necesario la realización de pruebas para la verificación de que las nuevas plataformas soporten las operaciones de la compañía. |
| A.14.2.4 | Restricción en los cambios a los paquetes de software | Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente. | SI | Crear políticas a través del Directorio Activo para contrarrestar estas modificaciones. |
| A.14.2.5 | Principios de construcción de los sistemas seguros | Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros , y aplicarlos a cualquier actividad de implementación de sistemas de información. | SI | Para el sistema seguro es necesario la implementación de un protocolo. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.14.2.6 | Ambiente seguro de desarrollo | Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas . | SI | Con la elaboración de un procedimiento adecuado se protege los ambientes de desarrollo como repositorios, restricciones en firewall y controles de acceso |
| A.14.2.7 | Desarrollo externamente contratado | La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. | SI | Se debe realizar seguimiento a los contratos periódicamente hasta que se de el cumplimiento total. |
| A.14.2.8 | Pruebas de seguridad de sistemas | Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad. | SI | Es necesario realizar pruebas de pentest de forma periódica para identificar las vulnerabilidades y posteriormente mitigarlas |
| A.14.2.9 | Prueba de aceptación de sistemas | Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados . | SI | Se deben realizar testeos para la prevención de caídas o fallos al momento de entrar a producción |
| **A.14.3** | **Datos de pruebas** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.14.3.1 | Protección de datos de pruebas | Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. | SI | Ya que son analizados y estos contienen mucha información sustancial. |
| **A.15** | **RELACIONES CON LOS PROVEEDORES** | | | |
| **A.15.1** | **Seguridad de la información en las relaciones con los proveedores** | | | |
| A.15.1.1 | Política de seguridad de la información para las relaciones con proveedores | Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar. | SI | Se deben establecer contratos de prestación de servicios y acuerdos de confidencialidad. |
| A.15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | SI | Es necesario que en los contratos realizados se detallen los requisitos necesarios en la seguridad de la información |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | SI | Es necesario solicitar a los proveedores acuerdos para proteger la empresa de los riesgos ocurridos por la operación de un proveedor. |
| **A.15.2** | **Gestión de la prestación de servicios de proveedores** | | | |
| A.15.2.1 | Seguimiento y revisión a los servicios proveedores | Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. | SI | Periódicamente se debe realizar seguimiento y auditorías a los servicios prestados. |
| A.15.2.2 | Gestión de cambios en los servicios de los proveedores | Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio | SI | Si mediante los contratos por prestación de servicios ya establecidos debe ir un ítem que diga servicios conexos el cual incluye la parte de suministros. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| | | involucrados, y la reevaluación de los riesgos. | | |
| **A.16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | | | |
| **A.16.1** | **Gestión de incidentes y mejoras en la seguridad de la información** | | | |
| A.16.1.1 | Responsabilidades y procedimientos | Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | SI | Para poder llevar un orden al momento de que se materialice un incidente. |
| A.16.1.2 | Reporte de eventos de seguridad de la información | Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. | SI | Para poder realizar las gestiones pertinentes dependiendo del incidente. |
| A.16.1.3 | Reporte de debilidades de seguridad de la información | Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | SI | Es necesario capacitar a los empleados en técnicas básicas para la identificación de vulnerabilidades |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Los eventos de seguridad de la información se deben evaluar y se debe decir si se van a clasificar como incidentes de seguridad de la información. | SI | Se debe identificar los incidentes dependiendo si se trata de una caída global o un ataque. |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. | SI | Es necesario la creación de procedimientos para dar respuesta de los incidentes de acuerdo a su criticidad |
| A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. | SI | Se deben realizar capacitaciones periódicas alos empleados de TI con los aspectos relacionados de la seguridad de la información |
| A.16.1.7 | Recolección de evidencia | La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que puede servir como evidencia. | SI | Es necesario la creación de procedimientos dependiendo la criticidad del caso y tener las pruebas de lo cometido para tomar las acciones pertinentes. |
| **A.17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO** | | | |
| **A.17.1** | **Continuidad de seguridad de la información** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | La organización debe determinar sus requisitos para la seguridad de la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres. | SI | Se debe elaborar un plan de contingencia ´garantizando la continuidad de la operación. |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | La organización debe establecer, documentar, implementar y mantener procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. | SI | Es necesario tener los planes de contingencia vigentes en caso de requerirlos |
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados , con el fin de asegurar que son válidos y eficaces durante situaciones adversas. | SI | Se deben programar pruebas periódicas en la operación de contingencia garantizando así la continuidad del negocio en caso de ser requerido o de una falla grave. |
| **A.17.2** | **Redundancia** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | SI | Para soportar las operaciones en cualquier caso: caída de fluido eléctrico, caída del ISP, etc. |
| **A.18** | **CUMPLIMIENTO** | | | |
| **A.18.1** | **Cumplimiento de requisitos legales y contractuales** | | | |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización. | SI | Es necesario estar actualizados con las normas vigentes ya que estas pueden ser derogadas. |
| A.18.1.2 | Derechos de propiedad intelectual | Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos , de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. | SI | Los desarrollos que se realicen en la compañía deben estar como propiedad intelectual |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.18.1.3 | Protección de registros | Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. | SI | Es necesario establecer un procedimiento para salvaguardar los registros de la organización. |
| A.18.1.4 | Privacidad y protección de información de datos personales | Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. | SI | Mediante la ley 1581 de 2012 |
| A.18.1.5 | Reglamentación de controles criptográficos | Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | NO | La compañía no cuenta con datos criptográficos |
| A.18.2 | **Revisiones de seguridad de la información** | | | |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.18.2.1 | Revisión independiente de la seguridad de la información | El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | SI | Para poder actualizar toda la operación de la compañía en los procedimientos o políticas. |
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad | Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas , y cualquier otro requisito de seguridad. | SI | Cada líder de área debe tener un procedimiento asignado y relacionado con las políticas de seguridad para futuras verificaciones. |

| No del Control | Objetivo de control | Control | SI/NO | Declaración de Aplicabilidad |
|---|---|---|---|---|
| A.18.2.3 | Revisión del cumplimiento técnico | Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. | SI | Para la protección de la información dando seguimiento a los protocolos establecidos. |