UNIVERSIDAD NACIONAL PEDRO RUÍZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

PARA OPTAR EL TÍTULO DE INGENIERO EN COMPUTACIÓN E INFORMÁTICA

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA AGROINDUSTRIAL POMALCA S.A.A. - 2016"

AUTORES:

Br. VILLEGAS RIVERA CÉSAR AUGUSTO

Br. ZAMORA LI GERMÁN SUISHING DE JESÚS

ASESORA:

Ing. AQUINO LALUPÚ JANET DEL ROSARIO

LAMBAYEQUE – PERÚ

2018

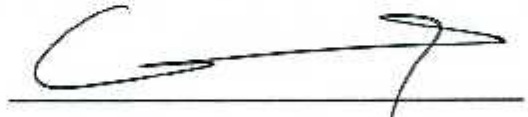
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA AGROINDUSTRIAL POMALCA S.A.A. – 2016

Tesis presentada a la Universidad Nacional Pedro Ruiz Gallo, para obtener el Título de: INGENIERO EN COMPUTACIÓN E INFORMÁTICA.

APROBADA POR HONORABLE JURADO:

Ing. Nilton César Germán Reyes
PRESIDENTE



M.Sc. Segundo Pedro Fiestas Rodríguez
SECRETARIO

M.Sc. Consuelo Ivonne Del Castillo Castro
VOCAL

LAMBAYEQUE – PERÚ – 2018

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA AGROINDUSTRIAL POMALCA S.A.A. – 2016

Tesis presentada a la Universidad Nacional Pedro Ruiz Gallo, para obtener el Título de: INGENIERO EN COMPUTACIÓN E INFORMÁTICA.

Bach. Villegas Rivera César Augusto
AUTOR

Bach. Zamora Li Germán Suishing de Jesús
AUTOR

Ing. Janet del Rosario Aquino Lalupú
ASESORA:

LAMBAYEQUE – PERÚ – 2018

AGRADECIMIENTO

Queremos dar nuestros agradecimientos generales con todos los involucrados en la realización de este trabajo de tesis, luego damos agradecimientos individuales de lo que nos nace de lo profundo de nuestros corazones.

A DIOS TODOPODEROSO que nos ha dado la vida y nos hace crecer en su amor cada día, que nos concedió la inteligencia y nos condujo a lo largo de la realización de nuestro proyecto, protegiéndonos, consolándonos y concediéndonos el ánimo y la fuerza para seguir adelante.

A Nuestra Familias, que han sido nuestro soporte emocional, físico y económico, dándonos todo lo necesario para culminar con éxito nuestra formación profesional y el Trabajo de Tesis.

A nuestra asesora la Ing. Janet Aquino Lalupú, que nos orientó en una forma muy profesional, nos brindó la confianza para avanzar en el trabajo y por creer en nosotros.

A nuestros jurados, quien con sus conocimientos, su experiencia y su motivación han logrado que concluyamos nuestra tesis y a la vez haber aportado en la formación de nuestra persona como investigador.

A la Empresa Agroindustrial Pomalca S.A.A., por concedernos la oportunidad de efectuar la tesis en su Institución, y por su colaboración tan generosa con nosotros.

A nuestros docentes de la Escuela Profesional de Ingeniería en Computación e Informática, por habernos brindado los conocimientos necesarios para lograr en un futuro ser unos profesionales con éxito.

A todos ellos les estamos infinitamente agradecidos, y esperamos que Dios les recompense todo el bien que han hecho por nosotros.

DEDICATORIA

Esta tesis se la dedico a mi Dios Todopoderoso quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi familia quienes por ellos soy lo que soy. Para mis padres por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, y mi coraje para seguir con mis objetivos.

CÉSAR

A mis Padres, por su Amor, Trabajo y Sacrificios en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy.

GERMÁN SUISHING

Los Autores

PRESENTACION

Señores miembros del jurado.

Se pone a vuestra disposición la tesis titulada: “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA AGROINDUSTRIAL POMALCA S.A.A. - 2016” para optar el grado de Ingeniero en Computación e Informática.

El trabajo de investigación y consta de 9 capítulos, los cuales van detallando el desarrollo del problema y dando los alcances necesarios. Los capítulos son Datos Generales de la Organización, Problemática de la investigación, Marco Metodológico, Marco Teórico, Desarrollo de la propuesta, Costos y Beneficios, Conclusiones, Recomendaciones y Referencias Bibliográficas.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles en el mercado, que conllevan a la aparición de nuevas amenazas y riesgos para los sistemas de información, que pueden poner en juego la estabilidad y el futuro de las organizaciones.

La realización de esta tesis se hizo con el fin de proponer controles para minimizar los riesgos significativos y de alto impacto para el negocio, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial y en general para la continuidad de las operaciones y la reputación de la Empresa Agroindustrial Pomalca S.A.A.

Los autores.

RESÚMEN

Los Sistemas de Gestión de Seguridad de la Información consisten en una serie de procesos cuyo objetivo es proteger los activos y mantener los principios de Confidencialidad, Integridad y Disponibilidad de ellos a través de un ciclo de mejoramiento continuo, donde la fase de diseño o planeación comprende en establecer políticas, objetivos, procesos y procedimientos relevantes a la gestión de los riesgos informáticos.

Para el caso del presente proyecto de tesis, se realizará un enfoque en la seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A., donde aplica la necesidad de proteger la información de gran importancia para la empresa, la cual debe estar resguardada correctamente para evitar que dicha información se pierda o caiga en manos indebidas y así garantizar la continuidad de la empresa y el logro los objetivos del negocio.

El presente trabajo de investigación se decidió realizar basándose en el ciclo de mejora continua (Ciclo PDCA) aplicando la Metodología MAGERIT, apoyándose en el análisis y vulnerabilidades existentes en los activos involucrados en el mantenimiento y proceso de la información, por su facilidad de comprensión, costo económico y poca duración en la aplicación del diseño.

Este proyecto permitió conocer los beneficios de un SGSI en la Empresa Agroindustrial Pomalca S.A.A. mediante la aplicación de la norma ISO/IEC 27001:2013. Esto a su vez, permitió elaborar las Políticas de Seguridad de la Información generales.

Palabras Claves: *Seguridad, Información, ISO/IEC 27001:2013, Sistemas de Gestión de la Seguridad de la Información, SGSI.*

ABSTRAC

Systems Management Information Security consist of a series of processes designed to protect assets and maintain the principles of confidentiality, integrity and availability of them through a cycle of continuous improvement, where the design phase or planning comprises establish policies, objectives, and processes relevant to IT risk management procedures.

In the case of this thesis project, a focus on information security of the Agroindustrial Pomalca S.A.A., which applies the need to protect information of great importance for the company, which must be protected properly to avoid be held that this information is lost or fall into the wrong hands and thus ensure the continuity of the company and achieving business goals.

This research was decided to perform based on the continuous improvement cycle (Cycle PDCA) using the MAGERIT methodology, based on the analysis and vulnerabilities on assets involved in the maintenance and processing of information, ease of understanding, economic cost and short duration in application design.

This project allowed us to know the benefits of an ISMS in Agroindustrial Pomalca S.A.A. by applying the ISO / IEC 27001: 2013. This in turn led to the development Policies Security General Information.

Key Word: *Security, Information, ISO/IEC 27001:2013, Systems Management, Information Security, ISMS.*

INDICE GENERAL

Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRÁFICOS

INDICE DE ANEXOS

INTRODUCCIÓN

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles en el mercado. La posibilidad de interconectarse a través de las redes ha traído consigo el mejoramiento de la productividad en las organizaciones, además de la aparición de nuevas amenazas y riesgos para los sistemas de información, que pueden poner en juego la estabilidad y el futuro de las organizaciones.

Ahora, también es un hecho cierto que así como existen especialistas en el mundo de la tecnología, dedicados a desarrollar, por el bien de la comunidad nuevos software que ayudan a mejorar y facilitar la vida de los seres humanos, ya sea en el área de negocios como en el área personal, también existen los llamados “hackers” o piratas cibernéticos, casi siempre jóvenes con avanzados conocimientos de informática que utilizan su inteligencia para robar información de grandes empresas, gobierno y hasta organizaciones sin o con fines de lucro.

Por lo expuesto anteriormente, la presente tesis tuvo como objetivo diseñar un sistema de gestión de seguridad de información para la Empresa Agroindustrial Pomalca S.A.A. basado en el estándar internacional ISO/IEC 27001:2013 para aumentar la seguridad de la información.

La realización de esta tesis se hizo con el fin de proponer controles para minimizar los riesgos significativos y de alto impacto para el negocio, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial y en general para la continuidad de las operaciones y la reputación de la Empresa Agroindustrial Pomalca S.A.A.

CAPÍTULO I:
DATOS GENERALES DE LA ORGANIZACIÓN

1.1. Descripción de la organización

La empresa se dedica a producir azúcar a partir del cultivo de caña de azúcar, así como sus derivados (melaza, chancaca y bagazo), al cultivo de remolacha azucarera en fase de experimentación, y a la agro exportación en menor escala con cultivos de pimientos dulces y picantes como páprika, guajillo, jalapeños habaneros y eventualmente alcachofas, basados en normas ambientales y responsabilidad social; estando a la vanguardia en la aplicación de tecnologías de última generación.

Unido a los cambios sustanciales en fabricación, es la responsabilidad social un puntual fundamental que no está ausente. Todo ello es reflejo de un trabajo ordenado y serio que transformó a la agroindustrial en una empresa viable, competitiva y rentable. Son diversos los proyectos que se han implementado en la comunidad regional, como salud, educación, medio ambiente, respeto laboral, capacitación del recurso humano, cumplimiento tributario tanto al Estado como a las Instituciones públicas tal cual como la ley gubernamental confiere efectuar.

La empresa azucarera continúa esforzándose para cumplir los más altos estándares de organización industrial, calidad productiva y ética laboral, cumplimiento que lo posiciona acorde a las exigencias de la mercadotecnia internacional.

1.2. Misión, Visión y Objetivos de la organización

1.2.1. Misión

Administrar de manera dinámica, responsable, eficiente e íntegra cada uno de los procesos de obtención agroindustrial establecidos en la E.A.I Pomalca S.A.A., lo cual se logra proporcionando una sólida red tecnológica e informática, una alta capacitación profesional y una continua orientación técnica

competitiva para que Pomalca posicione permanentemente a sus actores como líderes agroindustriales.

1.2.2. Visión

Desde Lambayeque, ser la mejor empresa agroindustrial del país y en el mercado internacional.

1.2.3. Objetivos

Como empresa atenta a la sociedad y a sus problemas, la E.A.I Pomalca S.A.A. orienta sus actividades prioritariamente a los cumplimientos de los siguientes objetivos:

- Ofrecer un servicio de calidad al país produciendo un producto de alto valor comercial.
- Convocar profesionales competentes comprometidos con la empresa.
- Promover la investigación agrícola y la creación de nuevos proyectos.
- Impulsar la proyección social hacia la mejora continua de la comunidad.
- Contribuir desde el quehacer propio de la Empresa, a un progreso sostenible, inclusivo y humano, afín a los valores que nos inspiran.

1.3. Estructura Orgánica

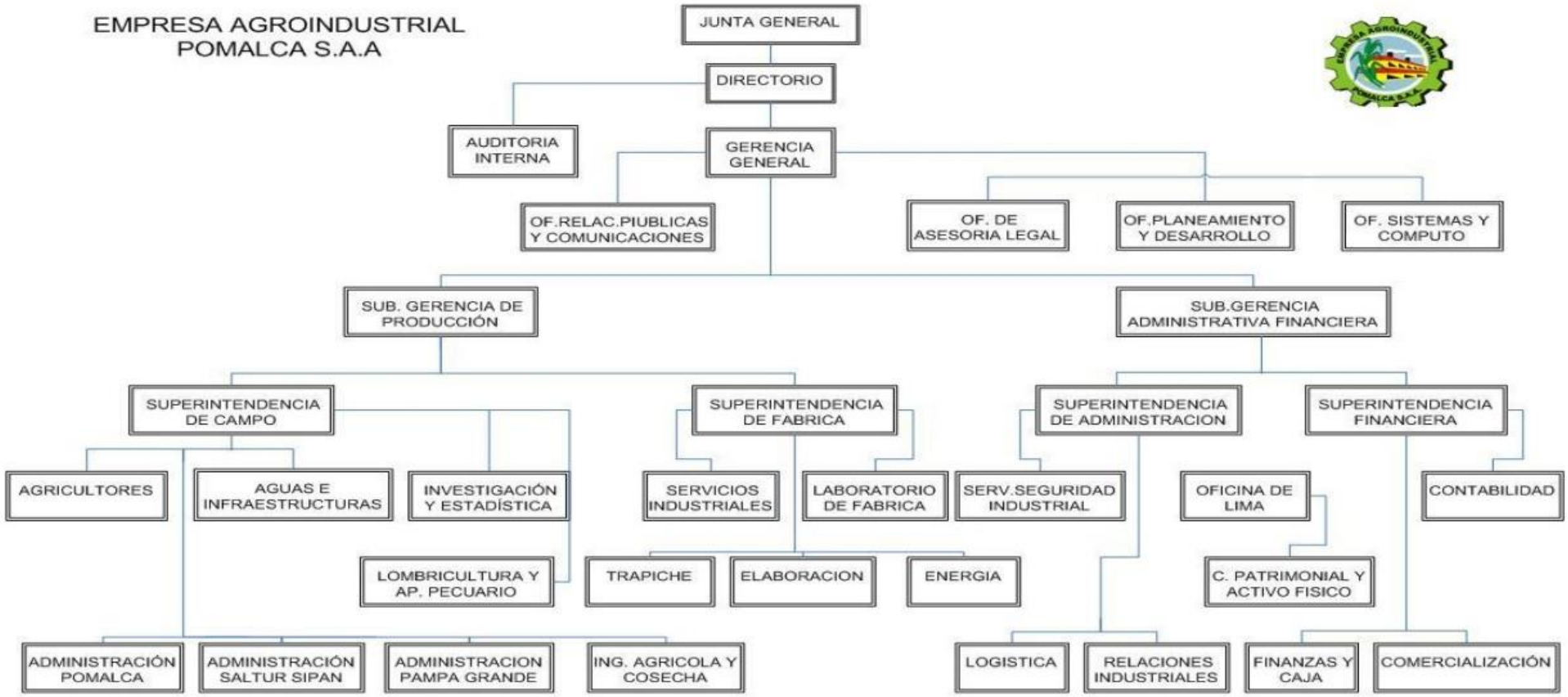


Figura N° 1: Estructura orgánica de la Empresa Agroindustrial Pomalca S.A.A.

Fuente: Empresa Agroindustrial Pomalca S.A.A.

CAPÍTULO II:
PROBLEMÁTICA DE LA INVESTIGACIÓN

2.1. Realidad Problemática

2.1.1. Planteamiento del Problema

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles en el mercado. La posibilidad de interconectarse a través de las redes ha traído consigo el mejoramiento de la productividad en las organizaciones, además de la aparición de nuevas amenazas y riesgos para los sistemas de información, que pueden poner en juego la estabilidad y el futuro de las organizaciones. En el contexto de la norma ISO 27001, un activo de información será: "…algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger". Siendo la información uno de los activos que requiere ser protegida de forma adecuada frente a cualquier amenaza que ponga en peligro la continuidad del negocio. (Altagracia López, 2011)

En la Figura N° 2 se puede apreciar como los activos de información de una organización están rodeados de un ambiente complejo lleno de amenazas que pueden ir desde simples virus de computadora hasta robo de la propiedad intelectual de la empresa.

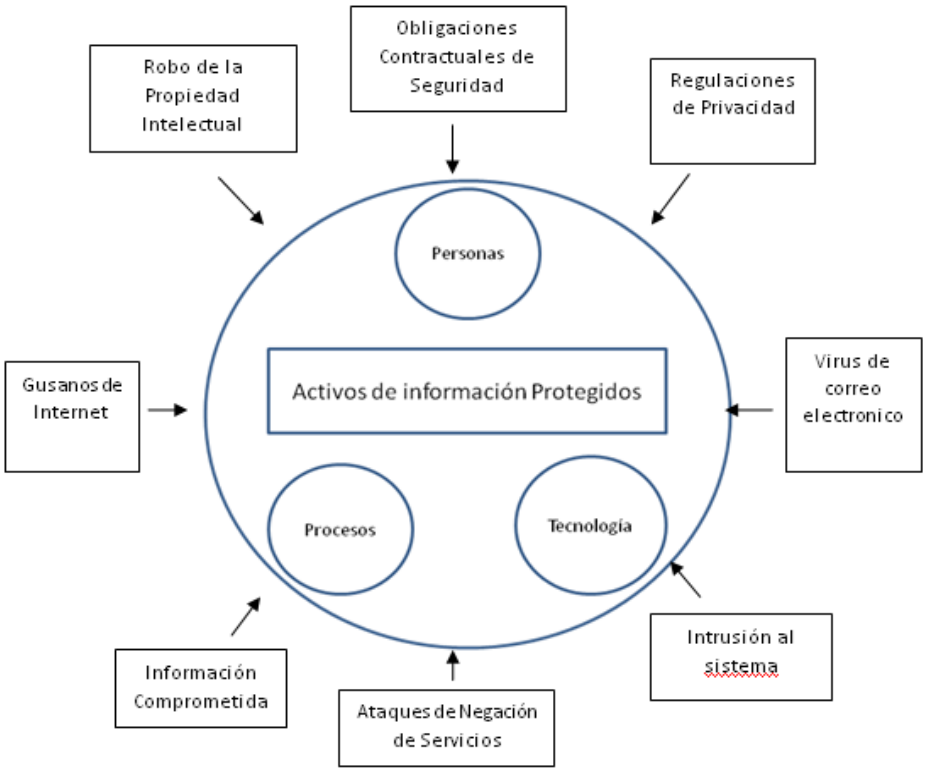


Figura N° 2: Activos de Información y sus amenazas

Fuente: (Espinoza Aguinaga, 2013)

Ahora, también es un hecho cierto que así como existen especialistas en el mundo de la tecnología, dedicados a desarrollar, por el bien de la comunidad nuevos software que ayudan a mejorar y facilitar la vida de los seres humanos, ya sea en el área de negocios como en el área personal, también existen los llamados “hackers” o piratas cibernéticos, casi siempre jóvenes con avanzados conocimientos de informática que utilizan su inteligencia para robar información de grandes empresas, gobierno y hasta organizaciones sin o con fines de lucro.

Las compañías deben mejorar sus sistemas y capacitar a su equipo para encontrar y resolver el problema, que no es nada barato. Después del robo, las compañías deben informar a sus clientes que la información está en riesgo, y deben gastar incluso

más para prevenir que vuelva a ocurrir. (Espinoza Aguinaga, 2013)

Para el caso del presente proyecto de tesis, se realizará un enfoque en la seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A., donde aplica la necesidad de proteger la información de gran importancia para la empresa, la cual debe estar resguardada correctamente para evitar que dicha información se pierda o caiga en manos indebidas y así garantizar la continuidad de la empresa y el logro los objetivos del negocio.

Además este sistema de gestión de seguridad de información que se diseñará, no solo será útil para el tipo de empresa de producción, sino también será útil para todos los tipos de empresas de producción que tengan información relevante. Algunos tipos de empresa son por ejemplo una empresa productora de espárragos, una empresa productora de ají paprika, una empresa productora de duraznos enlatados, etc. que precisamente tienen como información relevante datos de sus distintos tipos de productos (espárragos, ají paprika, duraznos enlatados), sus planes de producción, etc.

Para garantizar la seguridad de esta información, las empresas deben dejar de actuar reactivamente en respuesta a los incidentes y problemas relacionados con la seguridad de información y empezar a realizar un conjunto de acciones como identificar el activo y definir su impacto, luego evaluar cuáles de estos activos puede correr riesgos y por último la alta gerencia deben decidir qué acciones se tomarán para mitigar los riesgos.

Esta importancia de la información crea una necesidad de control y gestión de la seguridad sobre la misma y no solo desde un punto de vista legal en cuanto a datos personales se refiere, sino con carácter general a toda la información manejada por una compañía, convirtiéndose en un complemento importante y que

aporta un plus de confianza y compromiso ante clientes o terceros ajenos a la empresa. Como ejemplo de este punto es la cada vez más aceptada e incluso exigida aplicación de normas ISO en la contratación entre empresas a nivel internacional. Este sistema de gestión es de mucha importancia para que una organización pueda sobrevivir al mercado actual.

Para gestionar la seguridad de la información, las organizaciones pueden seguir algunas de las normas o modelos existentes en el mercado, tales como ISO/IEC 27001 e ISO/IEC 27002, RISK IT, COBIT, etc., que establecen determinadas reglas y estándares que sirven de guía para esta gestión.

2.2. Formulación del Problema

¿El diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 lograría aumentar la seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A.?

2.3. Justificación e Importancia de la Investigación

La importancia de la Seguridad de la Información se viene tratando desde hace algunos años en las organizaciones, las cuales hacen grandes inversiones en sistemas y dispositivos de seguridad como: firewalls, antivirus, sistemas de respaldo entre otros; sin embargo, esto no es suficiente para considerar que un sistema es seguro en relación a la integridad, la disponibilidad y la confidencialidad de la información que se maneja. De allí que los mecanismos de seguridad necesitan de un Plan de Gestión de la Seguridad que integre a las políticas generales de la empresa, considerando a la organización como un todo.

Un Plan de Gestión de Seguridad de la Información permite maximizar los esfuerzos desarrollados para asegurar la organización

en todos sus niveles, apoya el cumplimiento del marco legal, aporta una metodología para el análisis y gestión del riesgo y garantiza la implantación de medidas de seguridad consistente, eficiente y apropiada al valor de la información protegida.

Es así como la Empresa Agroindustrial Pomalca S.A.A. se beneficiaría con el diseño de un Sistema de Gestión de Seguridad de la Información, porque éste permitirá establecer políticas, procedimientos, objetivos y procesos claros para que permitan determinar y proponer controles de seguridad que ayuden a tratar los riesgos en la Seguridad de la Información comprendiendo espacios físicos, procesos automáticos y manuales, gestión del personal, usuarios de los sistemas y equipos para optimizar la gestión de los incidentes que se detecten y generar resultados en concordancia con las políticas y objetivos generales de la Empresa Agroindustrial Pomalca S.A.A.

2.4. Objetivos de la Investigación

2.4.1. Objetivo General

Diseñar un sistema de gestión de seguridad de información para la Empresa Agroindustrial Pomalca S.A.A. basado en el estándar internacional ISO/IEC 27001:2013 para aumentar la seguridad de la información.

2.4.2. Objetivos Específicos

- Diagnosticar la situación actual de la Empresa Agroindustrial Pomalca S.A.A. en relación a la seguridad de la información.

- Utilizar la metodología MAGERIT para identificar los activos de información más críticos y determinar el nivel de riesgo potencial, dentro de la organización.

- Proponer controles para minimizar los riesgos significativos y de alto impacto para el negocio, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial, la alteración o modificación de la misma, y en general la continuidad de las operaciones y la reputación de la Empresa Agroindustrial Pomalca S.A.A.

2.5. Limitaciones de la Investigación

Esta investigación busca proponer el diseño de un Sistema de Gestión de Seguridad de la Información en la Empresa Agroindustrial Pomalca S.A.A., de acuerdo al estándar internacional ISO/IEC 27001:2013, evaluando así las amenazas, riesgos e impactos, precedida por un diagnóstico de la situación actual de la seguridad de la información, que permita un análisis comparativo de los controles a ser implantados o requeridos en la empresa, respecto a los controles planteados en la norma.

Debido a que la norma suma 114 controles entre todas las secciones, se propone limitar este estudio de acuerdo necesidades propias de la empresa a algunos dominios de control.

La limitación de la investigación es pertinente, puesto que están relacionados intrínsecamente con los tres principios básicos de la seguridad como lo son: la confidencialidad, integridad y disponibilidad, además de abordar las tres áreas críticas de cualquier organización como son los activos, seguridad física y ambiental, y el control de acceso.

CAPÍTULO III:
MARCO METODOLÓGICO

3.1. Tipo de Investigación

Investigación Descriptiva – Simple, ya que en el presente estudio analizaremos el problema de seguridad de información con el que ya cuenta la Empresa Agroindustrial Pomalca S.A.A., y se planteará una solución al respecto, basándose en el estándar internacional ISO/IEC 27001:2013.

3.2. Hipótesis

El diseño del sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2013 permitirá optimizar la seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A.

3.3. Variables

3.3.1. Variable Independiente

Sistema de seguridad de información basado en la norma ISO/IEC 27001:2013.

3.3.2. Variable Dependiente

Seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A.

VARIABLE		DEFINICIÓN	DIMENSIONES
VARIABLE INDEPENDIENTE	**Sistema de seguridad de información basado en la norma ISO/IEC 27001:2013**	Desarrollado para el establecimiento, implementación, monitorización, revisión, mantenimiento, supervisión y mejora de un sistema de control de seguridad de la información.	Tiempo
			Cumplimiento de la norma
VARIABLE DEPENDIENTE	**Seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A.**	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.	Gestión de incidentes en la seguridad de la información
			Control de acceso
			Seguridad física y ambiental
			Gestión de activos

Tabla N° 1. Operacionalización de variables
Fuente: Elaboración propia.

CAPÍTULO IV:
MARCO TEÓRICO

4.1. Antecedentes de la Investigación

4.1.1. Antecedentes en el contexto internacional

- **Título:** “Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001 - 27002”.

  Autores:

  - ✓ José Luis Buenaño Quintana.
  - ✓ Marcelo Alfonso Granda Luces.

  Año: 2009

  Tesis para optar al título de Ingeniero Informático.
  Ecuador – Guayaquil: Universidad del Politécnica Salesiana.

  RESUMEN

  Durante el constante proceso de evolución del uso de la tecnología como soporte a las operaciones en las organizaciones, siempre ha existido la preocupación por evitar incidentes que comprometen la seguridad de la información.

  Es por eso que la seguridad de la información consiste en combinar de manera coherente las herramientas técnicas de seguridad y a la vez gestionar el comportamiento del factor humano tratando de reducir en la mayor medida posible las vulnerabilidades o posibles atentados contra la seguridad de la información y sistemas.

- **Título:**“Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial la Ofrenda”.

Autores:

- ✓ Juan David Aguirre Cardona.
- ✓ Catalina Aristizabal Betancourt.

Año: 2013

Tesis para optar al título de Ingeniero de Sistemas.
Colombia: Universidad Tecnológica de Pereira.

RESUMEN

El número de atacantes de las redes y de los sistemas en las organizaciones es cada vez mayor, frente a esta situación, un 46% de usuarios afirmó haber recibido un mensaje fraudulento que afirmaba provenir de servicios de correo electrónico como Yahoo, Microsoft y Gmail. Le siguen las redes sociales con un 45%, los bancos 44% y tiendas en línea 37%.

Un Sistema de gestión de seguridad de la información (SGSI), es la parte de un sistema de gestión global basado directamente en los riesgos para el negocio y los activos del mismo contemplado en la norma ISO 27001, ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información evitando las inversiones mal dirigidas, contrarrestando las amenazas presentes en el entorno y dentro de la misma, implementación de controles proporcionado y de un coste menos elevado.

4.1.2. Antecedentes en el contexto nacional

- **Título:** “Diseño e implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos”.

  Autores:

  - ✓ Carlos Eduardo Barrantes Porras.
  - ✓ Javier Roberto Hugo Herrera.

  Año: 2012

  Tesis para optar al Título de Ingeniero de Sistemas.
  Lima – Perú: Universidad de San Martin de Porres.

  RESUMEN

  En la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos.

  El propósito de este trabajo se centró en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001:2005 e ISO 17799:2005.

  Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú S.A, que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y

minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

- **Título:** “Análisis y Diseño de un Sistema de Gestión de Seguridad de Información basado en la Norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo”.

Autor:

- ✓ Hans Iyán Espinoza Aguinaga.

Año: 2013.

Tesis para Optar el título de Ingeniero Informático.
Lima – Perú: Pontificia Universidad Católica del Perú.

RESUMEN

En el presente proyecto de fin de carrera se tomaran en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información para que pueda ser empleado por una empresa dedicada a la producción de alimentos de consumo masivo en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo que respecta a seguridad de información.

Para efectos del análisis de riesgos para este proyecto de tesis, se decidió trabajar con el proceso de producción, ya que se consideró que era el proceso más importante dentro del funcionamiento de la empresa. Este proceso de

producción a su vez se dividió en 4 subprocesos que lo conforman, los cuales fueron el proceso de planificación, manufactura, calidad y bodegas e inventarios.

- **Título:** “Diseño de un Sistema de Gestión de Seguridad de Información para una central privada de información de riesgos”.

Autor:

- ✓ Josefina Ríos Villafuente.

Año: 2014.

Tesis para optar el título de ingeniero informático.
Lima – Perú: Pontificia Universidad Católica del Perú.

RESUMEN

Una Central de Riesgo privada está encargada principalmente de brindar información a terceros sobre el nivel de endeudamiento, antecedentes crediticios, comerciales, tributarios, laborales y de seguros de personas naturales y jurídicas, mediante la recolección y procesamiento de información de riesgo con el objeto de evaluar la capacidad de endeudamiento y pago de dichas personas.

Un Sistema de Gestión de Seguridad de la Información permite la calidad de la seguridad de la información, gestionando el acceso a la información, brindando confidencialidad, disponibilidad e integridad a la información evitando ataques, filtración, alteración y pérdida de ingresos, cumpliendo con las normas legales.

En este contexto se presenta como propuesta el Diseño de un Sistema de Gestión de Seguridad de Información (SGSI) que permita a una central de riesgos cumplir con la regulación vigente siguiendo normas internacionales actuales

4.1.3. Antecedentes en el contexto local

- **Título:** "Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, para Apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la Ciudad de Chiclayo".

  Autor:

  - ✓ Julio César Alcántara Flores.

  Año: 2015.

  Tesis para optar el título de ingeniero de Sistemas y Computación.
  Chiclayo – Perú: Universidad Católica Santo Toribio de Mogrovejo.

  RESUMEN

  Con la Guía de Implementación, se logró incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, y esto se vio reflejado en el incremento de políticas de seguridad que fueron puestas en marcha que beneficiaron a la institución y ayudaron a incrementar el nivel de seguridad en la misma.

  El uso de la Guía de Implementación, se logró mejorar el proceso para detectar las anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad

para salvaguardarla y prevenir su mal uso y divulgación no adecuada que perjudiquen a la institución.

- **Título:** “Elaboración Y Aplicación De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Para La Realidad Tecnológica De La Usat”.

Autores:

- ✓ César Wenceslao De la Cruz Guerrero
- ✓ Juan Carlos Vásquez Montenegro

Año: 2008.

Tesis para optar el título de ingeniero de Sistemas y Computación.
Chiclayo – Perú: Universidad Católica Santo Toribio de Mogrovejo.

RESUMEN

En la actualidad las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Es por esto que enfocando nuestro proyecto en la realidad peruana se vio por conveniente traer a la memoria algunas empresas del medio que cuentan con un Sistema de Gestión de la Seguridad de la Información como Telefónica

Empresas y Nextel S.A; dichas empresas refieren que los problemas de la Seguridad de la Información rara vez se centran en aspectos de carácter técnico exclusivamente, sino de gestión cómo alinear la tecnología con los objetivos de la organización.

4.2. Base Teórica

La presente sección tiene como finalidad reseñar los aspectos teóricos relacionados con el diseño de un Sistema de Gestión de Seguridad de la Información para la Empresa Agroindustrial Pomalca S.A.A.

4.2.1. Información

Según (Vittoriano, 2008) la información es considerada como: “Insumo fundamental que actúa como facilitador para los objetivos de la organización, con base en ella se desarrolla su negocio y es un elemento vital para el desarrollo modelo de negocio de la organización”. En el contexto de la norma ISO 27001, un activo de información será: “…algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger”.

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para sus actividades diarias, operaciones de su trabajo, para cumplir con sus funciones, el cual puede equivocarse o no, o hacer el bien o el mal. La información tiene estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

4.2.2. Sistemas de Información

(Soto, 2007) Define Sistema de Información como: El sistema de personas, registros de datos y actividades que procesa los datos y la información en cierta organización, incluyendo manuales de procesos o procesos automatizados.

Todos estos elementos interactúan para procesar los datos y dan lugar a información más elaborada, que se distribuye de la manera más adecuada posible en una determinada organización.

Estas actividades de recolección y procesamiento de información, eran actividades manuales y solo con la llegada de la tecnología, (computadoras, Internet, etc., se han convertido en sistemas con recursos informáticos y de comunicación).

El objetivo primordial de un sistema de información es apoyar la toma de decisiones y controlar todo lo que en ella ocurre.

Habitualmente el término "sistema de información" se usa de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente hablando, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la práctica esto no suela ocurrir). Se podría decir entonces que los sistemas de información informáticos son una subclase o un subconjunto de los sistemas de información en general.

ACTIVIDADES

Existen cuatro actividades en un sistema de información que producen la información que esas organizaciones necesitan para tomar decisiones, controlar operaciones, analizar problemas y crear nuevos productos o servicios.

Estas actividades son:

- **Recopilación:** captura o recolecta datos en bruto tanto del interior de la organización como de su entorno externo.
- **Almacenamiento:** guardar de forma estructurada la información recopilada.
- **Procesamiento:** convierte esa entrada de datos en una forma más significativa.
- **Distribución:** transfiere la información procesada a las personas o roles que la usarán.

TIPOS DE SISTEMAS DE INFORMACIÓN

Los sistemas de información pueden clasificarse de diversas formas:

- **Sistemas de procesamiento de transacciones**

  Los sistemas de procesamiento de transacciones (TPS por sus siglas en inglés) son los sistemas empresariales básicos que sirven al nivel operacional de la organización.

  Un sistema de procesamiento de transacciones es un sistema computarizado que realiza y registra las transacciones rutinarias diarias necesarias para el funcionamiento de la empresa. Se encuentran en el nivel más bajo de la jerarquía organizacional y soportan las actividades cotidianas del negocio.

- **Sistemas de control de procesos de negocio**

  Los sistemas de control de procesos de negocio (BPM por sus siglas en inglés) monitorizan y controlan los procesos industriales o físicos, como puede ser la refinación de petróleo, generación de energía o los sistemas de producción de acero en una planta siderúrgica.

  Por ejemplo, en una refinería de petróleo se utilizan sensores electrónicos conectados a ordenadores para monitorizar procesos químicos continuamente y hacer ajustes en tiempo real que controlan el proceso de refinación. Un sistema de control de procesos comprende toda una gama de equipos, programas de ordenador y procedimientos de operación.

- **Sistemas de colaboración empresarial**

  Los sistemas de colaboración empresarial (ERP por sus siglas en inglés) son uno de los tipos de sistemas de información más utilizados. Ayudan a los directivos de una empresa a controlar el flujo de información en sus organizaciones.

  Se trata de uno de los tipos de sistemas de información que no son específicos de un nivel concreto en la organización, sino que proporcionan un soporte importante para una amplia gama de usuarios. Estos sistemas de información están diseñados para soportar tareas de oficina como sistemas multimedia, correos electrónicos, videoconferencias y transferencias de archivos.

- **Sistemas de Información de Gestión**

  Los sistemas de información de gestión (MIS por sus siglas en inglés) son un tipo de sistemas de información que

recopilan y procesan información de diferentes fuentes para ayudar en la toma de decisiones en lo referente a la gestión de la organización.

Los sistemas de información de gestión proporcionan información en forma de informes y estadísticas. El siguiente nivel en la jerarquía organizacional está ocupado por gerentes y supervisores de bajo nivel. Este nivel contiene los sistemas informáticos que están destinados a ayudar a la gestión operativa en la supervisión y control de las actividades de procesamiento de transacciones que se producen a nivel administrativo.

Los sistemas de información de gestión utilizan los datos recogidos por el TPS para proporcionar a los supervisores los informes de control necesarios. Los sistemas de información de gestión son los tipos de sistemas de información que toman los datos internos del sistema y los resumen en formatos útiles como informes de gestión para utilizarlos como apoyo a las actividades de gestión y la toma de decisiones.

- **Sistemas de apoyo a la toma de decisiones**

  Un sistema de apoyo a la toma de decisiones o de soporte a la decisión (DSS por sus siglas en inglés) es un sistema basado en ordenadores destinado a ser utilizado por un gerente particular o por un grupo de gerentes a cualquier nivel organizacional para tomar una decisión en el proceso de resolver una problemática semi estructurada. Los sistemas de apoyo a la toma de decisiones son un tipo de sistema computarizado de información organizacional que ayuda al gerente en la toma de decisiones cuando necesita modelar, formular, calcular, comparar, seleccionar la mejor opción o predecir los escenarios.

Los sistemas de apoyo a la toma de decisiones están específicamente diseñados para ayudar al equipo directivo a tomar decisiones en situaciones en las que existe incertidumbre sobre los posibles resultados o consecuencias. Ayuda a los gerentes a tomar decisiones complejas.

- **Sistemas de Información Ejecutiva**

  Los sistemas de información ejecutiva (EIS por sus siglas en inglés) proporcionan un acceso rápido a la información interna y externa, presentada a menudo en formato gráfico, pero con la capacidad de presentar datos básicos más detallados si es necesario. Los sistemas información ejecutiva proporcionan información crítica de una amplia variedad de fuentes internas y externas en formatos fáciles de usar para ejecutivos y gerentes.

  Un sistema de información ejecutiva proporciona a los altos directivos un sistema para ayudar a tomar decisiones estratégicas. Está diseñado para generar información que sea lo suficientemente abstracta como para presentar toda la operación de la empresa en una versión simplificada para satisfacer a la alta dirección.

4.2.3. Seguridad de la Información

La Organización Internacional para la Estandarización (ISO) define Seguridad de la Información (SI) como:

La preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización.

Además, también pueden estar involucradas otras propiedades como son: la autenticidad, la responsabilidad, el no-repudio y la confiabilidad.

Es decir, estos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación:

Confidencialidad.- La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad.- Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Para garantizar la integridad de la información el remitente debe estar siempre autenticado. Esta se puede ver afectada por problemas de hardware, software, virus o personas malintencionadas.

Disponibilidad.- Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

A veces confundimos este tipo de seguridad con la seguridad informática, pero hay que tener en cuenta que esta última solo se centra en salvaguardar los datos dentro de un sistema informático, mientras que la información en general puede darse en otros muchos contextos entre los usuarios.

¿SEGURIDAD INFORMÁTICA O SEGURIDAD DE LA INFORMACIÓN? ACLARANDO LA DIFERENCIA

Según el portal de (Security, 2015), en la actualidad, un término ampliamente utilizado es “seguridad informática”, que puede asociarse con otras palabras como amenazas informáticas, criminales informáticos u otros conceptos. Aunque se tiene una percepción general sobre lo que representa, en ocasiones puede utilizarse como sinónimo de seguridad de la información.

La disyuntiva se presenta cuando es necesario aplicar de manera adecuada los conceptos, de acuerdo con las ideas que se pretenden expresar. Si bien existen distintas definiciones para la seguridad informática, es importante conocer cuándo se utiliza de forma correcta de acuerdo con el contexto, e identificar sus diferencias con los otros términos -por ejemplo, el de seguridad de la información.

La seguridad informática busca proteger la información digital en los sistemas interconectados. Está comprendida dentro de la seguridad de la información

En la pasada edición de bSecure Conference, profesionales de seguridad de ISACA (Information Systems Audit and Control Association) capítulo Monterrey, comenzaron su participación a partir de definir qué es la seguridad informática. De acuerdo con la asociación, puede entenderse como:

“Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

La norma ISO 27001 define activo de información como los conocimientos o datos que tienen valor para una organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.

Por lo tanto, la seguridad informática tiene como foco la protección de la información digital que “vive” en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

PRINCIPALES DIFERENCIAS ENTRE SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

Es posible identificar las principales diferencias y por lo tanto conocer cuándo aplicar un concepto u otro. En primer lugar, resaltamos que la seguridad de la información tiene un alcance mayor que la seguridad informática, puesto que la primera busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados.

Por el contrario, la seguridad informática se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.

Además, la seguridad de la información se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información; también involucra la aplicación y gestión de medidas de seguridad apropiadas, a través de un enfoque holístico.

Por lo tanto, sin importar los límites de cada concepto, el objetivo principal es proteger la información, independientemente de que ésta pertenezca a una organización o si se trata de información personal, ya que nadie está exento de padecer algún riesgo de seguridad.

4.2.4. Sistema de gestión de la seguridad de la información

El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS (siglas equivalentes en ingles a Information Security Management System).

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Ayuda a establecer la política de seguridad y los procedimientos en relación a los objetivos de negocio de la empresa, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Utilización:

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa.

La confidencialidad, integridad y disponibilidad de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurase de que haya beneficios económicos.

Las empresas y los sistemas de información se encuentran expuestos a un número cada vez más elevado de amenazas que aprovechan cualquier tipo de vulnerabilidad para someter a los activos críticos de información a ataques, espionajes, vandalismo, etc. Los virus informáticos o los ataques son ejemplos muy comunes y conocidos, pero también se deben asumir los riesgos de sufrir incidentes de seguridad que pueden ser causados voluntariamente o involuntariamente desde dentro de la propia

empresa o los que son provocados de forma accidental por catástrofes naturales.

El cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtiene el máximo beneficio son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

El nivel de seguridad que se alcanza gracias a los medios técnicos es limitado e insuficiente por sí mismo. Durante la gestión efectiva de la seguridad debe tomar parte activa toda la empresa, con la gerencia al frente, tomando en consideración a los clientes y a los proveedores de la organización.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos.

Beneficios de implantar un SGSI

Según (KWELL - Empresa líder de servicios de seguridad y gestión de riesgos tecnologógicos, 2008) los beneficios de implantar un sistema de gestión de Seguridad de la Información son:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.

- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costos y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

¿Por qué adoptar un estándar de seguridad de la información?

Existen varias razones por las que las organizaciones eligen tener un sistema de gestión de seguridad de la información (SGSI). Estas generalidades se ajustan a dos categorías: garantía del mercado y gobernabilidad. La garantía del mercado se refiere a la habilidad de un SGSI para proveer confianza dentro del mercado, en la capacidad de una organización para cuidar de la información de forma segura. En particular, inspirar la confianza de que la organización mantendrá la confidencialidad, integridad y disponibilidad de la información del cliente. La gobernabilidad se refiere a como son gestionadas las organizaciones. En este caso, un SGSI es reconocido por ser una forma proactiva de gestionar la seguridad de la información. (Vanguardia Industrial, 2015)

Una vez que se tenga un SGSI, y a medida que este madure, el personal de la organización a menudo experimentará los beneficios de ser capaz de mejorar la gestión de la seguridad de la información. Por lo tanto las razones de la organización para tener un SGSI pueden expandirse para cubrir tanto la garantía del mercado como el gobierno corporativo. Igualmente, otra organización puede iniciar teniendo un SGSI para una mejor gestión. Sin embargo, a medida que su SGSI madure, debe comunicar las experiencias y noticias sobre las auditorías exitosas de certificación al mercado y conocer el poder de la garantía del mercado para atraer nuevos clientes. (Vanguardia Industrial, 2015)

4.2.5. Análisis y Evaluación de Riesgos

(Daltabuit, Hernández, Mallén, & Vázquez, 2007), definen el análisis de riesgos como la selección de los mecanismos de protección, que permiten estimar las pérdidas potenciales de información, y ayudan a reducirlo facilitando la selección de los mismos. Como lo señala (Puig, 2008), el documento que de esta etapa se derive, será el que se implantará durante la primera fase del SGSI y sus acciones serán de corto, mediano y largo plazo.

Para (Muñoz, 2004), la metodología de análisis y gestión de riesgos de los sistemas de información es el núcleo de las actuaciones relacionadas con el análisis, la evaluación y la gestión del riesgo. Esta metodología analiza los riesgos, identifica las amenazas y su impacto, y gestiona el riesgo basado en:

- Elementos (activos, amenazas, vulnerabilidades, riesgos, impactos, salvaguardas).
- Eventos (estáticos, dinámicos organizativos, dinámicos físicos).

- Procesos (planificación, análisis de riesgos, gestión de riesgos, selección de salvaguardas).

Amenazas

De acuerdo con la normas ISO 27001, se considera amenaza aquella causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a una organización. (Alexander, Diseño de un sistema de gestión de seguridad de la información, 2007), coinciden en que las amenazas se pueden clasificar en grandes grupos para facilitar la toma de decisiones genéricas que reduzcan grupos de amenazas bajo una sola acción. Los grupos propuestos son:

- **Naturales.-** Fuego, inundación, terremotos, etcétera.
- **Humanas Accidentales.-** Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- **Humanas Intencionales.-** Robo de información, ataques.
- **Tecnológicas.-** Virus, hacker, crackers, pérdida de datos, fallas de software, hardware ó de red.

Luego de identificadas todas las amenazas, se evalúa su probabilidad de ocurrencia. El resultado de esta evaluación permitirá identificar las amenazas de mayor a menor concurrencia y la decisión sobre cuales atacar y cuales descartar de acuerdo con criterios técnicos, legales y de costos.

Vulnerabilidades

Las vulnerabilidades están asociadas a debilidades de los activos de información. De acuerdo con (Alexander, Análisis del riesgo y el sistema de gestión de Información: el enfoque ISO 27001:2005, 2006), la vulnerabilidad en el contexto de los

sistemas de información es considerada como la ausencia o debilidad en los controles que ayudan a mitigar un riesgo, aumentando el nivel de impacto y el factor de exposición. De acuerdo con la norma ISO 17799-2005, las vulnerabilidades son clasificables según como lo indica la tabla N° 2.

Recursos Humanos	Controles de acceso	Seguridad física y ambiental	Gestión de operaciones y comunicación	Mantenimiento, desarrollo y adquisición de sistemas de información
Falta de capacitación en temas de seguridad	Falta de políticas de escritorio	Controles de acceso físico no adecuado	Interfaces complicadas para los usuarios	No hay protección de llaves criptográficas
Falta de mecanismos de monitoreo	Segregación inapropiada de redes	Ubicación de áreas críticas en zonas de alto riesgo	Inadecuado manejo de controles de cambio	Falta de políticas en el uso de criptografía
Falta de políticas de uso de medios de telecomunicaciones	Falta de protección de equipos de telecomunicaciones	Falta de programas de renovación de equipos	Inadecuada gestión de redes	Falta de validación de datos procesados
No eliminación de accesos al retirar los empleados	Políticas débiles para el manejo de claves	Descuidos con los equipos	Falta de mecanismos de aseguramiento de envío de mensajes o datos	Falta de ambientes para pruebas
Falta de control de activos devueltos al finalizar los contratos		Falta de regulación de voltaje	Carencia de segregación de tareas	Falta de documentación de software
Desmotivación de empleados			Falta de protección de redes públicas	Malas prácticas en procesos de pruebas de ensayo

Tabla N° 2. Clasificación de vulnerabilidades
Fuente: (Alexander, 2006)

Según (Granada, 2009) las amenazas y las vulnerabilidades tienen interrelación, se parte de la pregunta sobre cuáles vulnerabilidades son aprovechadas por las amenazas, pues, una vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto sobre cualquier sistema de información. Esto es lo que para expertos en temas de seguridad de información se conoce como la relación causa-efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será el de integrar estos elementos para analizar y definir los niveles de riesgo que luego permitirán implementar los procedimientos que ayudarán a mitigar tales riesgos y eliminar las vulnerabilidades.

4.2.6. Cálculo de Riesgo

Una vez se listan y clasifican los activos y se identifican las amenazas y vulnerabilidades, se procede al cálculo del riesgo. Este cálculo utilizará valores cuantitativos pues el valor de un activo de información se tasa en el impacto en pérdidas económicas que el mismo genera si es vulnerado. Para (Daltabuit, Hernández, Mallén, & Vázquez, 2007), el análisis de riesgo se puede realizar de 2 formas:

- **Análisis cuantitativo.-** Basado en la métrica y el cálculo de valores que determinen el costo-beneficio, su cálculo demanda un gran esfuerzo, pero permiten la comparación de valores.

- **Análisis cualitativo.-** Es más ágil, pero sus resultados son más subjetivos los cuales no se basan en cifras y contienen análisis sencillos. No permiten la comparación de valores más allá del orden relativo.

4.2.7. Tratamiento de Riesgo

A partir del informe de evaluación de riesgos se procede a examinar cual es el tratamiento más adecuado para cada uno de los riesgos que han sido identificados.

Siguiendo los lineamientos de la norma ISO 27001, el tratamiento de riesgos comprende los siguientes enfoques:

Determinar si el riesgo es aceptable o si requiere un tratamiento, en cuyo caso se identificará una de las siguientes alternativas:

- Reducir el riesgo a un nivel aceptable, implantando algún control (combinación de personas, procesos y herramientas).
- Aceptar el riesgo porque no es posible realizar un tratamiento o porque éste resulta demasiado costoso.
- Evitar el riesgo, o
- Transferir el riesgo a una tercera parte (Por ejemplo, Compañías de Seguros).

En caso de que se decida mitigar el riesgo se debe definir que controles del SGSI se deben implementar. Además, si se considera necesario se pueden seleccionar controles específicos adicionales.

Para definir los controles a implementar en base al análisis de riesgo de deben realizar los siguientes pasos:

1. Preparar un Documento de Declaración de Aplicabilidad (DDA), en el que se detalle la relación de controles que se van a implantar.
2. Establecer el nivel de riesgo aceptable para la Organización.

3. Obtener la aprobación de la dirección a la DDA y a los riesgos no cubiertos.

4. Formular un plan de tratamiento de riesgos en el que se establecerán las acciones necesarias para conseguir mitigar los riesgos a un nivel aceptable y para implantar los controles que se consideren necesarios según requerimiento de la norma ISO/IEC 27001 en sus numerales 4.2.1.f, g y h.

5. Preparar los procedimientos necesarios para la implantación de controles.

4.2.8. ISO/IEC 27001:2013

ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) para cualquier organización sin importar su tipo o tamaño. BSI (British Standards Institution) recomienda que cada organización tenga un sistema implementado para mantener la confidencialidad, integridad y disponibilidad de la información. Esto deberá incluir su propia información así como la información de sus clientes y de otras partes interesadas.

COMPARANDO ISO/IEC 27001:2013 CON ISO/IEC 27001:2005

ISO/IEC 27001:2013 es la primera revisión de ISO/IEC 27001. En primer lugar y ante todo la revisión ha tomado en cuenta la experiencia práctica del uso del estándar: actualmente hay 17,000 certificados en el mundo. Sin embargo, ha habido otras dos influencias mayores en la revisión. La primera es un requerimiento de ISO que todo estándar nuevo o revisado debe ajustarse a la estructura de alto nivel y debe tener el texto central idéntico definido en el Anexo SL de la Parte 1 de las Directrices

de ISO/IEC. Conforme a estos requerimientos se tendrá una tendencia para hacer que todos los estándares de sistemas de gestión luzcan igual, con la intención de que los requerimientos del sistema de gestión que no son una disciplina específica sean redactados de la misma manera en todos los estándares de sistemas de gestión. Estas son buenas noticias para todas las organizaciones que operan sistemas de gestión integrados, por ejemplo los sistemas de gestión que conforman varios estándares, como ISO 9001 (calidad), ISO 22301 (continuidad del negocio) así como ISO/IEC 27001. La segunda influencia fue una decisión para alinear ISO/IEC 27001 con los principios y guías dados por ISO 31000 (gestión de riesgos). De nuevo, estas son buenas noticias para los sistemas de gestión integrados pues ahora una organización puede aplicar la misma metodología de riesgos a través de varias disciplinas.

El resultado es que estructuralmente ISO/IEC 27001:2013 luce muy diferente a ISO/IEC 27001:2005. Además, no hay requerimientos duplicados y están expresados de una manera que permite mayor libertad de elección sobre cómo implementarlos. Un buen ejemplo de esto es que la identificación de activos, amenazas y vulnerabilidades no es más larga que un pre requisito para la identificación de riesgos para la seguridad de la información. El estándar ahora es más claro en cuanto a que los controles no deben de ser seleccionados del Anexo A, pero son determinados a través del proceso de tratamiento de riesgos. Sin embargo, el Anexo A continúa sirviendo como una verificación para asegurar que no existen controles necesarios que se hayan pasado por alto.

Se han introducido nuevos conceptos (o actualizado) como los siguientes:

CONCEPTO NUEVO/ACTUALIZADO	EXPLICACIÓN
Contexto de la organización	El ambiente en el que la organización opera.
Problemas, riesgos y oportunidades	Reemplaza acciones preventivas.
Partes interesadas	Reemplaza accionistas (stakeholders).
Liderazgo	Requerimientos específicos para la alta dirección.
Comunicación	Hay requerimientos específicos tanto para comunicaciones internas como externas.
Objetivos de seguridad de la Información	Los objetivos de seguridad de la información ahora se establecen como funciones relevantes y niveles.
Evaluación de riesgos	La identificación de activos, amenazas y vulnerabilidades ya no es un pre requisito para la identificación de riesgos de seguridad de la información.
Propietario de riesgo	Reemplaza propietario de los activos.
Plan de tratamiento de riesgos	La efectividad del plan de tratamiento de riesgos es ahora considerada como más importante que la efectividad de los controles.
Controles	Los controles ahora son determinados durante el proceso de tratamiento de riesgos, en lugar de ser seleccionados del Anexo A.
Información documentada	Reemplaza documentos y registros.
Evaluación del desempeño	Cubre las mediciones del SGSI y de la efectividad del plan de tratamiento de riesgos.
Mejora continua	Se pueden utilizar metodologías distintas a Planear-Hacer-Verificar-Actuar (PDCA por sus siglas en inglés).

Tabla N° 3. Nuevos conceptos en la ISO/IEC 27001:2013

Fuente: (Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013)

Los cambios que destacan son:

- Desaparece la sección "enfoque a procesos" que contenía la versión 2005, en donde se describía el modelo PDCA, corazón del Sistema de Gestión de Seguridad de la Información (SGSI), dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Pasa de 102 requisitos a 130.
- Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios de 11 a 14 y disminuyendo el número de controles de 133 a 114.
- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades. (ISO/IEC 27001 (Wikipedia))

DATOS COMPARATIVOS

ISO 27001:2013	ISO 27001:2005
7 Clausulas: **La más restante es el contexto de la organización.**	5 Clausulas.
14 Dominios.	11 Dominios.
154 Requerimientos (32 nuevos requerimientos).	178 Requerimientos.
114 Controles	133 Controles.
El anexo A tiene 14 categorías de control (del 5 al 18).	El anexo A tiene 11 categorías de control (del 5 al 15).
Menciona a la ISO 31000 en la cláusula 6.1 Acciones para la dirección de riesgos y oportunidades.	No menciona la ISO 31000 u otro estándar.

Tabla N° 4. Datos comparativos entre ISO/IEC 27001:2005 e ISO/IEC 27001:2013
Fuente: (Collazos Balaguer, 2013)

ESTRUCTURA DEL NUEVO ESTÁNDAR

ISO/IEC 27001:2013 ha sido desarrollado con base en el anexo SL de ISO/IEC del “Suplemento Consolidado de las Directivas ISO/IEC” (anteriormente publicado como “Guía ISO:83”), en el cual se proporciona un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia. Así pues, la nueva estructura queda como sigue:

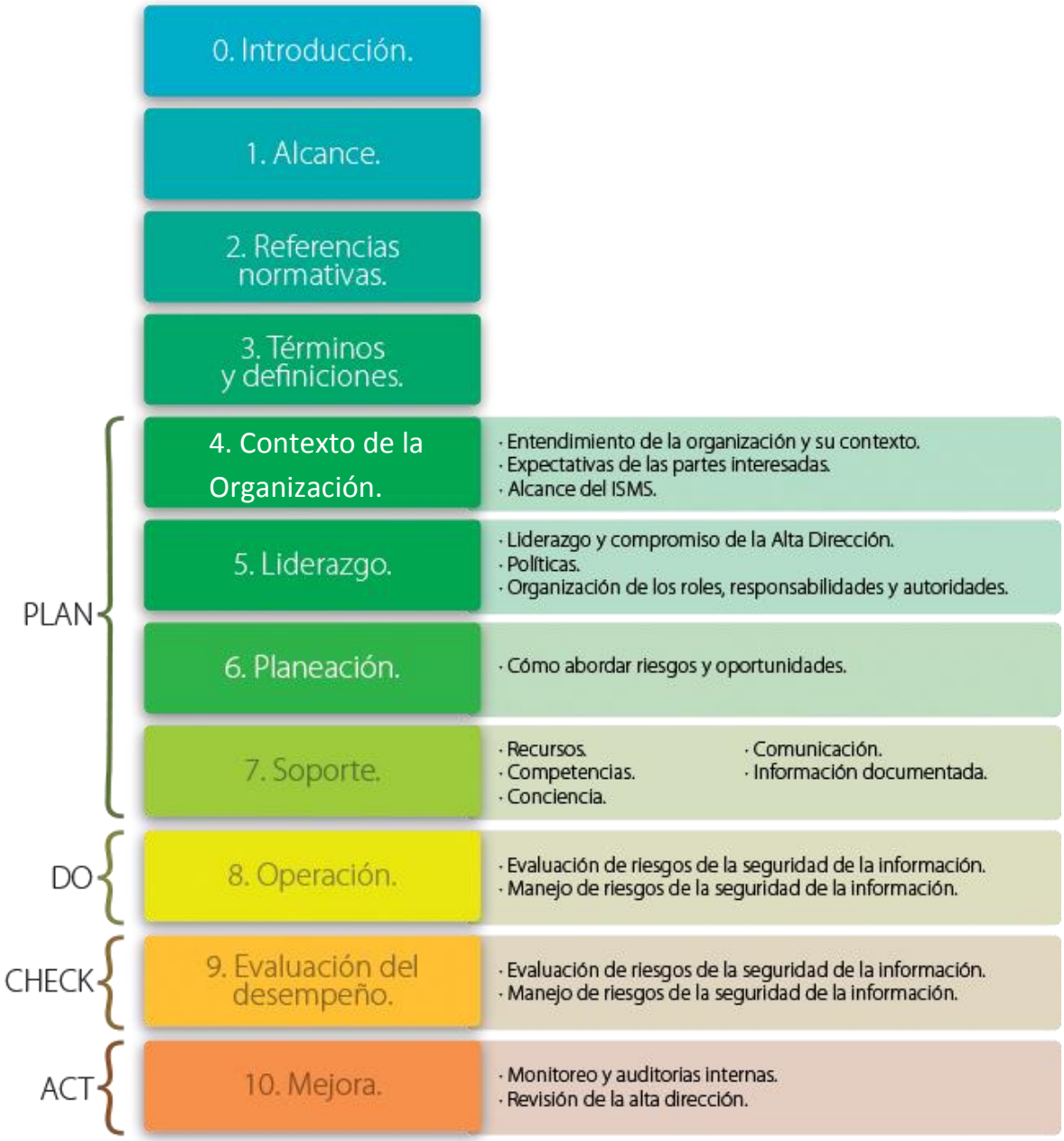


Figura N° 3: Estructura del nuevo estándar ISO 27001:2013
Fuente: (Collazos Balaguer, 2013)

DESCRIPCIÓN DE LAS PRINCIPALES SECCIONES

0. Introducción

Esta cláusula es mucho más corta que su predecesora. En particular la sección sobre el modelo PDCA ha sido eliminada. La razón para esto es que el requerimiento es para la mejora

continua (ver Cláusula 10) y el PDCA es solo una propuesta para cumplir con este requerimiento. Hay otras propuestas y las organizaciones son ahora libres de utilizarlas si así lo desean. La introducción también hace énfasis en el orden en el cual serán presentados los requerimientos, estableciendo que el orden no refleja la importancia o implica el orden en el cual serán implementados.

1. Alcance

Esta también es una cláusula mucho más corta. En particular no hay referencia a la exclusión de controles en el Anexo A.

En esta sección se establece la obligatoriedad de cumplir con los requisitos especificados en los capítulos 4 a 10 del documento, para poder obtener la conformidad de cumplimiento y certificarse.

2. Referencias normativas

El estándar ISO-27002 ya no es una referencia normativa para ISO-27001:2013, aunque continúa considerándose necesario en el desarrollo de la declaración de aplicabilidad (SOA, por sus siglas en inglés).

El estándar ISO 27000:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

3. Términos y definiciones

Los términos y definiciones que se manejaban en 27001:2005 los trasladaron y agruparon en la sección 3 de ISO 27000:2013 “Fundamentos y vocabulario” (lo cual se llevará a cabo en todos los documentos que forman parte de esta familia),

con el objetivo de contar con una sola guía de términos y definiciones que sea consistente.

4. Contexto de la organización

Esta cláusula hace hincapié en identificar los problemas externos e internos que rodean a la organización.

- ✓ Instituye los requerimientos para definir el contexto del SGSI sin importar el tipo de organización y su alcance.
- ✓ Introduce una nueva figura (las partes interesadas) como un elemento primordial para la definición del alcance del SGSI.
- ✓ Establece la prioridad de identificar y definir formalmente las necesidades de las partes interesadas con relación a la seguridad de la información y sus expectativas con relación al SGSI, pues esto determinará las políticas de seguridad de la información y los objetivos a seguir para el proceso de gestión de riesgos.

5. Liderazgo

Ajusta la relación y responsabilidades de la Alta Dirección respecto al SGSI, destacando de manera puntual cómo debe demostrar su compromiso, por ejemplo:

- ✓ Garantizando que los objetivos del SGSI y “La política de seguridad de la información”, anteriormente definida como “Política del SGSI”, estén alineados con los objetivos del negocio.
- ✓ Garantizando la disponibilidad de los recursos para la implementación del SGSI (económicos, tecnológicos, etcétera).
- ✓ Garantizando que los roles y responsabilidades claves para la seguridad de la información se asignen y se comuniquen adecuadamente.

6. Planeación

Esta es una nueva sección enfocada en la definición de los objetivos de seguridad como un todo, los cuales deben ser claros y se debe contar con planes específicos para alcanzarlos.

Se presentan grandes cambios en el proceso de evaluación de riesgos:

- ✓ El proceso para la evaluación de riesgos ya no está enfocado en los activos, las vulnerabilidades y las amenazas.
- ✓ Esta metodología se enfoca en el objetivo de identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información.
- ✓ El nivel de riesgo se determina con base en la probabilidad de ocurrencia del riesgo y las consecuencias generadas (impacto), si el riesgo se materializa.
- ✓ Se ha eliminado el término “Propietario del activo” y se adopta el término “Propietario del riesgo”.
- ✓ Los requerimientos del SOA no sufrieron transformaciones significativas.

7. Soporte

Marca los requerimientos de soporte para el establecimiento, implementación y mejora del SGSI, que incluye:

- ✓ Recursos
- ✓ Personal competente
- ✓ Conciencia y comunicación de las partes interesadas

Se incluye una nueva definición “información documentada” que sustituye a los términos “documentos” y “registros”; abarca el

proceso de documentar, controlar, mantener y conservar la documentación correspondiente al SGSI.

El proceso de revisión se enfoca en el contenido de los documentos y no en la existencia de un determinado conjunto de estos.

8. Operación

Establece los requerimientos para medir el funcionamiento del SGSI, las expectativas de la Alta Dirección y su realimentación sobre estas, así como el cumplimiento con el del estándar.

Además, plantea que la organización debe planear y controlar las operaciones y requerimientos de seguridad, erigiendo como el pilar de este proceso la ejecución de evaluaciones de riesgos de seguridad de la información de manera periódica por medio de un programa previamente elegido.

Los activos, vulnerabilidades y amenazas ya no son la base de la evaluación de riesgos. Solo se requiere para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

9. Evaluación del desempeño

La base para identificar y medir la efectividad y desempeño del SGSI continúan siendo las auditorías internas y las revisiones del SGSI.

Se debe considerar para estas revisiones el estado de los planes de acción para atender no conformidades anteriores y se establece la necesidad de definir quién y cuándo se deben realizar estas evaluaciones así como quién debe analizar la información recolectada.

10. Mejora

El principal elemento del proceso de mejora son las no-conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurar que no se repitan y que las acciones correctivas sean efectivas.

Aquí se observa uno de los cambios más importantes porque las medidas preventivas se fusionarán con la evaluación y tratamiento del riesgo, algo más natural e intuitivo que permite enfrentar los riesgos y las oportunidades con base en cuándo estos se identifican y cómo se tratan. Además, se distingue entre las correcciones que se ejecutan como una respuesta directa a una "no conformidad", en oposición a las acciones correctoras que se realizan para eliminar la causa de la no conformidad. (Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013)

4.3. Selección de la metodología a utilizar para el desarrollo de la investigación

4.3.1. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración y en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

El análisis y gestión de los riesgos es un aspecto clave en el ámbito de la Administración Electrónica que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información. MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema de Seguridad. (PAE: portal de administración electrónica, 2012)

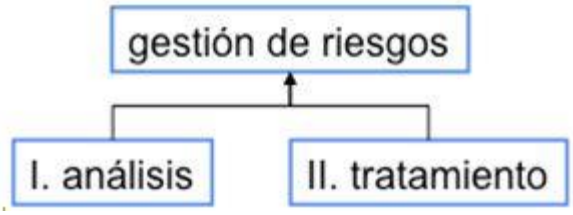


Figura N° 4: Gestión de riesgo de MAGERIT
Fuente:
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vwvgs5zhBdg

OBJETIVOS

MAGERIT persigue los siguientes objetivos directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

La metodología de Gestión del Riesgo se ha dividido en 4 partes:

- Inventario de Activos de Información
- Análisis del Riesgo
- Evaluación del Riesgo
- Tratamiento del Riesgo

DERECHOS DE UTILIZACIÓN

MAGERIT es una metodología de carácter público, su utilización no requiere autorización previa del mismo. (PAE: portal de administración electrónica, 2012)

4.3.2. Metodología basada en el Ciclo de Mejora Continua

(Wikipedia, 2014)

Para la evaluación de Sistema de Gestión de Seguridad de Información, se ha tomado como criterio la metodología establecida en el ciclo de mejora continua dada por la Norma ISO 27001, norma de referencia para el desarrollo de la Circular N° G-140-2009 del Sistema de Gestión de Seguridad de Información.

Los criterios usados para la evaluación de un Sistema de Gestión de Seguridad de Información, comprenden la evaluación del razonable cumplimiento de las etapas del Sistema de Gestión de Seguridad de Información, la cual se presenta a continuación:

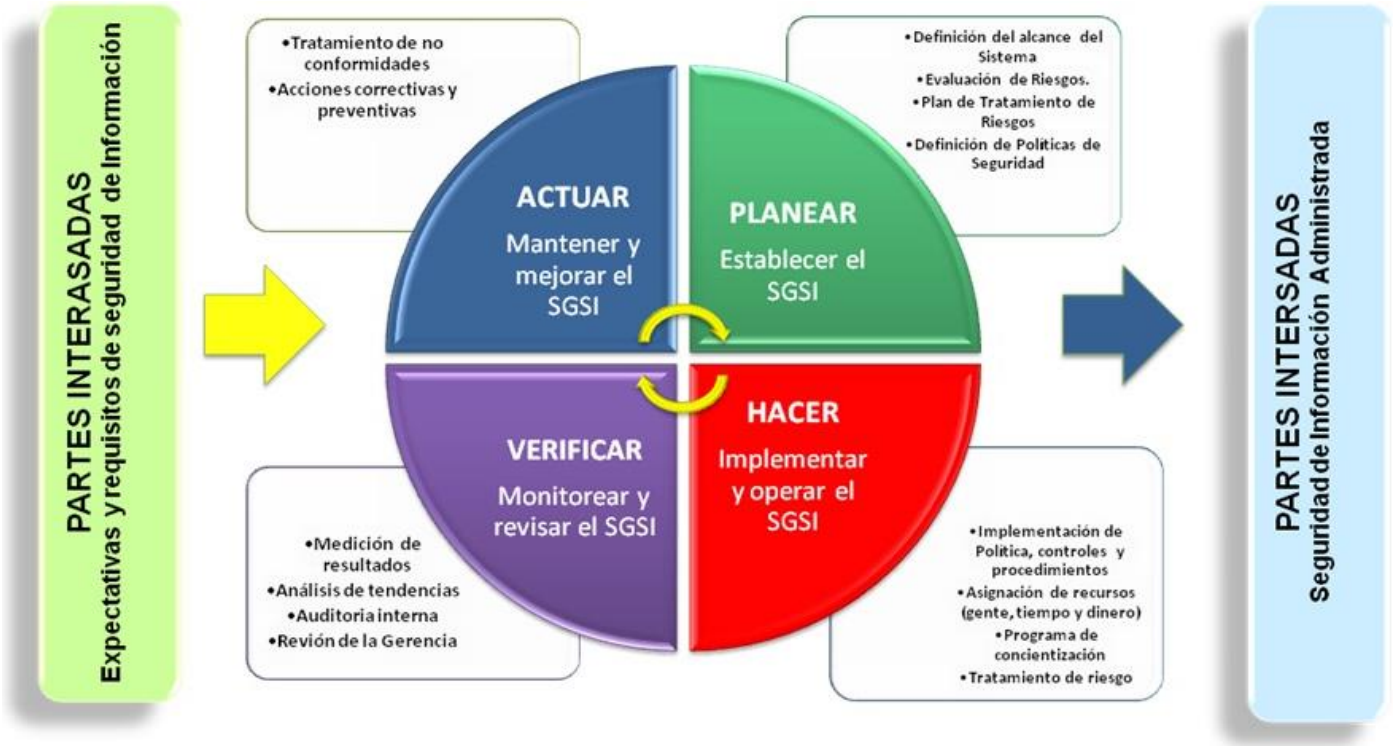


Figura N° 5Ciclo PDCA
Fuente: http://toddleoutsourcing.es/tecnologia/seguridad/implementacion-sgsi/

Etapa 1: Establecer el SGSI (PLAN)

Conocida como plan, comprende el establecimiento del Sistema de Gestión de Seguridad de Información, en esta etapa se definen las políticas, objetivos, procesos y procedimientos del SGSI pertinentes para gestionar el riesgo y mejorar la seguridad de la información, a fin de entregar resultados conforme a las políticas y objetivos generales de la organización.

Etapa 2: Implementar y Operar el SGSI (HACER)

Conocida como Hacer, en esta etapa se busca implementar y operar la política, controles, procesos y procedimientos del SGSI.

Etapa 3: Monitorear y Revisar el SGSI (VERIFICAR)

Conocida como Comprobar, en esta etapa se busca evaluar y, donde corresponda, medir el desempeño del proceso según la política, objetivos y experiencia práctica del SGSI e informar los resultados a la Gerencia para su examen.

Etapa 4: Mantener y Mejorar el SGSI (ACTUAR)

En esta etapa se busca tomar medidas correctivas y preventivas, basado en los resultados de la auditoría interna del SGSI y el examen de la gerencia u otra información pertinente, para lograr el mejoramiento continúo del SGSI.

4.3.3. Operativamente amenaza crítica de activos y evaluación de la vulnerabilidad (OCTAVE).

(Talero Benitez, 2015)

Es una metodología de análisis de riesgos orientado a activos y a la gestión de los riesgos para garantizar la seguridad de sistemas informativos.

Realiza una evaluación de riesgos en la seguridad de información considerando los temas organizacionales y técnicos, examina como la gente emplea la infraestructura en forma diaria.

El objetivo de esta metodología es desarrollar una perspectiva de seguridad dentro de una organización, teniendo en cuenta perspectiva de todos los niveles para asegurarse que las soluciones puedan implementarse con facilidad.

La metodología OCTAVE se divide en 3 partes:

- Visión organizativa
  - Activos
  - Amenazas
  - Prácticas actuales
  - Vulnerabilidades organizativas
  - Requerimientos de seguridad
- Visión tecnológica
  - Componentes claves
  - Vulnerabilidades técnicas
  - Prácticas actuales
- Estrategia y plan de desarrollo.
  - Riesgos
  - Estrategia de protección
  - Planes de mitigación

4.3.4. CCTA Risk Analysis and Management Method (CRAMM)

(Huerta, Security Artwork, 2012)

Metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. El significado del acrónimo proviene de CCTA Risk Analysis and Management Method.

La metodología de CRAMM incluye las siguientes 3 etapas:

- La primera de las etapas recoge la definición global de los objetivos de seguridad entre los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en el negocio y la identificación.

- En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las amenazas que afecta al sistema, así como las vulnerabilidades que explotan dichas amenazas y por último el cálculo de los riesgos de materialización de las mismas.

- En la tercera etapa se identifican y seleccionan las medidas de seguridad aplicadas en la entidad obteniendo los riesgos residuales, CRAMM proporciona una librería unas 3000 medidas de seguridad.

4.3.5. National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30)

El NIST (National Institute of Standards and Technology) ha dedicado una serie de publicaciones especiales, la SP 800 a la seguridad de la información. Esta serie incluye una metodología

para el análisis y gestión de riesgos de seguridad de la información, alineada y complementaria con el resto de documentos de la serie.

La Metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo:

Caracterización del Sistema

Durante esta tarea se identifican (por medio de entrevistas y accediendo a información de configuración de los sistemas de información de los sistemas de información) los activos necesarios para que el sistema informático funcione diariamente.

Identificación de Amenaza

Las fuentes de amenazas accidentales o deliberadas deben ser identificadas y su posibilidad de ocurrencia debe ser evaluada.

Identificación de Vulnerabilidades

El objetivo de este paso es de desarrollar una lista de vulnerabilidades del sistema (defectos o debilidades) que podrían ser explotadas por las fuentes de una amenaza potencial.

Control de Análisis

El objetivo de este paso es analizar los controles que han sido puestos en práctica, o son planeados por la organización para reducir al mínimo la probabilidad de ejercer una amenaza sobre las vulnerabilidades del sistema.

Determinación de la Probabilidad

Para obtener la probabilidad de que una potencial vulnerabilidad pueda ser ejecutada en un ambiente de amenazas, los siguientes factores principales deben ser considerados:

Capacidad y Motivación de la fuente de amenaza, Naturaleza de la vulnerabilidad, Existencia y eficacia de controles actuales.

La probabilidad de que una vulnerabilidad potencial podría ser ejercida por una fuente de amenaza dada puede ser descrita como alta, media, o baja.

Análisis de Impacto

Dentro de la medición del nivel de riesgo es importante determinar el impacto adverso, resultado de la ejecución exitosa de una amenaza sobre la organización.

Determinación del Riesgo

El objetivo de este paso es de evaluar el nivel de riesgo en el sistema de información.

Recomendaciones de Control

Durante este paso del proceso, se proporcionan los controles que podrían mitigar o eliminar los riesgos identificados. El objetivo de los controles recomendados es de reducir el nivel de riesgo del sistema de información y sus datos a un nivel aceptable.

Resultado de la Implementación o Documentación

Una vez que la evaluación de riesgo ha sido completada (fuentes de amenaza y vulnerabilidades identificadas, controles evaluados, y recomendados), los resultados deberían ser documentados en un informe oficial o dentro de una reunión informativa. Un informe de evaluación de riesgos es una gestión que ayuda a la dirección de la organización, a los dueños de la empresa, para la toma de decisiones sobre la política, procesal, el presupuesto, y el sistema operacional y cambios de en la gestión de la seguridad.

El proceso de gestión de riesgos definido en la metodología NIST SP 800-30 está compuesto por los siguientes 7 pasos:

- Priorización de acciones.
- Evaluación de opciones de controles recomendados.
- Análisis coste-beneficio.
- Selección de controles.
- Asignación de responsabilidades.
- Desarrollo de plan de implantación de salvaguardas.
- Implantación de controles seleccionados.

4.3.6. Mehari

(Huerta, Security Artwork, 2012)

MEHARI es la metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (**C**lu*b de la* **S***écurité de* **I***nformation* **F***rançais*) en 1995 y deriva de las metodologías previas *Melissa* y *Marion*. La metodología ha evolucionado proporcionando una guía de implantación de la seguridad en una entidad a lo largo del ciclo de vida. Del mismo modo, evalúa riesgos en base a los criterios de disponibilidad, integridad y confidencialidad.

Objetivos

MEHARI es un conjunto de herramientas y funcionalidades metodológicas para la gestión de la seguridad y de las medidas asociadas, basado en un análisis de riesgos preciso.

Los aspectos fundamentales de MEHARI son:

- Su modelo de riesgos (cualitativo y cuantitativo).
- El examen de la eficacia de las medidas de seguridad en vigor o previstas.
- La capacidad para evaluar y simular los niveles de riesgos derivados de medidas adicionales.

MEHARI, se puede integrar de forma sencilla en el proceso PDCA (Plan-Do-Check-Act).

4.3.7. Construct a platform for Risk Analysis of Security critical system (CORAS)

(Seguridad Informática, 2012)

Desarrollado a partir de 2001 por SINTEF (Noruego: Stiftelsen for Industrial Log Teknisk for Skning), un grupo de investigación noruego financiado por organizaciones del sector público y privado.

Los siete pasos del método CORAS son:

- Presentación: Reunión inicial, para presentar los objetivos y el alcance del análisis y recabar información inicial.
- Análisis de alto nivel: Entrevistas para verificar la comprensión de la información obtenida y la documentación analizada. Se identifican amenazas, vulnerabilidades, escenarios e incidentes.
- Aprobación: Descripción detallada de los objetivos, alcance y consideraciones, para su aprobación por parte del destinatario del análisis de riesgos.
- Identificación de riesgos: Identificación detallada de amenazas, vulnerabilidades, escenarios e incidentes.
- Estimación de riesgo: Estimación de probabilidades e impactos de los incidentes identificados en el paso anterior.

- Evaluación de riesgo: Emisión del informe de riesgos, para su ajuste fino y correcciones.
- Tratamiento del riesgo: Identificación de las salvaguardas necesarias, y realización de análisis coste/beneficio.

4.3.8. Expression des Besoins Et Identification des Objectifs de Sécurité (EBIOS)

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives) es una metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información.

El método EBIOS permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI). Posibilita también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos SSI. Brinda las justificaciones necesarias para la toma de decisiones; puede utilizarse para numerosas finalidades y procedimientos de seguridad, tales como la elaboración de esquemas directivos, de políticas, de políticas de protección o de objetivos de seguridad, de los planes de acción o de cualquier otra forma de pliego de condiciones de SSI.

EBIOS puede ser utilizado para estudiar tanto sistemas por diseñar como sistemas ya existentes. En el primer caso, permite determinar progresivamente las especificaciones de seguridad integrándose a la gestión de proyectos. En el segundo caso, considera las medidas de seguridad existentes e integra la seguridad a los sistemas en funcionamiento.

Las cinco fases de la metodología EBIOS son:

- Análisis de contexto

- Requerimientos de seguridad
- Análisis de riesgo
- Identificación de objetivos de seguridad
- Determinación de requerimientos de seguridad

4.3.9. Otras Metodologías

- **ITIL:** Information Technology Infraestructure Library, proporciona un planteamiento sistemático para la provisión de servicios de TI con calidad.

- **ISO 31000:** Esta normativa establece principio y guías para diseñar, implementar mantener la gestión de los riesgos en forma sistemática y de transparencia de toda forma de riesgo, por ejemplo: financiera, operativa, de mercadeo, de imagen, y de seguridad de información.

- **NIST SP 800-39:** Gestión de Riesgos de los Sistemas de Información, una perspectiva organizacional.

- **AS/NZS:** Norma de Gestión de Riesgos publicada conjuntamente por Australia y Nueva Zelanda.

- **ANÁLISIS HOLANDÉS A&K:** Es método de análisis de riesgos, del que hay publicado un manual, que ha sido desarrollado por el Ministerio de Asuntos Internos de Holanda, y se usa en el gobierno y a menudo en empresas holandesas.

- **Integración de modelos de madurez de capacidades o Capabilit Maturity Model Integration (CMMI):** es un modelo para la mejora y evaluación de procesos para el

desarrollo, mantenimiento y operación de sistemas de software.

- **ISO/IEC 15504**: también conocido como Software Process Improvement Capability Determination, abreviado SPICE, en español, «Determinación de la Capacidad de Mejora del Proceso de Software» es un modelo para la mejora, evaluación de los procesos de desarrollo, mantenimiento de sistemas de información y productos de software.

4.3.10. Criterios de selección de la metodología

Para el presente trabajo de investigación se ha realizado un cuadro comparativo de las metodologías de análisis y gestión de riesgos más usadas y sobre las cuales se obtuvo mayor información de interés acorde a las necesidades del proyecto, clasificando sus fortalezas y bondades en una escala de “muy bajo” a “muy alto” con el objetivo de escoger una metodología apropiada para este proyecto.

Escala	Valor de importancia
1	MUY BAJO
2	BAJO
3	MEDIO
4	ALTO
5	MUY ALTO

Tabla N° 5. Criterios de selección de metodologías
Fuente: (Carrillo Sanchéz, 2013)

El puntaje total por metodología está dado por la siguiente fórmula:

$$Total = AR + GR + FC - CA$$

Donde **AR:** Análisis de riesgos.

GR: Gestión de riesgos.

FC: Facilidad de comprensión.

CA: Costo por la aplicación de la Metodología.

Clasificación:

Enunciado	MAGERIT	OCTAVE	CRAMM	NIST SP 800-30
ALCANCE CONSIDERADO				
Análisis de riesgos	5	5	5	5
Gestión de riesgos	5	5	5	5
COMPRENSIÓN				
Facilidad de comprensión	5	4	4	4
FINANCIAMIENTO				
Costos por la aplicación de la Metodología	1	4	5	3
RESULTADO				
Puntaje Total	**14**	10	9	11

Tabla N° 6. Cuadro comparativo de metodologías de gestión de riesgo
Fuente: (Carrillo Sanchéz, 2013)

Según el análisis del cuadro comparativo de metodologías podemos concluir que MAGERIT es la mejor metodología para la aplicación de este proyecto de investigación, obteniendo está el mayor puntaje de entre todas las metodologías, por su facilidad de comprensión y menor costo económico enla aplicación del diseño.

Por lo tanto para el presente trabajo de investigación se decidió realizar nuestra propuesta basándonos en el ciclo de

mejora continua (Ciclo PDCA) y hemos optado por aplicar la Metodología MAGERIT, apoyándose en el análisis y vulnerabilidades existentes en los activos involucrados en el mantenimiento y proceso de la información.

4.4. Conceptos y Definiciones

- **Activos.-** Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse (Estos pueden ser: ficheros, bases de datos, contratos, acuerdos, documentación del sistema, etc.).

- **Amenaza.-** Es la probabilidad de que ocurra un hecho indeseado y que tenga un efecto negativo sobre un activo.

- **Análisis de Riesgo.-** Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas.

- **Auditoria.-**Es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

- **Autenticidad.-** Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quiénes dicen ser que son.

B

- **Backup.-** Una "copia de seguridad", "copia de respaldo" o también llamado "backup" (su nombre en inglés) es una copia de los datos y/o archivos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

C

- **COBIT.-** (Control Objectives for Information and Related Technology) que traduce como: Objetivos de Control para Tecnología de Información y Tecnologías relacionadas, es un modelo utilizado para auditar los sistemas de información de toda la organización, incluyendo los computadores personales y las redes.

- **Confidencialidad.-** Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

- **Control.-** Son medidas que se implementan con el fin de mitigar los riesgos.

- **Control de acceso.-** Es el proceso de conceder permisos a usuarios o grupos de acceder a objetos tales como ficheros o impresoras en la red.

D

- **Documento de Declaración de Aplicabilidad.-** Se trata de un documento que enlista los controles de seguridad establecidos en

el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad).

E

- **Evaluación de Riesgo.-** Es el proceso global de identificación, análisis y estimación de riesgos.

F

- **Firewalls.-** (Cortafuegos en español). Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

G

- **Gestión de riesgo.-** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

H

- **Hackers.-** Un hacker es una persona que por sus avanzados conocimientos en el área de informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador.

I

- **Infraestructura de clave pública (PKI).-** En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

- **Integridad.-** Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados.

- **Interfaces.-** Se utiliza para nombrar a la conexión funcional entre dos sistemas o dispositivos de cualquier tipo dando una comunicación entre distintos niveles.

- **ISO/IEC.-** Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

L

- **Llaves Criptográficas.-** Es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

- **Logs.-** Un log es un registro oficial de eventos durante un rango de tiempo en particular. Los profesionales en seguridad

informática lo usan para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

M

- **MAGERIT.-** Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.

- **Malware.-** Es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra malware proviene del término en inglés malicious software, y en español es conocido con el nombre de código malicioso.

- **Mitigar.**- Disminuir la intensidad, la gravedad o la importancia de algo.

N

- **No Repudio.**- Garantizar que la transferencia de un mensaje ha sido enviado y recibido por entidades que son quienes dicen ser.

O

- **Octave.**- Es un sistema basado en estrategias y técnicas de planificación de la Compañía de Seguridad Interna, hecha por riesgo CERT (Equipo de Respuesta a Emergencias). Es

especialmente adecuado para las empresas que desean conocer completamente lo que sus necesidades de seguridad.

P

- **PDCA.-**Plan-Do-Check-Act. Tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización.

- **Política de seguridad.-** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

R

- **Riesgo.-** Es la probabilidad de que se materialice una amenaza y determine el nivel de impacto en una organización.

- **RISK IT.-** Es un marco complementario a COBIT, que establece prácticas dirigidas a identificar, gobernar y administrar los riesgos asociados al negocio en su relación con las TIC: el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TIC dentro de una organización.

S

- **Seguridad de la Información.-** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas

tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

- **SGSI.-** Sistema de gestión de la seguridad de la información, como el nombre lo sugiere, es un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

- **Sistema de Información.-** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

T

- **Telecomunicaciones.-** Es el estudio y aplicación de la técnica que diseña sistemas que permitan la comunicación a larga distancia a través de la transmisión y recepción de señales.

- **Tratamiento de riesgo.-** Es el proceso de modificar el riesgo, mediante la implementación de controles.

V

- **Virus.-** Es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan Archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

- **VLAN.-** Una VLAN es un acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

- **Vulnerabilidad.-** Son errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario.

CAPÍTULO V:
DESARROLLO DE LA PROPUESTA

Para desarrollar el diseño de un sistema de gestión de seguridad de la información se tiene que cumplir con los lineamientos establecidos por la ISO/IEC 27001:2013. A continuación el desarrollo de la propuesta:

5.1. Soporte de la dirección

PROPÓSITO

El propósito de este documento es establecer una propuesta para el Diseño de un Sistema de Gestión de la Seguridad de la Información mediante la aplicación del estándar ISO/IEC 27001:2013.

RAZONES

Las razones principales de esta propuesta mediante el estándar ISO/IEC 27001:2013 son:

- Establecer un punto de partida para el diseño de un Sistema de Gestión de la Seguridad de la Información que garantice la confidencialidad, integridad y disponibilidad de la información, asumiendo niveles de riesgos aceptables.
- Comprender la importancia y beneficios que ofrece un Sistema de Gestión de la Seguridad de la Información en la optimización de los procesos institucionales.
- Cumplir con las leyes y regulaciones a las cuales está sujeta la empresa.

ESTRUCTURA DEL PROYECTO

El diseño del proyecto solamente corresponde a la fase de ***planeación*** del Sistema de Gestión de la Seguridad de la Información. No se implementan controles de seguridad, ni se elabora la documentación respectiva de las fases subsiguientes. Dentro de esta fase de planeación se desarrollan las siguientes actividades:

N°	Actividad
1	Análisis Diferencial
2	Políticas de Seguridad de la Información
3	Análisis y Evaluación de Riesgos
4	Declaración de Aplicabilidad
5	Plan de Tratamiento de Riesgos

Tabla N° 7. Planeación de actividades del proyecto.
Fuente: Elaboración propia

RECURSOS

Los recursos incluidos para la planeación del Sistema de Gestión de la Seguridad de la Información están catalogados en Humanos y Técnicos.

- **Humanos**: Trabajadores de las oficinas de la Empresa Agroindustrial Pomalca S.A.A.
- **Técnicos**: Herramientas de ofimática (procesador de texto, hojas de cálculo).
- **Otros**: Documentos del estándar ISO/IEC 27001:2013y documentación correspondiente a las metodologías de análisis y evaluación de riesgos.

5.2. Alcance del Sistema de Gestión de Seguridad de la Información

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir claramente el alcance y límite de la planeación del Sistema de Gestión de la Seguridad de la Información en la Empresa Agroindustrial Pomalca S.A.A.

Este documento es aplicable a toda la documentación y actividades relativas a la planeación del SGSI en cuestión e involucra a todos los trabajadores de empresa.

DOCUMENTOS DE REFERENCIA

- Estándar ISO/IEC 27001:2013, cláusula 4.3. (Determinación del alcance del SGSI).

DEFINICIÓN DEL ALCANCE DEL SGSI

La oficina de Sistemas y Cómputo necesita establecer los límites de la planeación del SGSI con el fin de proteger los activos informáticos que prestan el servicio a la Empresa Agroindustrial Pomalca S.A.A.

Con el fin de alcanzar este objetivo, se ha propuesto desarrollar la fase de planeación de un SGSI mediante el estándar ISO/IEC 27001:2013.

Esta fase de planeación del SGSI comprenderá las siguientes áreas:

- **Oficina de Sistemas y Cómputo**: Comprende el personal administrativo, sus activos informáticos y toda la infraestructura que le presta servicios de TI a la empresa.
- **Oficina de Planeamiento y Desarrollo**: Comprende el personal administrativo y los activos informáticos que se utilizan para llevar a cabos sus actividades diarias y el servicio que le prestan a la empresa.
- **Oficina de Soporte Técnico**: Comprende solamente al personal de soporte del software y hardware de la empresa.

5.3. Análisis Diferencial

La norma o estándar ISO/IEC 27001:2013 requiere el cumplimiento de ciertos criterios para establecer, implementar,

mantener y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información (SGSI) en el contexto de una organización.

Para verificar el estado actual del cumplimiento del estándar ISO/IEC 27001:2013 de la Empresa Agroindustrial Pomalca S.A.A., se realiza un **Análisis Diferencial** de los numerales obligatorios4 al 10 (Requisitos de la Norma ISO/IEC 27001:2013) y del Anexo A (Dominios, Objetivos de Control y Controles de Seguridad). Este análisis permite comparar las condiciones actuales con el fin de encontrar las deficiencias existentes y el nivel de cumplimiento en base al estándar y desarrollar un plan de mejoramiento de acuerdo a los objetivos de seguridad deseados.

5.3.1. Requisitos de la Norma ISO/IEC 27001:2013

Para que una organización esté conforme al estándar ISO/IEC 27001:2013, no se deben excluir ninguno de los requisitos especificados en los numerales 4 al 10.

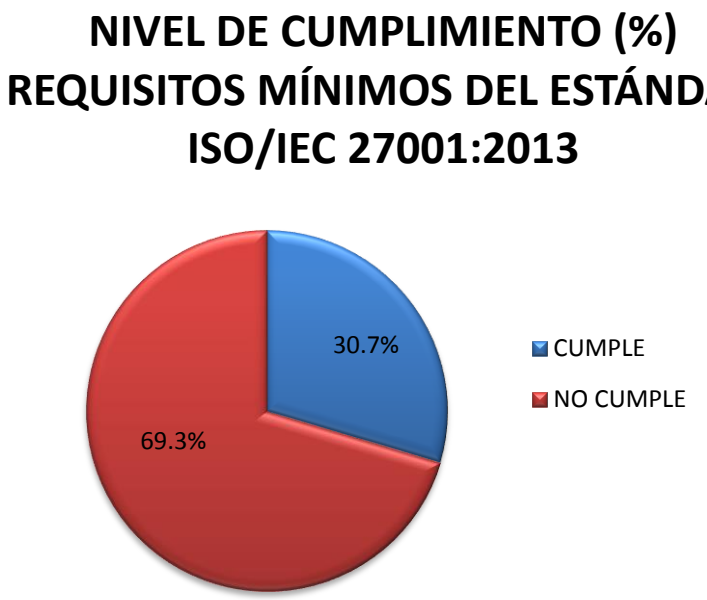
En el Anexo N° 01 (Pág. 128) se muestran los resultados del nivel de conformidad y cumplimiento de estos requisitos.

De esta manera, el nivel de cumplimiento para cada uno de los requisitos mínimos de la norma ISO/IEC 27001:2013 se resume de la siguiente manera:

NOMBRE DEL REQUISITO	CANTIDAD DE REQUISITOS CUMPLIDOS	CUMPLE (%)	NO CUMPLE (%)
4. CONTEXTO DE LA ORGANIZACIÓN	3 de 4	75	25
5. LIDERAZGO	2 de 3	66.7	33.3
6. PLANIFICACIÓN	1 de 4	25	75

7. SOPORTE	2 de 7	28.6	71.4
8. OPERACIÓN	0 de 3	0	100
9. EVALUACIÓN DEL DESEMPEÑO	0 de 3	0	100
10. MEJORA	0 de 2	0	100

Tabla N° 8. Nivel de cumplimiento de los requisitos del estándar ISO/IEC 27001:2013.
Fuente: Elaboración propia



Gráfica N° 1. Nivel de cumplimiento de los requisitos mínimos del estándar ISO/IEC 27001:2013.
Fuente: Elaboración propia

Mediante este Análisis Diferencial fue posible determinar que la Empresa Agroindustrial Pomalca S.A.A. comprende la importancia y beneficios de un SGSI y posee el liderazgo necesario para realizarlo; sin embargo aún no se ha establecido formalmente una metodología de análisis y evaluación de riesgos informáticos y su tratamiento, así como tampoco ningún documento requerido por el estándar ISO/IEC 27001:2013.

5.3.2. Dominios, Objetivos de control y Controles de Seguridad

Se realiza a su vez un Análisis Diferencial referente al Anexo A del estándar ISO/IEC 27001:2013 con el fin de determinar el nivel de cumplimiento de los Dominios, Objetivos de Control y Controles de Seguridad conformes al estándar ISO/IEC 27002:2013. Estos corresponden a los numerales 5 al 18.

En el Anexo N° 02 (Pág. 136) se muestran los resultados del nivel de conformidad y cumplimiento de estos requisitos.

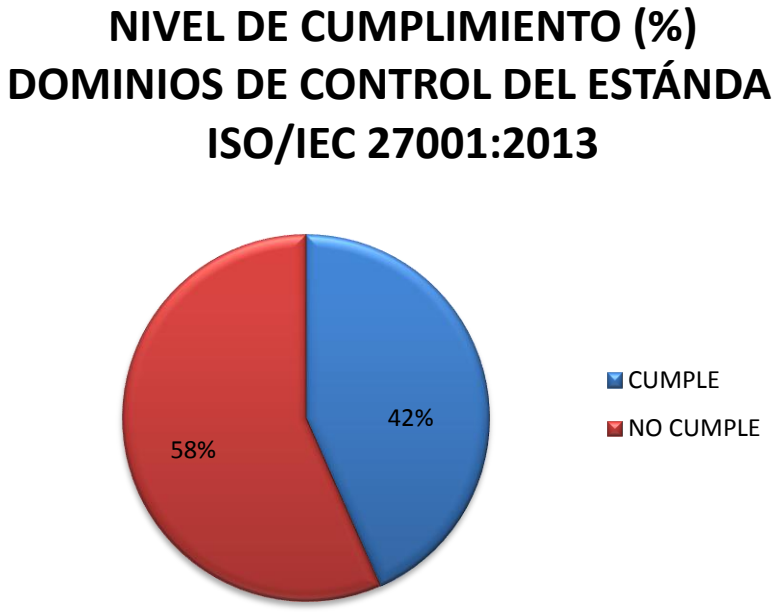
De esta manera, el nivel de cumplimiento para cada uno de los Dominios, Objetivos de Control y Controles de Seguridad del Anexo A del estándar ISO/IEC 27001:2013 (ISO/IEC 27002:2013) se resume de la siguiente manera:

DOMINIO DE CONTROL	CANTIDAD DE DOMINIOS CUMPLIDOS	CUMPLE (%)	NO CUMPLE (%)
A5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0 – 2	0	100
A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1 – 7	14.3	85.7
A7. SEGURIDAD DE LOS RECURSOS HUMANOS	3 – 6	50	50
A8. GESTIÓN DE ACTIVOS	2 – 10	20	80
A9. CONTROL DE ACCESO	8 – 14	57.1	42.9
A10. CRIPTOGRAFÍA	0 – 2	0	100
A11. SEGURIDAD FÍSICA Y DEL ENTORNO	9 – 15	60	40
A12. SEGURIDAD DE LAS OPERACIONES	8 – 14	57.1	42.9

A13. SEGURIDAD DE LAS COMUNICACIÓN	3 – 7	42.9	57.1
A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	7 – 13	53.8	46.2
A15. RELACIONES CON LOS PROVEEDORES	0 – 5	0	100
A16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	4 – 7	57.1	42.9
A17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0 – 4	0	100
A18. CUMPLIMIENTO	3 – 8	37.5	62.5

Tabla N° 9. Nivel de los Dominios de Control del estándar ISO/IEC 27002:2013.
Fuente: Elaboración propia

Y el nivel de cumplimiento general que se tiene actualmente referente a estos Dominios de Control es el siguiente:



Gráfica N° 2. Nivel de cumplimiento de los Dominios de control del estándar ISO/IEC 27002:2013.
Fuente: Elaboración propia

Mediante este Análisis Diferencial es posible determinar que la Empresa Agroindustrial Pomalca S.A.A. no cumple con la mayoría de los Dominios, Objetivos de Control y Controles de Seguridad propuestos en la norma ISO/IEC 27002:2013. Esto se refleja en que no se tiene la documentación correspondiente al estándar ISO/IEC 27001:2013 así como tampoco el empleo de mecanismos de seguridad en la transmisión de la información.

Por otro lado, aunque las instalaciones físicas estén protegidas con algunos métodos de vigilancia, el personal y algunos activos informáticos no están lo suficientemente protegidos ante una eventualidad de orden mayor, y no existen procedimientos de contingencia para garantizar la continuidad de las operaciones.

5.4. Políticas de Seguridad de la Información

PROPÓSITO, ALCANCE Y USUARIOS

La Empresa Agroindustrial Pomalca S.A.A. se compromete a proteger los pilares fundamentales de la seguridad informática como lo son la Confidencialidad, Integridad y Disponibilidad de la información, así como todos sus recursos y activos informáticos que garantice el cumplimiento de sus funciones y los requerimientos reguladores, operacionales y contractuales.

Este documento será aplicado a todo el Sistema de Gestión de la Seguridad de la Información de acuerdo a lo definido en su alcance y será de conocimiento público para todos los trabajadores.

PROPÓSITO, ALCANCE Y USUARIOS

Los documentos de referencia son los siguientes:

- Estándar ISO/IEC 27001:2013, cláusulas 5.2 y 5.3.
- Documento del Alcance del Sistema de Gestión de la Seguridad de la Información.
- Documento de Metodología del Análisis, Evaluación y Tratamiento de Riesgos.
- Documento de Declaración de Aplicabilidad.

ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

Se implementa una estrategia y un marco de trabajo que gestione los riesgos a los que está expuesta la información, así como sus activos informáticos a través procedimientos y controles que permitan mantener y cumplir esta política de seguridad.

OBJETIVOS

En su compromiso de proteger la Confidencialidad, Integridad y Disponibilidad de la información, las Políticas de Seguridad de la Información tendrán los siguientes objetivos:

- Garantizar la Confidencialidad, Integridad y Disponibilidad de la información de los administrativos, entre otros usuarios, así como los datos catalogados como confidenciales, privados y sensitivos.
- Proponer políticas para prevenir el ingreso, modificación, robo y/o divulgación de la información de personas no autorizadas.
- Garantizar la continuidad, operación y prestación de servicios de la empresa en caso de incidentes mayores de seguridad.

- Motivar al personal en la seguridad de información con el fin de minimizar riesgos.

ALCANCE E IMPORTANCIA

El presente documento establece la Política de Seguridad de la información de la Empresa Agroindustrial Pomalca S.A.A. en pro de ayudar a conseguir los objetivos organizacionales.

5.4.1. Políticas de seguridad de los activos de la información

POLÍTICA DE SEGURIDAD GENERAL

Todos los directivos y trabajadores están en la obligación de mantener la información lo más segura posible. Se prohíbe la reproducción total o parcial de los documentos clasificados como confidenciales, sin la debida autorización o consentimiento del ente competente, así como el deterioro adrede de los dispositivos informáticos, software, cableado de datos, suministro eléctrico, o cualquier activo institucional.

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN GENERAL

Se emplean políticas y lineamientos de seguridad que fuerzan a mantener la información de clientes y administrativos en un entorno seguro. Estas políticas están dirigidas a mantener los principios de la Seguridad Informática como lo son la *Confidencialidad, Integridad y Disponibilidad*.

POLÍTICA DE LOS SERVICIOS ORGANIZACIONALES

Para el acceso a los servicios de los sistemas de información organizacionales, se solicita siempre las credenciales

de acceso obtenidas por la oficina de Sistemas y Cómputo de la Empresa Agroindustrial Pomalca S.A.A. Ésta es una cuenta personal única e intransferible. Si los datos de acceso son extraviados, se pueden recuperar a través del usuario del correo organizacional.

POLÍTICA DEL DESARROLLO DE APLICACIONES

Para el desarrollo de software de aplicación por grupos o proyectos de investigación organizacionales, se verifican que sean bajo las herramientas de desarrollo de software con los cuales la empresa mantiene contratos de licencia.

POLÍTICA DELA GESTIÓN DE RIESGO

Se emplean mecanismos de gestión de riesgos y controles necesarios para mantener el normal funcionamiento de los procesos.

POLÍTICA DE LA PROTECCIÓN DE DATOS

La oficina de Sistemas y Cómputo implementa un sistema de protección multiniveles a los datos e información que se almacena en las bases de datos de la empresa. También se emplean restricciones a nivel de usuario en base al rol y perfil.

POLÍTICA DE AUDITORIA

Para mantener la calidad de los procesos organizativos, se hacen auditorías programadas en cada una de las áreas y procesos críticos de la institución.

POLÍTICA DE CALIDAD

La oficina de Sistemas y Cómputo realiza controles y cambios en pro de mejorar continuamente sus procesos. Se

realizan evaluaciones periódicas para medir el nivel de calidad en áreas críticas y en otras donde sea necesario.

La calidad es un componente fundamental. Se cumplen con los requerimientos de gestión para el logro de certificaciones de estándares internacionales, así como la alineación con los sistemas de calidad existentes en la empresa.

POLÍTICA DE LOS DISPOSITIVOS TRAÍDOS POR EL USUARIO

Los trabajadores que prefieran trabajar con equipos de uso personal, deben estar previamente autorizados para hacerlo, el equipo se configura de acuerdo a los lineamientos de la organización y bajo las mismas condiciones que los equipos de la empresa, ya que no se aceptan riesgos como la propagación de software de código malicioso debido a una falla de seguridad en el equipo. Los dispositivos de uso personal proveen mecanismos de autenticación aprobados por la oficina de Sistemas y Cómputo.

POLÍTICA DE DISPOSITIVOS PORTABLES

La instalación de los dispositivos portables en los equipos de la empresa, son escaneados por el software antivirus contratado. No se permite su ejecución si se detecta el código malicioso y no es removido del dispositivo.

POLÍTICA DE LA CREACIÓN DE USUARIOS

Los usuarios acceden a los diferentes servicios utilizando un esquema de identificación único, personal e intransferible. Este es el usuario organizacional y se entrega en un período no máximo a las 24 horas desde el momento en el que el usuario tiene vínculo con la empresa.

POLÍTICA DE LA INSTALACIÓN DE SOFTWARE Y HARDWARE

Para la instalación del software y hardware, estos componentes son únicamente instalados por el personal técnico capacitado de la empresa. A cada equipo se le realiza un inventario de hardware y la información se mantiene en una base de datos. Se realiza un chequeo de este componente cada vez que se inicie el equipo y se conecte a la red; si se detectan cambios no autorizados, queda deshabilitado automáticamente.

POLÍTICA DE LA COMUNICACIÓN ORGANIZACIONAL

La información y comunicación organizacional es única y exclusivamente informada por medio de los correos electrónicos de la organización y no de los web comerciales. Se realiza un escaneo con software antivirus a los documentos adjuntos tanto subidos como recibidos.

5.4.2. Responsabilidad

Cada persona administrativa de la empresa es responsable de la seguridad de los activos informáticos que están a su disposición, y debe seguir los lineamientos estipulados en este documento de una manera satisfactoria y de acuerdo a las reglamentaciones contractuales.

El no actuar con responsabilidad frente a la Política de la Seguridad de la Información, es sancionado de acuerdo al código ético de la empresa.

5.4.3. Procedimientos en incidentes de seguridad

Si la persona administrativa detecta que ha sido violado un procedimiento referente a las Políticas de Seguridad establecidas en este documento, debe informarlo inmediatamente al líder de la

oficina de Sistemas y Cómputo mediante un documento formal reportando el incidente, posibles causas y fallas que podrían haberlo generado, así como las recomendaciones y/o controles para mitigarlo.

5.5. Metodología de análisis y evaluación de riesgo y reporte de evaluación de riesgo

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir la metodología de análisis y evaluación de riesgos y evaluar el reporte de evaluación de riesgos en la Empresa Agroindustrial Pomalca S.A.A., y definir cuáles son los riesgos que tienen mayor impacto en la empresa de acuerdo al estándar ISO/IEC 2001:2013.

El análisis de riesgos es aplicado a todo el alcance del Sistema de Gestión de la Seguridad de la Información incluyendo todos los activos inventariados que podrían tener un impacto en la seguridad de la información.

Los usuarios de este documento son todos aquellos trabajadores que intervienen en el proceso de análisis y evaluación de riesgos.

DOCUMENTOS DE REFERENCIA

- Estándar ISO/IEC 27001:2013, cláusulas 6.1.2, 6.1.3, 8.2, y 8.3.
- Políticas de la Seguridad de la Información.
- Declaración de Aplicabilidad.

5.5.1. Metodología MAGERIT

MAGERIT es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por el CSAE

(Consejo Superior de Administración Electrónica) que supone los beneficios evidentes de emplear las tecnologías de información, pero gestionando los riesgos inherentes a ella, donde actualmente está en su versión 3. (PAE: portal de administración electrónica, 2012)

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar al alcance de la misión de una organización de acuerdo a las Dimensiones de Seguridad propuestas:

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

Tabla N° 10. Dimensiones de seguridad para la Identificación y Valoración de Amenazas en MAGERIT.
Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

Para el proceso de Gestión del Riesgo, MAGERIT contempla dos grandes tareas a realizar: el Análisis de Riesgos y el Tratamiento de Riesgos. El Análisis de Riesgos pretende calificar los riesgos encontrados cuantificando sus consecuencias (análisis cuantitativo) o determinando su importancia relativa (análisis cualitativo). Este proceso de análisis conlleva la identificación de los activos, sus amenazas y los controles de seguridad propuestos, estimando así el impacto y el riesgo al que están expuestos cada uno de los activos y su repercusión en el nivel de seguridad de la información en una organización. Por su parte, el Tratamiento de Riesgos consta de las actividades que se ejecutan para modificar la situación o nivel de riesgo.

Como MAGERIT es una metodología sistemática, sigue una serie de pasos para realizar la Gestión del Riesgo, los cuales son los siguientes:

1. **Inventario de Activos:** Los activos son aquellos componentes o funcionalidades de un sistema de información que son susceptibles a ser atacados deliberada o intencionalmente con consecuencias para una organización. (Amutio Gómez, Candau, & Mañas, 2012). Son también los elementos que una organización posee para el tratamiento de la información. (Suárez & Amaya, 2013). MAGERIT clasifica los activos en los siguientes tipos:

TIPO DE ACTIVO	NOMENCLATURA	DEFINICIÓN
Activos Esenciales	[Essential]	Son aquellos que son esenciales para la supervivencia de la organización y que su carencia o daño afectaría directamente su existencia. Generalmente desarrollan misiones críticas.

Arquitectura del Sistema	[Arch]	Son aquellos que permiten estructurar el sistema, su arquitectura interna y sus relaciones con el exterior.
Datos/Información	[D]	Es aquella información que le permite a una organización prestar sus servicios.
Claves Criptográficas	[K]	Son aquellos que permiten cifrar la información. Incluye los algoritmos de encriptación.
Servicios	[S]	Son aquellos que satisfacen las necesidades de los usuarios.
Software/Aplicaciones Informáticas	[SW]	Son aquellos que procesan los datos y permiten brindar información para la prestación de servicios.
Hardware/Equipamiento Informático	[HW]	Son los medios físicos donde se depositan los datos y prestan directa o indirectamente un servicio.
Redes de comunicaciones	[COM]	Son los medios de transporte por donde viajan los datos.
Soportes de Información	[Media]	Son los dispositivos físicos que permiten el almacenamiento temporal o permanente de la información.
Equipamiento Auxiliar	[AUX]	Son aquellos equipos que brindan soporte a los sistemas de información sin estar relacionado

		con los datos.
Instalaciones	[L]	Son los lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	[P]	Son las personas relacionadas con los sistemas de información.

Tabla N° 11. Clasificación de los tipos de activos informáticos en MAGERIT
Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

2. **Valoración de Activos:** Los activos que generan valor son aquellos que se necesitan proteger, y cada activo tiene una importancia mayor o menor en la organización. MAGERIT establece dos tipos de valoraciones: Cualitativa que es aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización; y la Cuantitativa que estima el costo del activo (incluyendo costo de compra, de reparación, configuración, mantenimiento, etc.). Mientras que la Cualitativa permite establecer órdenes de magnitud (**MA** [*Muy Alto*], **A**[*Alto*], **M**[*Medio*], **B**[*Bajo*] y **MB**[*Muy Bajo*]) y no genera valores numéricos, la Cuantitativa sí permite calcular el costo y/o valor monetario.

3. **Identificación y Valoración de Amenazas:** MAGERIT establece cinco Dimensiones de Seguridad (**D**[*Disponibilidad*], **I**[*Integridad*], **C**[*Confidencialidad*], **A**[*Autenticidad*] y **T**[*Trazabilidad*]) donde es necesario determinar los criterios de valoración en cada dimensión. Estos valores y/o criterios son similares a los establecidos en la *tabla de Dimensiones de seguridad para la Identificación y Valoración de Amenazas en MAGERIT.*

3.1. Identificación de Amenazas: Las amenazas son los eventos que ocurren sobre un activo que podría causarle daño a una organización. MAGERIT emplea un catálogo de amenazas posibles sobre los activos de un sistema de información (Amutio Gómez, Candau, & Mañas, 2012), los cuales están clasificados de la siguiente manera:

TIPO DE AMENAZA	NOMENCLATURA	DEFINICIÓN
Desastres Naturales	[N]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	[I]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	[E]	Fallos no intencionales causados por las personas.
Ataques Intencionados	[A]	Fallos deliberados causados por las personas.

Tabla N° 12. Catálogo de Amenazas sobre los activos Informáticos en MAGERIT
Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

3.2. Valoración de Amenazas: Para establecer la valoración de las amenazas es necesario determinarla frecuencia o probabilidad de ocurrencia. En MAGERIT, las frecuencias o probabilidades se muestran a continuación (Suárez & Amaya, 2013):

PROBABILIDAD O FRECUENCIA	RANGO	VALOR
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50

Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Tabla N° 13. Probabilidad o Frecuencia de ocurrencia de las amenazas en MAGERIT
Fuente: (Suárez & Amaya, 2013)

3.3. Impacto Potencial: Se determina el nivel de daño o impacto que tendría un activo si se llegara a materializar una amenaza determinada en cada una de sus dimensiones de seguridad.

3.4. Riesgo Potencial: El riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Por ende, el riesgo es calculado como:

Riesgo = Probabilidad x Impacto.

El riesgo crece con el impacto y con la probabilidad como se muestra en la siguiente ilustración:

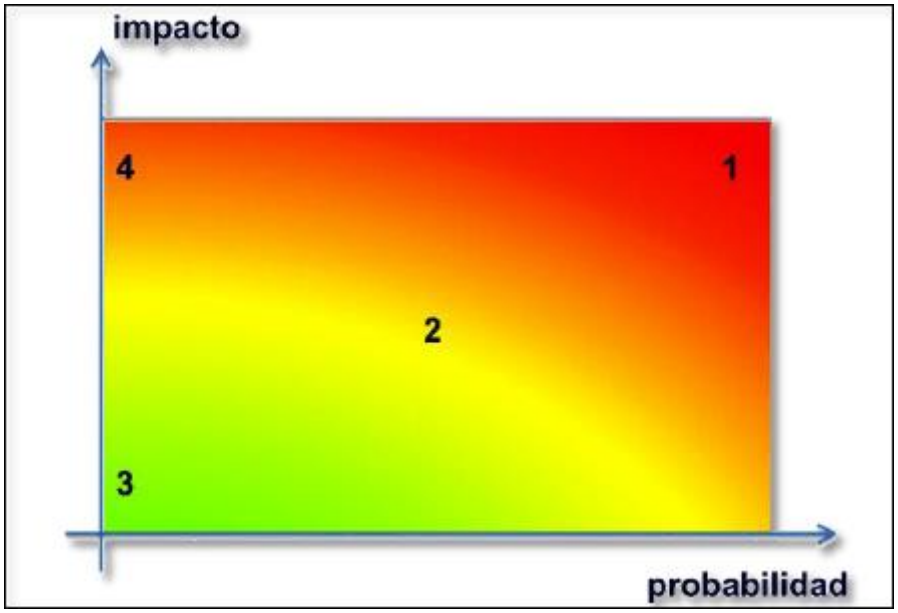


Figura N° 6: Zona de riesgos

Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

Donde las zonas identifican lo siguiente (Amutio Gómez, Candau, & Mañas, 2012):

- ***Zona 1***: Riesgos muy probables y de muy alto impacto (***MA: Críticos***).
- ***Zona 2***: Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables pero de impacto bajo o muy bajo (***M: Apreciables***).
- ***Zona 3***: Riesgos improbables y de bajo impacto (***MB, B: Despreciables o Bajos***).
- ***Zona 4***: Riesgos improbables pero de muy alto impacto (***A: Importantes***).

A su vez, la relación de la probabilidad e impacto para determinar el riesgo de forma cualitativa se muestra en la siguiente tabla:

RIESGO		**PROBABILIDAD**				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla N° 14. Estimación cualitativa del Riesgo en MAGERIT
Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

4. **Controles de Seguridad (Salvaguardas):** Los Controles de Seguridad o Salvaguardas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, donde se deben establecer los controles para cada amenaza de cada activo. Los salvaguardas propuestos en MAGERIT se clasifican en los siguientes (Amutio Gómez, Candau, & Mañas, 2012):

SALVAGUARDA	NOMENCLATURA
Protecciones generales u horizontales	H
Protección de los datos / información	D
Protección de las claves criptográficas	K
Protección de los servicios	S
Protección de las aplicaciones (software)	SW
Protección de los equipos (hardware)	HW
Protección de las comunicaciones	COM
Protección en los puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	MP
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	L
Salvaguardas relativas al personal	PS
Salvaguardas de tipo organizativo	G
Continuidad de operaciones	BC
Externalización	E
Adquisición y desarrollo	NEW

Tabla N° 15. Salvaguardas sobre los activos informáticos en MAGERIT
Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

5.5.2. Inventario y Clasificación de Activos Informáticos

Un activo o recurso informático está representado por los ***objetos físicos*** (hardware [*routers*, *switches*, *hubs*, *firewalls*, *antenas*, *computadoras*]), ***objetos abstractos*** (*software*, *sistemas de información*, *bases de datos*, *sistemas operativos*) e incluso el ***personal de trabajo*** y las ***instalaciones físicas***.

Los activos o recursos informáticos encontrados en la Empresa Agroindustrial Pomalca S.A.A. se encuentran clasificados según el Tipo de Activo en la metodología MAGERIT; en el Anexo N° 03 (Pág. 198).

- **VALORACIÓN DE LOS ACTIVOS DE ACUERDO AL IMPACTO**

Se determina la valoración de los activos de la Empresa Agroindustrial Pomalca S.A.A. de acuerdo al tipo ***Cualitativo*** que establece MAGERIT y el impacto que tiene en la organización, de acuerdo a la siguiente escala:

IMPACTO	NOMENCLATURA	VALOR	DESCRIPCIÓN
MUY ALTO	**MA**	**10**	El daño tiene consecuencias muy graves para la organización y podrían ser irreversibles.
ALTO	**A**	**7-9**	El daño tiene consecuencias muy graves para la organización.
MEDIO	**M**	**4-6**	El daño contiene consecuencias relevantes para la organización y su operación.
BAJO	**B**	**1-3**	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la organización.

MUY BAJO	**MB**	**0**	El daño no contiene consecuencias relevantes para la organización.

Tabla N° 16. Valoración cualitativa de los activos informáticos en MAGERIT
Fuente: (Suárez & Amaya, 2013)

La valoración de los activos de acuerdo al impacto de la Empresa Agroindustrial Pomalca S.A.A. se encuentra en el Anexo N° 04 (Pág. 205).

- **VALORACIÓN DE LOS ACTIVOS DE ACUERDO A LAS DIMENSIONES DE SEGURIDAD**

La valoración de los activos de acuerdo a las dimensiones de seguridad de la Empresa Agroindustrial Pomalca S.A.A. se encuentra en el Anexo N° 05 (Pág. 212).

- **IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS**

De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia.

La identificación y valoración de amenazas de la Empresa Agroindustrial Pomalca S.A.A. (basado en el Catálogo de Amenazas sobre los activos Informáticos en MAGERIT) se encuentra en el Anexo N° 06 (Pág. 224).

- **RIESGO POTENCIAL**

Se determina el nivel de riesgo potencial de cada uno de los activos en una valoración cualitativa de acuerdo a las zonas de riesgo que propone MAGERIT. El riesgo es calculado en base al impacto que tiene cada activo y según el tipo de amenaza general (Naturales, Industriales, Errores No Intencionados, Ataques Intencionados); es decir, no se calcula

en cada dimensión de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad). Sólo se toma en cuenta que ocurra cualquier amenaza dentro de su respectiva categoría y se escoge el peor de los casos.

El Riesgo Potencial de la Empresa Agroindustrial Pomalca S.A.A. (basado en el Catálogo de Amenazas sobre los activos Informáticos en MAGERIT) se encuentra en el Anexo N° 07 (Pág. 248).

En la Empresa Agroindustrial Pomalca S.A.A. la mayoría de los riesgos están clasificados en zonas de alto riesgo (A) y muy alto (MA) los cuales deberían ser tratados con la debida rigurosidad y control, y están asociados con el funcionamiento normal del hardware y de las redes de comunicaciones de datos, identificándose así que la disponibilidad del servicio de los dispositivos físicos es esencial para la operación efectiva de los procesos, porque de ellos también depende que el software pueda procesar la información y que los datos estén accesibles. En su mayoría, la amenaza de mayor probabilidad de ocurrencia sería la fluctuación en el servicio eléctrico.

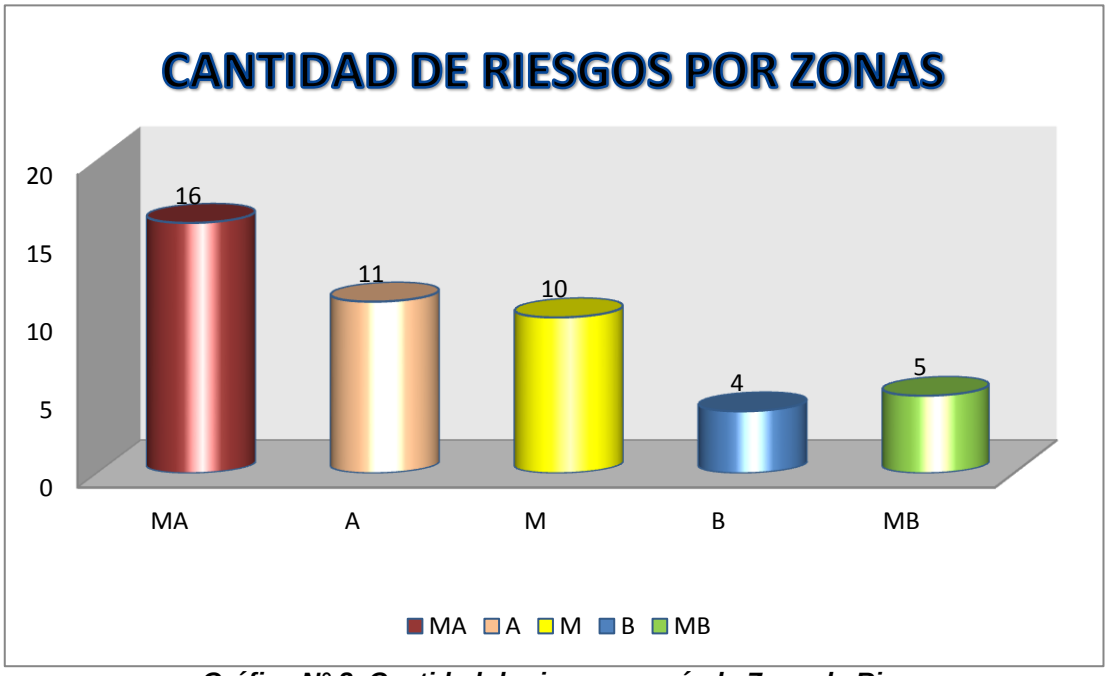
Otro riesgo importante a tener en consideración sería la posible filtración de información debido a una eventual interceptación no autorizada por violación de confidencialidad en los datos transmitidos, donde probablemente se deba a la falta de mecanismos de encriptación/cifrado en la comunicación en el acceso web a los diferentes servicios y software de uso organizacional.

Por otra parte, el software de uso ofimático y el hardware que no es de procesamiento de información se catalogan en una zona de riesgo baja debido a que tienen

muy bajo impacto en la operación de los procesos de la organización.

Por último, aunque las posibilidades de catástrofes ambientales o desastres naturales que afecten la instalación son mínimas debido a que la empresa no se encuentra en un lugar cercano a fuentes de agua o de temperaturas extremas; en la ciudad de Pomalca no se registran constantes movimientos telúricos o fuerzas naturales destructivas como huracanes, tornados o tsunamis, la falta de un personal constante de vigilancia, cámaras de control y sobretodo el constante acceso de personal no autorizado (personas particulares) podrían ocasionar serios daños voluntarios o involuntarios en el hardware o equipos auxiliares que podrían denegar el servicio por tiempo ilimitado.

Se puede verificar entonces que la mayoría de los riesgos están clasificados como críticos e importantes como lo muestra la siguiente gráfica:



Gráfica N° 3. Cantidad de riesgos según la Zona de Riesgos
Fuente: Elaboración propia

5.6. Declaración de Aplicabilidad

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir que controles serán los apropiados para ser implementados en la Empresa Agroindustrial Pomalca S.A.A., los objetivos de estos controles y su justificación.

Este documento incluye todos los controles listados en el Anexo A del estándar ISO/IEC 27001:2013. Los controles son aplicables a todo el alcance del Sistema de Gestión de la Seguridad de la Información.

DOCUMENTOS DE REFERENCIA

- Estándar ISO/IEC 27001:2013, cláusula 6.1.3.
- Documento de las Políticas de la Seguridad de la Información.
- Metodología de Análisis y Evaluación de Riesgos.

APLICABILIDAD DE CONTROLES

La aplicabilidad de controles para la Empresa Agroindustrial Pomalca S.A.A. (basado en el anexo A del estándar ISO/IEC 27001:2013) se encuentra en el Anexo N° 08 (Pág. 254).

5.7. Plan de Tratamiento de Riesgo

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir que controles de seguridad o salvaguardas de MAGERIT son los apropiados para enfrentar las amenazas de cada uno de los activos y mitigar los riesgos

en la Oficina de Sistemas y Cómputo de la Empresa Agroindustrial Pomalca S.A.A., así como definir el tratamiento de cada uno de ellos.

Este documento también determina cuáles controles de seguridad del Anexo A del estándar ISO/IEC 27001:2013 son aplicables a todo el alcance del Sistema de Gestión de la Seguridad de la Información.

DOCUMENTOS DE REFERENCIA

- Estándar ISO/IEC 27001:2013, cláusulas 8.2. y 8.3.
- Anexo A del estándar ISO/IEC 27001:2013.
- Estándar ISO/IEC 27002:2013.
- Documento de las Políticas de la Seguridad de la Información.
- Metodología de Análisis y Evaluación de Riesgos.

TRATAMIENTO DE RIESGOS

El tipo de tratamiento que se le dará a cada riesgo: ***Asumirlos (AS), Definir Controles (DC)*** o ***Transferirlos a Terceros (TT).***

APLICABILIDAD DE CONTROLES DE SEGURIDAD

Con el fin de alcanzar los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen controles de seguridad basados en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A del estándar ISO/IEC 27001:2013. (Ver Anexo N° 09) Pág. 272.

CAPÍTULO VI:
COSTOS Y BENEFICIOS

6.1. Análisis de costos

6.1.1. Costo de Personal

ÍTEM	DESCRIPCIÓN	COSTO (S/.)
1	Personal	1000
Total Costo de Personal		**1000**

6.1.2. Costo de Servicios y Materiales

ÍTEM	DESCRIPCIÓN	COSTO (S/.)
1	Consultoría Externa	1200
2	Servicio de Internet	400
3	Servicios Telefónicos	300
4	Energía Eléctrica	500
Total Costo de Servicios y Materiales		**2 400**

6.1.3. Costo de Hardware

ÍTEM	DESCRIPCIÓN	COSTO (S/.)
1	Laptop HP	3 200
2	Laptop Toshiba	2 900
3	Impresora Epson	250
Total Costo de Hardware		**6 350**

6.1.4. Costo de Mantenimiento

ÍTEM	DESCRIPCIÓN	COSTO (S/.)
1	Recargar tinta color negro	50
2	Recargar tinta de colores	50
Total Costo de Mantenimiento		**100**

6.1.5. Otros gastos

ÍTEM	DESCRIPCIÓN	COSTO (S/.)
1	Papelería (Documentación)	200
2	Alimentación	300
3	Traslado	650
Total Otros gastos		**1 150**

6.1.6. Resumen de costos

ÍTEM	DESCRIPCIÓN	COSTO (S/.)
1	Total Costo de Personal	1 000
2	Total Costo de Servicios y Materiales	2 400
3	Total Costo de Hardware	6 350

4	Total Costo de Mantenimiento	100
5	Total Otros Gastos	1 150
Costo Total		**11 000**

6.2. Beneficios

6.2.1. Beneficios Tangibles

- ✓ Mejora de productividad de los trabajadores.
- ✓ Generar confianza a los clientes por la garantía de confidencialidad comercial.
- ✓ Disponibilidad de la información.
- ✓ Reducción de inventarios.

6.2.2. Beneficios Intangibles

- ✓ Reduce la pérdida o robo de información.
- ✓ Diferencia en la competencia a nivel regional y/o nacional.
- ✓ Mejorará la seguridad, autenticidad, confiabilidad de la información ante algún incidente de seguridad.
- ✓ Confianza y reglas claras para los trabajadores de la organización.
- ✓ Fortalece los conocimientos de los trabajadores respecto a temas de seguridad de la información.

CAPÍTULO VII:
CONCLUSIONES

Este proyecto permitió conocer mediante la aplicación del estándar internacional de seguridad de la información ISO/IEC 27001:2013 que la Empresa Agroindustrial Pomalca S.A.A. no cumple con la mayoría de los Dominios, Objetivos de Control y Controles de Seguridad propuestos en la dicha norma. Esto se refleja en la carencia de documentación correspondiente al estándar ISO 27001; así como tampoco el empleo de los mecanismos de seguridad en la transmisión, tratamiento de información y datos relevantes para la empresa.

Para poder superar dichas deficiencias y que la Empresa Agroindustrial Pomalca S.A.A. pueda alcanzar sus objetivos organizacionales, se diseñaron las Políticas de Seguridad de la Información.

También, se pudieron clasificar los activos de información y determinar el nivel de riesgo potencial de cada uno de ellos aplicando la metodología de gestión de riesgos MAGERIT, donde se identificaron los activos más críticos que requieren de mayor atención y controles de seguridad dado el alto impacto que tienen en la prestación de servicios y funcionamiento óptimo de los procesos de la empresa.

Para finalizar, los sistemas de información juegan un papel fundamental en la prestación de servicios de las organizaciones, en el logro de objetivos e incluso sacan una ventaja competitiva. Sin embargo, el uso de la tecnología, en especial cuando la estructura cuenta con un alto nivel de complejidad conlleva riesgos desconocidos por la alta gerencia y no invertir en mecanismos de protección así como en la implementación de modelos de seguridad de la información puede poner en riesgo la eficiencia y garantía de los activos de información de las organizaciones; por lo que se desarrolló la Declaración de Aplicabilidad con el fin de proponer controles y así minimizar los riegos significativos y de alto impacto para el negocio de la Empresa Agroindustrial Pomalca S.A.A.

CAPÍTULO VIII:

RECOMENDACIONES

Capacitar de manera periódica al personal sobre las nuevas formas de seguridad de la información, de esta manera se lograría que los trabajadores de la Empresa Agroindustrial Pomalca S.A.A. estén más involucrados con el diseño de sistema de gestión de seguridad de la información planteado en el presente trabajo.

Establecer un área de seguridad de la información con sus respectivos responsables, de modo que se pueda distribuir el trabajo que requiere la clasificación e identificación de activos de la información para posteriormente gestionar los riesgos a los cuáles estos están expuestos.

Comprometer al personal de la empresa con las actividades que involucran la seguridad de la información, debido a que se debe revisar el desempeño de los trabajadores frente al sistema de gestión de seguridad para lograr los objetivos trazados por la organización.

Implementar el diseño de sistema de gestión de seguridad del presente trabajo para mejorar la confidencialidad, integridad y disponibilidad de la información.

Evaluar el nivel de cumplimiento de los controles propuestos en el presente trabajo basándose en la norma ISO 27001:2013 para evidenciar las mejoras obtenidas y las etapas no superadas.

CAPÍTULO IX:
REFERENCIAS BIBLIOGRÁFICAS

Bibliografía

KWELL - Empresa líder de servicios de seguridad y gestión de riesgos tecnologógicos. (2008). Recuperado el 9 de diciembre de 2015, de http://www.kwell.net/kwell/index.php?option=com_content&view=article&id=77&Itemid=274&lang=es

PAE: portal de administración electrónica. (2012). Recuperado el 15 de Marzo de 2016, de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vwvgs5zhBdg

Seguridad Informática. (18 de Agosto de 2012). Recuperado el 3 de Mayo de 2017, de http://msnseguridad.blogspot.pe/2012/08/seguridad-informatica-la-seguridad.html

Wikipedia. (2014). Recuperado el 10 de Febrero de 2016, de https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

Vanguardia Industrial. (2015). Recuperado el 2 de Febrero de 2016, de https://www.vanguardia-industrial.net/como-ganarte-la-confianza-de-tus-clientes/

Aguirre Cardona, J. D., & Aristizabal Betancourt, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Tesis Ing.* Universidad Tecnológica de Pereira, Colombia.

Alcántara Flores, J. C. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sitemas informáticos de la comisaría del norte P.N.P. en la ciudad de Chiclayo. Tesis Ing.* Chiclayo, Universidad Católica Santo Toribio de Mogrovejo, Perú.

Alexander, A. (2006). *Análisis del riesgo y el sistema de gestión de información: el enfoque ISO 27001:2005*. Recuperado el 15 de diciembre de 2015, de http://www.eficienciagerencial.com/

Alexander, A. (2007). *Diseño de un sistema de gestión de seguridad de la información.* Bogotá, Colombia: Ediciones Alfaomega.

Altagracia López, A. (2011). *Diseño de un plan de gestión de seguridad de la información. Caso: Dirección de informática de la alcaldía del municipio Jiménez del estado Lara. Tesis MgSc.* Barquisimeto, Venezuela.

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Barrantes Porras, C. E., & Hugo Herrera, J. R. (2012). *Diseño e implementación de un sistema de gestión de seguridad deinformación en procesos tecnológicos. Tesis Ing.* Lima, Universidad San Martin de Porres, Perú.

Buenaño Quintana, J. L., & Granda Luces, M. A. (2009). *Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 - 27002. Tesis Ing.* Guayaquil, Ecuador: Universidad Politécnica Salesiana.

Carrillo Sanchéz, J. (13 de Diciembre de 2013). *Enfoque UTE.* Recuperado el 5 de Marzo de 2016, de http://oaji.net/articles/2015/1783-1426290171.pdf

Collazos Balaguer, M. (2013). *La nueva versión ISO 27001:2013.* Lima.

Daltabuit, E., Hernández, L., Mallén, G., & Vázquez, J. (2007). *La seguridad de la información.* México: Ediciones Limusa.

De la Cruz Guerrero, C. W., & Vásquez Montenegro, J. C. (2008). *Elaboración y aplicación de un sistema de gestión de la seguridad de la información (SGSI) para la realidad tecnológica de la USAT. Tesis Ing.* Chiclayo, Universidad Católica Santo Toribio de Mogrovejo, Perú.

Doria Corcho, A. F. (2015). *Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de Córdoba.* Córdoba, Colombia.

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

Gonzáles Trejo, D. (30 de Agosto de 2013). *Magazcitum*. Recuperado el 28 de Marzo de 2016, de http://www.magazcitum.com.mx/?p=2397#.Vwvdv5zhBdh

Granada, C. (2009). *Gestión de seguridad de la información en el sector bancario. Especialización en gerencia de sistemas y tecnología.* Colombia.

Huerta, A. (30 de Marzo de 2012). *Security Artwork*. Recuperado el 1 de abril de 2017, de https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Huerta, A. (2 de Abril de 2012). *Security Artwork*. Recuperado el 1 de abril de 2017, de https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

ISO/IEC 27001 (Wikipedia). (s.f.). Recuperado el 20 de Marzo de 2016, de https://es.wikipedia.org/wiki/ISO/IEC_27001

Muñoz, J. (2004). *Metodología para la incorporación de medidas de seguridad en sistemas de información de gran implantación: confianza dinámica distribuida y regulación del nivel de servicio para sistemas y protocolos de internet. Tesis Dr.* Madrid, España: E.T.S.I. Telecomunicación (UPM).

(s.f.). *Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013.* BSI Group México, México D.F.

Puig, T. (2008). *Implantación de un sistema de gestión de seguridad*. Recuperado el 13 de diciembre de 2015, de http://www.mailxmail.com/curso-implantacion-sistema-gestion-seguridad

Quintero, I. (21 de Enero de 2015). *Prezi.* Recuperado el 1 de Marzo de 2016, de https://prezi.com/5qkvzofvin7l/cobit5/

Ríos Villafuente, J. (2014). *Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos. Tesis Ing.* Lima, Pontificia Universidad Católica del Perú, Perú.

Security, W. (16 de Junio de 2015). *Welive Security*. Recuperado el 18 de Marzo de 2018, de https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Soto, L. (2007). Recuperado el 10 de Diciembre de 2015, de http://mitecnologico.com/Main/ConceptoSistemaInformacion

Suárez, L., & Amaya, C. A. (2013). *Sistema de Gestión de la Seguridad de la Información.* Bogotá, Colombia: UNAD.

Talero Benitez, A. F. (2 de Marzo de 2015). *Prezi.* Recuperado el 1 de Marzo de 2016, de https://prezi.com/38p8cjhldc0n/metodologia-de-analisis-de-riesgo-octave/

Vittoriano, E. (2008). *La información como activo.* Santiago, Chile: Latin America CACS.

Zeña Ortíz, V. (2015). *Estándar internacional ISO 27001 para la gestión del seguridad de la información en la oficina central de informática de la UNPRG.* Lambayeque, Perú.

ANEXOS

ANEXO Nº 1

REQUISITOS DE LA NORMA ISO/IEC 27001:2013

CONTEXTO DE LA ORGANIZACIÓN

REQUISITO	CONTEXTO DE LA ORGANIZACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
4.1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	SI	Se tiene el conocimiento de la organización, su contexto, así como la comprensión de su misión, visión y objetivos estratégicos.	Implementar un Gobierno de Tecnología Informática que se ajuste a las necesidades de la organización y que esté acorde a los objetivos estratégicos, capacidades, recursos, sistemas de información y estructura organizacional.
4.2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	SI	Se tiene el conocimiento de las partes interesadas en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). La oficina de Sistemas y Cómputo y todas las unidades administrativas que dependen de su correcto funcionamiento para ejercer el desarrollo normal de sus procesos, así como los trabajadores para realizar sus labores.	Vincular a las unidades administrativas de más alto nivel (Directorio, Gerencia General, Oficina de Planeamiento y Desarrollo) en la implementación de un SGSI y los beneficios que genera para la empresa en general.

REQUISITO	CONTEXTO DE LA ORGANIZACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
4.3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SI	El SGSI se diseñará para la Empresa Agroindustrial Pomalca S.A.A. y las unidades de apoyo como lo son la oficina de Sistemas y Cómputo, la oficina de Planeamiento y Desarrollo y la oficina de Soporte Técnico.	Comunicar a los empleados (directores, jefes y operarios de sistemas) la importancia de un SGSI en la empresa y establecer un nivel de compromiso, liderazgo y concientización con las políticas de seguridad de la información que allí sean contenidas.
4.4	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	NO	Actualmente no se tiene implementado un SGSI.	Diseñar y/o planear un SGSI que mediante un proceso sistemático y mejoramiento continuo ayude a establecer los niveles de riesgos aceptables de la empresa. La recomendación es el estándar internacional ISO 27001:2013 aplicable a las organizaciones de cualquier tamaño y actividad.

LIDERAZGO

REQUISITO	LIDERAZGO	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
5.1	LIDERAZGO Y COMPROMISO	SI	El jefe de la oficina de Sistemas y Cómputo tiene conocimiento de la fase de diseño del SGSI, apoya la	Establecer una comunicación y liderazgo efectivo a los trabajadores sobre la importancia del SGSI

REQUISITO	LIDERAZGO	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
			investigación e incluso da su aval para una futura implementación y certificación en la norma, comprendiendo así la importancia y beneficios que genera para la empresa.	
5.2	POLÍTICA	NO	No se tiene una política de seguridad de la información documentada.	Implementar una política de seguridad de la información para la empresa y que sea públicamente accesible a todos los trabajadores para su conocimiento y aplicación.
5.3	ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	SI	Los roles y responsabilidades están asignadas.	Documentar los roles y responsabilidades en base a la seguridad de la información.

PLANIFICACIÓN

REQUISITO	PLANIFICACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
6.1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	--	--	--

REQUISITO	PLANIFICACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
6.1.1	GENERALIDADES	SI	Existen todas las condiciones para diseñar el SGSI. No existen riesgos a gran escala o implicaciones legales que impidan esta fase así como que eviten su mejoramiento continuo.	No aplica.
6.1.2	VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	NO	No existe una metodología claramente definida que clasifique, analice, evalúe y gestione los riesgos de la seguridad de la información.	Analizar las distintas metodologías de evaluación de riesgos y escoger la que mejor se adapte a las necesidades de la empresa.
6.1.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No se tiene una matriz de riesgos que pueda complementarse con los riesgos de seguridad de la Información.	Elaborar una matriz de riegos y determinar los controles necesarios para mitigar los riesgos encontrados en el análisis y documentar el plan de tratamiento para cada uno de ellos justificando su elección.
6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLO	NO	No están documentados los objetivos de la seguridad de la información.	Definir los objetivos de la seguridad de la información y establecer la forma de alcanzarlos comprometiendo a los empleados en su alcance y logro.

SOPORTE

REQUISITO	SOPORTE	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
7.1	RECURSOS	SI	Los recursos para esta fase de diseño y planeación están asignados.	Para un SGSI total, la empresa debe garantizar los recursos para la implementación, mantenimiento y mejoramiento durante todas sus fases contratando el personal calificado.
7.2	COMPETENCIA	SI	Se tiene la persona con el conocimiento necesario relativo para la fase de diseño y planeación del SGSI.	Contratar a personas certificadas en implementar un SGSI con la norma ISO 27001:2013.
7.3	TOMA DE CONCIENCIA	NO	Aunque existen acuerdos de confidencialidad y los trabajadores emplean algunas técnicas de seguridad informática, no existen las políticas de seguridad de la información a cumplir así como los objetivos.	Informar a los trabajadores de las diferentes áreas administrativas la importancia de la seguridad de la información y los beneficios que genera para la empresa e incluso de forma personal.
7.4	COMUNICACIÓN	NO	Aunque existen los medios para la comunicación organizacional efectiva, aún no se realiza para efectos de la seguridad de la información.	Aprovechar los medios de comunicación organizacional para distribuir información relevante a la seguridad.
7.5	INFORMACIÓN DOCUMENTADA	--	--	--
7.5.1	GENERALIDADES	NO	No se tiene la información	Redactar toda la información requerida

REQUISITO	SOPORTE	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
			documentada relevante a un SGSI y al estándar ISO 27001:2013.	por el estándar ISO 27001:2013.
7.5.2	CREACIÓN Y ACTUALIZACIÓN	NO	No se actualizan los documentos del SGSI ya que no hay uno implementado.	Actualizar los documentos del SGSI y del estándar ISO 27001:2013 cuando sea necesario incluyendo razones y autores.
7.5.3	CONTROL DE LA INFORMACIÓN DOCUMENTADA	NO	No existe un control de los documentos del SGSI ya que no hay uno implementado.	Mantener un control de los documentos del SGSI preservando su confidencialidad, integridad, disponibilidad y autenticidad, así como mantener el control de cambios en las actualizaciones.

OPERACIÓN

REQUISITO	OPERACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
8.1	PLANIFICACIÓN Y CONTROL OPERACIONAL	NO	No se tiene implementado un control de los procesos necesarios para alcanzar los objetivos de la seguridad de la información.	Establecer los procesos necesarios para planear, mantener y mejorar el SGSI.
8.2	VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA	NO	No existe una valoración de riesgos informáticos que permita determinar el	Establecer un esquema de clasificación de riesgos informáticos que permita analizarlos y valorarlos para determinar

REQUISITO	OPERACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
	INFORMACIÓN		nivel crítico o de riesgo aceptable.	los controles a implementar con el fin de mitigarlos.
8.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No existe un plan para el tratamiento de riesgos.	Proponer el plan de tratamiento de riesgos informáticos.

EVALUACION DEL DESEMPEÑO

REQUISITO	EVALUACIÓN DEL DESEMPEÑO	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	NO	No se tienen los métodos definidos así como tampoco los procesos y controles de seguridad que deben ser medidos, analizados y evaluados.	Establecer los métodos para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad del SGSI.
9.2	AUDITORIA INTERNA	NO	No está definido un plan de auditorías internas, así como tampoco los formatos para llevarla a cabo en relación a la seguridad de la información.	Proponer y mantener un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.
9.3	REVISIÓN POR LA DIRECCIÓN	NO	No está documentado un plan de la revisión del SGSI por parte del	Planear a intervalos regulares una revisión al SGSI de forma general y a las políticas de seguridad de la información

REQUISITO	EVALUACIÓN DEL DESEMPEÑO	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
			directorio.	con el fin de implementar las acciones correctivas pertinentes.

MEJORA

REQUISITO	MEJORA	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
10.1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS	NO	No está documentada la forma de cómo tratar a las no conformidades con el SGSI.	Determinar las causas de las no conformidades con el SGSI y proponer acciones correctivas identificando la vulnerabilidad.
10.2	MEJORA CONTINUA	NO	No se tiene el SGSI implementado.	Proponer un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.

ANEXO Nº 2

ANÁLISIS DIFERENCIAL REFERENTE AL ANEXO "A" DE LA NORMA ISO/IEC 27002:2013

<table>
<tr><td>A.5</td><td colspan="3">POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="3">Directrices establecidas por la dirección para la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td rowspan="6">A.5.1.1</td><td rowspan="6">Políticas para la seguridad de la información</td><td rowspan="6">Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las políticas de la seguridad de la información proveen un direccionamiento estratégico acorde a los requerimientos de la empresa y cumplimiento con leyes y regulaciones. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se tiene implementado un SGSI ni existe un documento que contemple las políticas de seguridad de la información.</td></tr>
</table>

<table>
<tr><td rowspan="6">A.5.1.2</td><td rowspan="6">Revisión de las políticas para seguridad de la información</td><td rowspan="6">Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las políticas de la seguridad de la información deberían ser evaluadas con el fin de responder a los cambios de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una revisión de las políticas de seguridad de la información ya que actualmente no se tiene el documento relacionado (ver A.5.1.1).</td></tr>
</table>

<table>
<tr><td>A.6</td><td colspan="3">ORGANIZACIÓN DE LASEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.6.1</td><td colspan="3">Organización interna</td></tr>
<tr><td colspan="4">Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.</td></tr>
<tr><td rowspan="3">A.6.1.1</td><td rowspan="3">Roles y responsabilidad es para la seguridad de información</td><td rowspan="3">Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los roles y responsabilidades son vitales para la protección de los activos informáticos individuales, así como los procesos</td></tr>
</table>

			específicos para la seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.
			IMPLEMENTA
			SI / **NO**
			Los roles y responsabilidades relativas a la seguridad de la información aún no están definidas, debido a que no se tiene implementado un SGSI.
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	**APLICA**
			SI / **NO**
			Ningún empleado debería tener acceso a modificar los activos informáticos sin autorización previa.
			IMPLEMENTA
			SI / **NO**
			El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.	**APLICA**
			SI / **NO**
			Deberían existir procedimientos para contactar a las autoridades

			pertinentes y reportar las incidencias relativas a la seguridad de la información.
			IMPLEMENTA
			SI / **NO**
			Las incidencias relativas a la seguridad de la información son resueltas internamente.
A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesional esespecializadas en seguridad.	**APLICA**
			SI / **NO**
			Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad de la información, así como las actualizaciones de los equipos y/o dispositivos.
			IMPLEMENTA
			SI / **NO**
			No se mantienen contactos con autoridades nacionales para los incidentes de seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	**APLICA**
			SI / **NO**
			Una metodología de análisis de riesgos debería ser parte del proceso de implementación de un proyecto de TI con el fin de

			direccionarlos y controlarlos.	
			IMPLEMENTA	
			SI	**NO**
			Los riesgos asociados a la seguridad de la información no son contemplados desde los inicios de los proyectos de TI.	
A.6.2	**Dispositivos móviles y Teletrabajo**			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.				
A.6.2.1	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	**APLICA**	
			SI	**NO**
			Los dispositivos móviles son un riesgo potencial para la seguridad de la información.	
			IMPLEMENTA	
			SI	**NO**
			No existe una política de seguridad para los dispositivos móviles.	
A.6.2.2	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para	**APLICA**	
			SI	**NO**

		proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	El teletrabajo debería tener una política de seguridad sobre las condiciones y restricciones.	
			IMPLEMENTA	
			SI	**NO**
			Aunque se permite el acceso a algunos dispositivos de forma remota, no se implementa el teletrabajo.	

A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	**Antes de asumir el empleo**			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían 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.	**APLICA**	
			SI	**NO**
			Aparte de las competencias técnicas, el personal contratado debería ser éticamente correcto y confiable especialmente si accede a información sensitiva de la organización.	
			IMPLEMENTA	
			SI	**NO**

<table>
<tr><td></td><td></td><td></td><td colspan="2">El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.</td></tr>
<tr><td rowspan="6">A.7.1.2</td><td rowspan="6">Términos y condiciones del empleo</td><td rowspan="6">Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los acuerdos contractuales de los empleados deberían tener cláusulas relativas a la confidencialidad de la información y respecto a las leyes y derechos de propiedad intelectual.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.</td></tr>
<tr><td>A.7.2</td><td colspan="4">Durante la ejecución del empleo</td></tr>
<tr><td colspan="5">Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
<tr><td rowspan="3">A.7.2.1</td><td rowspan="3">Responsabilidades de la dirección</td><td rowspan="3">Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La dirección debe asegurar que los roles y responsabilidades están claramente definidos antes de brindar acceso confidencial, así como los empleados estén comprometidos con</td></tr>
</table>

<table>
<tr><td></td><td></td><td>la organización.</td><td>las políticas de seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.
IMPLEMENTA
SI | NO
No se tiene implementado un SGSI y no existen políticas de la seguridad de la información.</td></tr>
<tr><td>A.7.2.2</td><td>Toma de conciencia, educación y formación en la seguridad de la información</td><td>Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.</td><td>APLICA
SI | NO
Mediante un programa de entrenamiento relativo a la seguridad de la información, los empleados son conscientes de su importancia y cómo pueden cumplir con las políticas del SGSI.
IMPLEMENTA
SI | NO
No se tiene implementado un SGSI ni un plan de concientización formal relativo a la seguridad de la información.</td></tr>
<tr><td>A.7.2.3</td><td>Proceso disciplinario</td><td>Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la</td><td>APLICA
SI | NO
Los procesos disciplinarios son analizados en base al grado de responsabilidad del empleado y el impacto que tiene en la</td></tr>
</table>

<table>
<tr><td></td><td></td><td>información.</td><td>organización.</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>Aunque no se tiene implementado un SGSI y no se tiene plan de concientización relativo a la seguridad de la información, el empleado está sujeto a un proceso disciplinario en caso de haber una incidencia.</td></tr>
<tr><td>A.7.3</td><td colspan="3">Terminación o cambio de empleo</td></tr>
<tr><td colspan="4">Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.</td></tr>
<tr><td rowspan="5">A.7.3.1</td><td rowspan="5">Terminación o cambio de responsabilidades de empleo</td><td rowspan="5">Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los acuerdos contractuales deberían plasmar el compromiso relativo a la confidencialidad de la información aún después de la terminación o cambio de empleo.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>Al terminar o cambiar de empleo no se notifica al empleado sobre la validez de sus responsabilidades y deberes relativos a la seguridad de la información.</td></tr>
</table>

<table>
<tr><td>A.8</td><td colspan="3">GESTIÓN DE ACTIVOS</td></tr>
<tr><td>A.8.1</td><td colspan="3">Responsabilidad por los activos</td></tr>
<tr><td colspan="4">Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.</td></tr>
<tr><td rowspan="6">A.8.1.1</td><td rowspan="6">Inventario de activos</td><td rowspan="6">Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El inventario y clasificación de activos permite identificar la importancia de cada uno de ellos y su impacto en la organización. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.</td></tr>
<tr><td rowspan="4">A.8.1.2</td><td rowspan="4">Propiedad de los activos</td><td rowspan="4">Control: Los activos mantenidos en el inventario deberían tener un propietario.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los propietarios son responsables del uso de los activos informáticos durante todo su ciclo de vida. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.</td></tr>
</table>

			IMPLEMENTA
			SI / **NO**
			No se especifican los propietarios de los activos informáticos inventariados.
A.8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	**APLICA**
			SI / **NO**
			Los empleados o contratistas son responsables del uso que le dan a los activos informáticos de la organización.
			IMPLEMENTA
			SI / **NO**
			No se especifican las reglas para el uso aceptable de los activos.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	**APLICA**
			SI / **NO**
			La devolución de activos debe ser formalizada y la información almacenada en los dispositivos personales transferida a la organización.
			IMPLEMENTA

			SI	**NO**
			Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.	
A.8.2	**Clasificación de la información**			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A.8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	**APLICA**	
			SI	**NO**
			La clasificación de la información es vital para determinar el grado y control de seguridad que debería tener. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.	
			IMPLEMENTA	
			SI	**NO**
			Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.	
A.8.2.2	Etiquetado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para	**APLICA**	
			SI	**NO**

<table>
<tr><td></td><td></td><td>el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.</td><td>El etiquetado de la información debe reflejar el esquema de clasificación adoptador por la organización (ver A.8.2.1).</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>Actualmente no existe procedimiento alguno para el etiquetado y/o clasificación de la información.</td></tr>
<tr><td rowspan="5">A.8.2.3</td><td rowspan="5">Manejo de activos</td><td rowspan="5">Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El acceso a los activos debería restringirse de acuerdo a su esquema de clasificación.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
Actualmente no existen procedimientos para el manejo de la información, ya que ésta no está clasificada (ver A.8.2.1).</td></tr>
<tr><td>A.8.3</td><td colspan="3">Manejo de los soportes de almacenamiento</td></tr>
<tr><td colspan="4">Objetivo: Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.</td></tr>
<tr><td>A.8.3.1</td><td>Gestión de medios</td><td>Control: Se deberían implementar</td><td>APLICA</td></tr>
</table>

	removibles	procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	**SI**	**NO**
			Los medios removibles podrían almacenar información confidencial y deberían tener el mismo tratamiento y esquema de clasificación que cualquier otro activo informático.	
			IMPLEMENTA	
			SI	**NO**
			Los medio removibles son protegidos, pero no cuentan con un nivel de clasificación de información ***(ver A.8.2.1)***.	
A.8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	**APLICA**	
			SI	**NO**
			Los medios removibles podrían almacenar información confidencial y deberían ser removidos almacenando copias de seguridad en lugares seguros y garantizar que su información no sea revocable o legible.	
			IMPLEMENTA	
			SI	**NO**
			Los medios removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.	
A.8.3.3	Transferencia de	Control: Los medios que	**APLICA**	

	medios físicos	contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	**SI**	**NO**
			Los medios transportados podrían tener información sensitiva.	
			IMPLEMENTA	
			SI	**NO**
			No se transportan activos informáticos.	

A.9	**CONTROL DE ACCESO**			
A.9.1	**Requisitos del negocio para control de acceso**			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A.9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**APLICA**	
			SI	**NO**
			El control de acceso físico y lógico con principios del menor privilegio permite tener un control sobre los riesgos de diseminación de información o acceso físico a los activos a personas no autorizadas.	
			IMPLEMENTA	
			SI	**NO**

<table>
<tr><td></td><td></td><td></td><td colspan="2">Aunque se mantienen controles físicos y lógicos que garantizan el acceso con menor privilegio, no está documentada en una política de seguridad de la información.</td></tr>
<tr><td rowspan="6">A.9.1.2</td><td rowspan="6">Política sobre el uso de los servicios de red</td><td rowspan="6">Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las redes y servicios de red proveen acceso a diferentes servicios dentro de la organización al personal autorizado.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El acceso a las redes está protegido a personas no autorizadas.</td></tr>
<tr><td>A.9.2</td><td colspan="3">Gestión de acceso de usuarios</td></tr>
<tr><td colspan="4">Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.</td></tr>
<tr><td rowspan="5">A.9.2.1</td><td rowspan="5">Registro y cancelación del registro de usuarios</td><td rowspan="5">Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los identificadores únicos de los empleados mantienen un registro de las acciones realizadas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">A los empleados no se les asigna un identificador único dentro de la organización.</td></tr>
<tr><td rowspan="6">A.9.2.2</td><td rowspan="6">Suministro de acceso de usuarios</td><td rowspan="6">Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso formal.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">A los empleados no se les asigna un identificador único dentro de la organización (ver A.9.2.1).</td></tr>
<tr><td rowspan="6">A.9.2.3</td><td rowspan="6">Gestión de derechos de acceso privilegiado</td><td rowspan="6">Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">A los empleados se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo.</td></tr>
</table>

<table>
<tr><td rowspan="6">A.9.2.4</td><td rowspan="6">Gestión de información de autenticación secreta de usuarios</td><td rowspan="6">Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La autenticación de los empleados en los sistemas debería mantenerse confidencial y secreta para evitar alteración y/o modificación de la información por parte de personas no autorizadas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La entrega de claves de acceso se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.</td></tr>
<tr><td rowspan="6">A.9.2.5</td><td rowspan="6">Revisión de los derechos de acceso de usuarios</td><td rowspan="6">Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los derechos de acceso verifican qué puede hacer un usuario sobre la información o sistemas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se realizan verificaciones regulares de los derechos de acceso a los sistemas.</td></tr>
</table>

<table>
<tr><td rowspan="6">A.9.2.6</td><td rowspan="6">Retiro o ajuste de los derechos de acceso</td><td rowspan="6">Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La remoción de los derechos de acceso permite que los empleados no sigan teniendo acceso a información o a los sistemas una vez terminado el contrato o cambio en el cargo.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe un proceso y/o documentación formal de remoción de los privilegios de acceso de los empleados que cambian el cargo o terminan contrato.</td></tr>
<tr><td>A.9.3</td><td colspan="4">Responsabilidades de los usuarios</td></tr>
<tr><td colspan="5">Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.</td></tr>
<tr><td rowspan="6">A.9.3.1</td><td rowspan="6">Uso de la información de autenticación secreta</td><td rowspan="6">Control: Se debería exigir a los usuarios que cumplan las prácticas dela organización para el uso de información de autenticación secreta.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La información confidencial debería ser accedida sólo por las personas autorizadas y para fines de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2"></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">La información de autenticación del empleado en los sistemas y acceso a información es confidencial.</td></tr>
<tr><td>A.9.4</td><td colspan="4">Control de acceso a sistemas y aplicaciones</td></tr>
<tr><td colspan="5">Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.</td></tr>
<tr><td rowspan="5">A.9.4.1</td><td rowspan="5">Restricción de acceso Información</td><td rowspan="5">Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El acceso a la información debe ser granular para evitar revelar información confidencial y evitar el acceso a personas no autorizadas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td rowspan="5">A.9.4.2</td><td rowspan="5">Procedimiento de ingreso seguro</td><td rowspan="5">Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El inicio de sesión seguro permite que una persona no autorizada tenga acceso a información privilegiada.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td colspan="2">Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del trabajador en la empresa.</td></tr>
</table>

			SI	**NO**
			Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.	
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	**APLICA**	
			SI	**NO**
			Los sistemas de gestión de contraseñas son un mecanismo fuerte de autenticación de usuarios y evita que sean adivinadas por ataques de fuerza bruta y/o diccionario.	
			IMPLEMENTA	
			SI	**NO**
			Los sistemas de gestión de contraseñas no son interactivos ya que es otorgada de forma manual.	
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	**APLICA**	
			SI	**NO**
			Los programas utilitarios deben ser instalados cuidadosamente para que no afecten a los sistemas o a la información existente.	
			IMPLEMENTA	
			SI	**NO**

<table>
<tr><td></td><td></td><td></td><td colspan="2">Los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados.</td></tr>
<tr><td rowspan="6">A.9.4.5</td><td rowspan="6">Control de acceso a códigos fuente de programas</td><td rowspan="6">Control: Se debería restringir el acceso a los códigos fuente de los programas.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El código fuente contiene la información de cómo se ha implementado el programa y bajo que lenguaje de programación, así como las librerías empleadas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El código fuente sólo es accedido por las personas autorizadas.</td></tr>
</table>

<table>
<tr><td>A.10</td><td colspan="4">CRIPTOGRAFÍA</td></tr>
<tr><td>A.10.1</td><td colspan="4">Controles criptográficos</td></tr>
<tr><td colspan="5">Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.</td></tr>
<tr><td rowspan="3">A.10.1.1</td><td rowspan="3">Política sobre el uso de controles criptográficos</td><td rowspan="3">Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La criptografía cifra mediante algoritmos de encriptación los</td></tr>
</table>

<table>
<tr><td></td><td></td><td>información.</td><td>mensajes transmitidos garantizando la confidencialidad, integridad y autenticidad de los mensajes, impidiendo así que sea legible por personas no autorizadas.</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>No existe una política sobre el uso de algoritmos de encriptación para el cifrado de la información transmitida.</td></tr>
<tr><td rowspan="6">A.10.1.2</td><td rowspan="6">Gestión de llaves</td><td rowspan="6">Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>La gestión de llaves criptográficas vela por su seguridad, mantenimiento, renovación, distribución y destrucción.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>No existe una política sobre el uso y distribución de llaves criptográficas (ver A.10.1.1).</td></tr>
</table>

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO
A.11.1	**Áreas seguras**

<table>
<tr><td colspan="4">Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.</td></tr>
<tr><td rowspan="6">A.11.1.1</td><td rowspan="6">Perímetro de seguridad física</td><td rowspan="6">Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El perímetro de seguridad física impide el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Existe un perímetro físico, así como personal de seguridad.</td></tr>
<tr><td rowspan="6">A.11.1.2</td><td rowspan="6">Controles físicos de entrada</td><td rowspan="6">Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los controles de accesos físicos impiden el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El acceso físico sólo está controlado por medio del personal de seguridad.</td></tr>
</table>

<table>
<tr><td rowspan="7">A.11.1.3</td><td rowspan="7">Seguridad de oficinas, recintos e instalaciones</td><td rowspan="7">Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las oficinas y lugares de trabajo claves deberían estar protegidas impidiendo el acceso físico a personas no autorizadas así como no ser públicamente visibles</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las oficinas y lugares de trabajo están protegidas por medios físicos para controlar el acceso.</td></tr>
<tr><td rowspan="7">A.11.1.4</td><td rowspan="7">Protección contra amenazas externas y ambientales</td><td rowspan="7">Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Protección física contra los desastres naturales y/o humanos.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una protección física contra los desastres naturales y/o humanos.</td></tr>
<tr><td rowspan="3">A.11.1.5</td><td rowspan="3">Trabajo en áreas seguras</td><td rowspan="3">Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2"></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">Las áreas seguras deben estar físicamente aseguradas y revisadas periódicamente.</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI</td><td>NO</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">No se tienen áreas seguras para ser aseguradas físicamente.</td></tr>
<tr><td rowspan="5">A.11.1.6</td><td rowspan="5">Áreas de despacho y carga</td><td rowspan="5">Control: Se deberían 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.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los lugares de entrega de equipos y otros dispositivos están controlados y se restringe el acceso a áreas externas de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="3"></td><td colspan="2">El lugar de entrega de equipos y otros dispositivos ocurre al interior de la oficina.</td></tr>
<tr><td>A.11.2</td><td colspan="4">Controles físicos de entrada</td></tr>
<tr><td colspan="5">Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.</td></tr>
<tr><td>A.11.2.1</td><td>Ubicación y</td><td>Control: Los equipos deberían</td><td colspan="2">APLICA</td></tr>
</table>

	protección de los equipos	estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	**SI**	**NO**
			Los equipos deberían estar protegidos físicamente de amenazas ambientales (fuego, incendio, agua, humo) y humanas así como evitar el acceso no autorizado.	
			IMPLEMENTA	
			SI	**NO**
			Los equipos no están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc.	
A.11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	**APLICA**	
			SI	**NO**
			Los servicios de suministros como energía, agua, ventilación y gas deberían estar acordes a la manufacturación de los equipos.	
			IMPLEMENTA	
			SI	**NO**
			Los servicios de suministros como energía, agua, ventilación y gas están acordes a la manufacturación de los equipos.	
A.11.2.3	Seguridad del cableado	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o soporta	**APLICA**	
			SI	**NO**

		servicios de información debería estar protegido contra interceptación, interferencia o daño.	El cableado provee la transmisión de datos o energía a los dispositivos.
			IMPLEMENTA
			SI / **NO**
			El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	**APLICA**
			SI / **NO**
			El mantenimiento de los equipos garantiza su óptimo funcionamiento y rendimiento.
			IMPLEMENTA
			SI / **NO**
			Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.
A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	**APLICA**
			SI / **NO**
			El retiro de los equipos, eliminación de software e información sólo debería ser realizada por el personal autorizado.

			IMPLEMENTA
			SI / **NO**
			El retiro de los equipos, eliminación de software e información sólo es realizada por el personal autorizado.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían 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.	**APLICA**
			SI / **NO**
			Los equipos y/o dispositivos que pertenecen a la organización deberían ser gestionados sólo por el personal autorizado, así como tampoco ser utilizado en lugares públicos.
			IMPLEMENTA
			SI / **NO**
			Los equipos sólo son utilizados dentro de las instalaciones físicas de la organización.
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o	**APLICA**
			SI / **NO**
			Para la disposición o reutilización de equipos se debería tener un procedimiento que garantice la destrucción total de la información contenida con el fin de evitar de ser leída por personas no autorizadas.

		reutilización.	**IMPLEMENTA**
			SI / **NO**
			Se realiza un procedimiento seguro para la disposición o reutilización de equipos.
A.11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	**APLICA**
			SI / **NO**
			Los usuarios deberían cerrar sesiones y proteger el equipo con contraseñas fuertes cuando no lo estén utilizando ya que podría estar expuesto a acceso no autorizado.
			IMPLEMENTA
			SI / **NO**
			Aunque no exista una política documentada, los usuarios son conscientes y aplican la seguridad apropiada cuando el equipo está en desuso.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería 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.	**APLICA**
			SI / **NO**
			El almacenamiento de información confidencial no debería ser visible al público.
			IMPLEMENTA

			SI	**NO**
			La información confidencial es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.	

A.12	**SEGURIDAD DE LASOPERACIONES**			
A.12.1	**Procedimientos operacionales y responsabilidades**			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	**APLICA**	
			SI	**NO**
			Los procedimientos operacionales deberían estar documentados y disponibles para todos los usuarios. Estos procedimientos incluyen las copias de seguridad, almacenamiento, manejo de errores, encendido/apagado de equipos, instalación/configuración de sistemas, etc. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.	
			IMPLEMENTA	
			SI	**NO**
			Los procedimientos operacionales no están documentados, ya	

<table>
<tr><td></td><td></td><td></td><td colspan="2">que no existe aún una implementación de un SGSI.</td></tr>
<tr><td rowspan="6">A.12.1.2</td><td rowspan="6">Gestión de cambios</td><td rowspan="6">Control: Se deberían 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.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los cambios en los equipos que afectan la seguridad de la información deberían ser controlados y debidamente planeados y probados.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.</td></tr>
<tr><td rowspan="6">A.12.1.3</td><td rowspan="6">Gestión de capacidad</td><td rowspan="6">Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los recursos deberían ser monitoreados con el fin de gestionar su capacidad y rendimiento, así como proyectar que responda a las necesidades de la organización a largo plazo.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se les realiza un monitoreo continuo a los recursos y la adquisición de nuevos se proyecta de acuerdo a las</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">necesidades críticas de la organización.</td></tr>
<tr><td rowspan="6">A.12.1.4</td><td rowspan="6">Separación de los ambientes de desarrollo, pruebas y operación</td><td rowspan="6">Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La separación de ambientes de desarrollo y pruebas reduce el riesgo de operaciones no autorizadas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los ambientes de desarrollo y prueban están separados.</td></tr>
<tr><td>A.12.2</td><td colspan="4">Protección contra códigos maliciosos</td></tr>
<tr><td colspan="5">Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</td></tr>
<tr><td rowspan="4">A.12.2.1</td><td rowspan="4">Controles contra códigos maliciosos</td><td rowspan="4">Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El malware o software malicioso es un riesgo potencial para los sistemas y equipos, ya que pueden hacer que los sistemas operen de forma ineficiente, captura ilegal de información confidencial y borrado total.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
</table>

			SI	**NO**
			Aunque no existe una política claramente definida contra el malware, los usuarios son conscientes de los efectos nefastos que éstos podrían tener sobre el sistema y/o información. Pero muchos equipos no se mantienen actualizados con algún software antimalware y/o antivirus licenciado.	
A.12.3	**Copias de respaldo**			
Objetivo: Proteger contra la pérdida de datos.				
A.12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	**APLICA**	
			SI	**NO**
			Las copias de seguridad (backups) e imágenes de los sistemas garantizan que la información esencial e instalación de software podría ser recuperada después de fallas o desastres.	
			IMPLEMENTA	
			SI	**NO**
			Las copias de seguridad se realizan a intervalos programados de forma manual, sólo por el personal autorizado.	
A.12.4	**Registro y seguimiento**			
Objetivo: Registrar eventos y generar evidencia.				

A.12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	**APLICA**	
			SI	**NO**
			Los registros (logs) almacenan información relevante sobre los eventos ocurridos en la operación de un sistema.	
			IMPLEMENTA	
			SI	**NO**
			Se mantienen los registros de los eventos ocurridos en los sistemas.	
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	**APLICA**	
			SI	**NO**
			Los registros de eventos deberían ser custodiados para prevenir modificación no autorizada.	
			IMPLEMENTA	
			SI	**NO**
			Los registros de eventos están protegidos contra el acceso no autorizado.	
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y	**APLICA**	
			SI	**NO**

<table>
<tr><td></td><td></td><td>los registros se deberían proteger y revisar con regularidad.</td><td colspan="2">Los administradores tienen accesos privilegiados y podrían modificar información de los registros de eventos.</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI</td><td>NO</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.</td></tr>
<tr><td rowspan="6">A.12.4.4</td><td rowspan="6">Sincronización de relojes</td><td rowspan="6">Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La sincronización de los relojes de los sistemas permite mantener una referencia única de tiempo y zona horaria.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Aunque no existe una política documentada sobre la sincronización de los relojes, todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria.</td></tr>
<tr><td>A.12.5</td><td colspan="4">Control de software operacional</td></tr>
<tr><td colspan="5">Objetivo: Asegurar la integridad de los sistemas operacionales.</td></tr>
<tr><td>A.12.5.1</td><td>Instalación de</td><td>Control: Se deberían implementar</td><td colspan="2">APLICA</td></tr>
</table>

	software en sistemas operativos	procedimientos para controlar la instalación de software en sistemas operativos.	**SI**	**NO**
			Se debería controlar las instalaciones de software en los sistemas operativos.	
			IMPLEMENTA	
			SI	**NO**
			No existe una política documentada o procedimientos sobre la instalación de software en los sistemas operativos.	
A.12.6	**Gestión de la vulnerabilidad técnica**			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.				
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería 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.	**APLICA**	
			SI	**NO**
			El inventario de los activos se debería mantener actualizado con el fin de identificar a tiempo los riesgos asociados a las vulnerabilidades y amenazas técnicas.	
			IMPLEMENTA	
			SI	**NO**
			Aunque existe un inventario de los activos físicos y del software operacional, no se tiene una metodología de riesgos que los evalúe.	

<table>
<tr><td rowspan="6">A.12.6.2</td><td rowspan="6">Restricciones sobre la instalación de software</td><td rowspan="6">Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Cualquier persona con elevados privilegios de acceso podría instalar cualquier software en un equipo y/o dispositivo. El no control podría liderar a la instalación de software malicioso o no permitido.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Algunos trabajadores se aprovechan de los privilegios con los que cuentan para instalar cualquier software en su equipo asignado, trayendo consigo la posibilidad de algún software malicioso</td></tr>
<tr><td>A.12.7</td><td colspan="3">Consideraciones sobre auditorias de sistemas de información</td></tr>
<tr><td colspan="4">Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.</td></tr>
<tr><td rowspan="4">A.12.7.1</td><td rowspan="4">Información controles de auditoría de sistemas</td><td rowspan="4">Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las auditorías de los sistemas deberían ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
</table>

			SI	**NO**
			No se tiene un plan de auditoría para la verificación de los sistemas operativos.	

A.13	**SEGURIDAD DE LAS COMUNICACIONES**			
A.13.1	**Gestión de la seguridad de las redes**			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A.13.1.1	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	**APLICA**	
			SI	**NO**
			Las redes deberían proteger la transmisión de la información garantizando su confidencialidad e integridad y en algunos casos su disponibilidad.	
			IMPLEMENTA	
			SI	**NO**
			No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura.	
A.13.1.2	Seguridad de los	Control: Se deberían identificar	**APLICA**	

	servicios de red	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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	**SI**	**NO**
			El acceso a la red de los proveedores de servicios de red debería ser controlado y monitoreado.	
			IMPLEMENTA	
			SI	**NO**
			El acceso a la red de los proveedores de servicios de red es controlado y monitoreado.	
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	**APLICA**	
			SI	**NO**
			Los usuarios y servicios deberían estar separados lógicamente en unidades organizacionales o dominios, o a través de VLANS.	
			IMPLEMENTA	
			SI	**NO**
			Los usuarios y servicios están separados a través de dominios y VLANS.	
A.13.2	**Transferencia de información**			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Políticas y	Control: Se debería contar con	**APLICA**	

	procedimientos de transferencia de información	políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	**SI**	**NO**
			Los procedimientos y controles ayudan a mantener la seguridad de la información cuando es transferida a otra entidad.	
			IMPLEMENTA	
			SI	**NO**
			No existe una documentación sobre los procedimientos y controles a implementar para la transferencia segura de la información.	
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	**APLICA**	
			SI	**NO**
			Se deberían tener acuerdos sobre los procedimientos para la transferencia segura de la información.	
			IMPLEMENTA	
			SI	**NO**
			No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.	
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería	**APLICA**	
			SI	**NO**

<table>
<tr><td></td><td></td><td>electrónica.</td><td>Se deberían proteger los mensajes enviados internamente de los empleados de la organización.</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.</td></tr>
<tr><td rowspan="6">A.13.2.4</td><td rowspan="6">Acuerdos de confidencialidad o de no divulgación</td><td rowspan="6">Control: Se deberían 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.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los acuerdos con los empleados o con entes externos deberían tener acuerdos de confidencialidad de la información.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información.</td></tr>
</table>

A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS
A.14.1	**Requisitos de seguridad de los sistemas de información**

<table>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.</td></tr>
<tr><td rowspan="6">A.14.1.1</td><td rowspan="6">Análisis y especificación de requisitos de seguridad de la información</td><td rowspan="6">Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los requerimientos de la seguridad de la información deberían ser identificados utilizando varios métodos en concordancia con las políticas y regulaciones.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una política de seguridad de información que ayude a determinar la adquisición de los nuevos sistemas de información.</td></tr>
<tr><td rowspan="6">A.14.1.2</td><td rowspan="6">Seguridad de servicios de las aplicaciones en redes publicas</td><td rowspan="6">Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura (Ver A.13.1.1).</td></tr>
<tr><td rowspan="6">A.14.1.3</td><td rowspan="6">Protección de transacciones de los servicios de las aplicaciones</td><td rowspan="6">Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura (Ver A.13.1.1).</td></tr>
<tr><td>A.14.2</td><td colspan="4">Seguridad en los procesos de desarrollo y soporte</td></tr>
<tr><td colspan="5">Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.</td></tr>
<tr><td rowspan="3">A.14.2.1</td><td rowspan="3">Política de desarrollo seguro</td><td rowspan="3">Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las políticas y controles de seguridad deberían ser aplicados en el desarrollo de software.</td></tr>
</table>

			IMPLEMENTA	
			SI	**NO**
			Las políticas y controles de seguridad son aplicados en el desarrollo de software.	
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	**APLICA**	
			SI	**NO**
			El procedimiento formal de los cambios en el desarrollo de software debería ser documentado para garantizar la integridad del sistema o aplicación.	
			IMPLEMENTA	
			SI	**NO**
			El procedimiento formal de los cambios en el desarrollo de software es documentado para garantizar la integridad del sistema o aplicación.	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la	**APLICA**	
			SI	**NO**
			Los cambios en las aplicaciones deberían ser revisados y probados antes de implementarlas de manera que se garantice que no comprometa la seguridad.	

<table>
<tr><td></td><td></td><td>organización.</td><td colspan="2">IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI</td><td>NO</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Las aplicaciones y plataformas de operación son revisadas y probadas antes de implementarse.</td></tr>
<tr><td rowspan="5">A.14.2.4</td><td rowspan="5">Restricciones en los cambios a los paquetes de software</td><td rowspan="5">Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Limitar las modificaciones de software sólo a lo estrictamente necesario.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Las modificaciones de software sólo se hacen a lo estrictamente necesario.</td></tr>
<tr><td rowspan="5">A.14.2.5</td><td rowspan="5">Principios de construcción de sistemas seguros</td><td rowspan="5">Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían establecer y documentar los principios de desarrollo de software seguro.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">Se establecen y documentan los principios de desarrollo de software seguro.</td></tr>
<tr><td rowspan="6">A.14.2.6</td><td rowspan="6">Ambiente de desarrollo seguro</td><td rowspan="6">Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los ambientes de desarrollo de software también deberían estar protegidos de acceso no autorizado o de ejecución de software malicioso.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los ambientes de desarrollo de software están protegidos de acceso no autorizado o de ejecución de software malicioso.</td></tr>
<tr><td rowspan="6">A.14.2.7</td><td rowspan="6">Desarrollo contratado externamente</td><td rowspan="6">Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El software desarrollado externamente debería tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se desarrolla software externamente.</td></tr>
</table>

<table>
<tr><td rowspan="7">A.14.2.8</td><td rowspan="7">Pruebas de seguridad de sistemas</td><td rowspan="7">Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían realizar visitas y pruebas de seguridad al software que se está desarrollando.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se realizan pruebas de seguridad al software durante su período de desarrollo.</td></tr>
<tr><td rowspan="7">A.14.2.9</td><td rowspan="7">Prueba de aceptación de sistemas</td><td rowspan="7">Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se realizan las pruebas de seguridad debido a que aún no existen los lineamientos o políticas de la seguridad de la información.</td></tr>
<tr><td>A.14.3</td><td colspan="3">Datos de prueba</td></tr>
</table>

<table>
<tr><td colspan="5">Objetivo: Asegurar la protección de los datos usados para pruebas.</td></tr>
<tr><td rowspan="6">A.14.3.1</td><td rowspan="6">Protección de datos de prueba</td><td rowspan="6">Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los datos de prueba deberían ser seleccionados cuidadosamente y que no contengan ninguna información confidencial.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.</td></tr>
</table>

<table>
<tr><td>A.15</td><td colspan="4">RELACIÓN CON LOSPROVEEDORES</td></tr>
<tr><td>A.15.1</td><td colspan="4">Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="5">Objetivo: Asegurar la protección de los activos de la organización quesean accesibles a los proveedores.</td></tr>
<tr><td rowspan="3">A.15.1.1</td><td rowspan="3">Política de seguridad de la información para las relaciones con</td><td rowspan="3">Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La organización debería emplear los controles y procedimientos</td></tr>
</table>

<table>
<tr><td></td><td>proveedores</td><td>deberían acordar con estos y se deberían documentar</td><td>de seguridad para el acceso a los activos por parte de los proveedores.</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>No se tiene una política de seguridad definida.</td></tr>
<tr><td rowspan="5">A.15.1.2</td><td rowspan="5">Tratamiento de la seguridad dentro de los acuerdos con proveedores</td><td rowspan="5">Control: Se deberían 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.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.</td></tr>
<tr><td rowspan="3">A.15.1.3</td><td rowspan="3">Cadena de suministro de tecnología de información y comunicación</td><td rowspan="3">Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los suministros de los proveedores deberían estar acordes a las políticas de seguridad de la información de la organización.</td></tr>
</table>

		servicios de tecnología de información y comunicación.	**IMPLEMENTA**
			SI / **NO**
			No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.
A.15.2	**Gestión de la prestación deservicios con los proveedores**		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con lo sproveedores.			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	**APLICA**
			SI / **NO**
			El monitoreo y acceso de los proveedores debería ser acorde las políticas de seguridad de la organización.
			IMPLEMENTA
			SI / **NO**
			No existe una política de seguridad de la información y procedimientos.
A.15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los	**APLICA**
			SI / **NO**

<table>
<tr><td rowspan="5"></td><td rowspan="5"></td><td rowspan="5">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 involucrados, y la revaloración de los riesgos.</td><td colspan="2">Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una política de seguridad de la información y procedimientos.</td></tr>
</table>

<table>
<tr><td>A.16</td><td colspan="4">GESTIÓN DE INCIDENTES DESEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.16.1</td><td colspan="4">Gestión de incidentes y mejoras en la seguridad de la información</td></tr>
<tr><td colspan="5">Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.</td></tr>
<tr><td rowspan="4">A.16.1.1</td><td rowspan="4">Responsabilidad y procedimientos</td><td rowspan="4">Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los planes y procedimientos para gestionar los incidentes relacionados a la seguridad de la información deberían estar documentados.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
</table>

			SI	**NO**
			No existen los procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.	
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	**APLICA**	
			SI	**NO**
			Todos los empleados deben estar pendientes de los eventos y reportes de seguridad de la información.	
			IMPLEMENTA	
			SI	**NO**
			Los empleados están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información.	
A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	**APLICA**	
			SI	**NO**
			Se deberían implementar mecanismos de reportes de incidentes de seguridad de la información en donde todos los empleados deberían reportar las brechas de seguridad con el fin de prevenir incidentes.	
			IMPLEMENTA	
			SI	**NO**

<table>
<tr><td></td><td></td><td></td><td colspan="2">Los empleados están comprometidos en reportar las brechas lo antes posible.</td></tr>
<tr><td rowspan="6">A.16.1.4</td><td rowspan="6">Evaluación de eventos de seguridad de la información y decisiones sobre ellos</td><td rowspan="6">Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La clasificación y priorización de los incidentes de seguridad ayudan a identificar el impacto en la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los activos no están clasificados y no existe una metodología de análisis y evaluación de riesgos informáticos.</td></tr>
<tr><td rowspan="6">A.16.1.5</td><td rowspan="6">Respuesta a incidentes de seguridad de la información</td><td rowspan="6">Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Deberían existir procedimientos documentados para dar respuesta a los incidentes restableciendo la operación al nivel de seguridad aceptable lo más pronto posible.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Aunque las respuestas son inmediatas, los procedimientos de respuesta no están documentados.</td></tr>
</table>

<table>
<tr><td rowspan="6">A.16.1.6</td><td rowspan="6">Aprendizaje obtenido de los incidentes de seguridad de la información</td><td rowspan="6">Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se debería recolectar información de los incidentes ocurridos con el fin de prevenirlos en el futuro.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se recolecta la información de los incidentes y se aplican los controles necesarios para prevenirlos.</td></tr>
<tr><td rowspan="6">A.16.1.7</td><td rowspan="6">Recolección de evidencia</td><td rowspan="6">Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían recolectar las evidencias y registros para tomar acciones legales.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las evidencias son recolectadas formalmente para emprender las acciones legales.</td></tr>
</table>

<table>
<tr><td>A.17</td><td colspan="3">ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO</td></tr>
<tr><td>A.17.1</td><td colspan="3">Continuidad de seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.</td></tr>
<tr><td rowspan="6">A.17.1.1</td><td rowspan="6">Planificación de la continuidad de la seguridad de la información</td><td rowspan="6">Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un evento.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe la documentación o los procedimientos para los BCP y DRP.</td></tr>
<tr><td rowspan="3">A.17.1.2</td><td rowspan="3">Implementación de la continuidad de la seguridad de la información</td><td rowspan="3">Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un</td></tr>
</table>

<table>
<tr><td></td><td></td><td>durante una situación adversa.</td><td colspan="2">evento.</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI</td><td>NO</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">No existe la documentación o los procedimientos para los BCP y DRP.</td></tr>
<tr><td rowspan="6">A.17.1.3</td><td rowspan="6">Verificación, revisión y evaluación de la continuidad de la seguridad de la información</td><td rowspan="6">Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los procedimientos y controles para la restablecer los servicios se deberían revisar en intervalos regulares con cada uno de los responsables para verificar su efectividad.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe la documentación o los procedimientos para los BCP y DRP.</td></tr>
<tr><td>A.17.2</td><td colspan="4">Redundancias</td></tr>
<tr><td colspan="5">Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.</td></tr>
<tr><td rowspan="2">A.17.2.1</td><td rowspan="2">Disponibilidad de instalaciones de procesamiento de</td><td rowspan="2">Control: Las instalaciones de procesamiento de información se deberían implementar con</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
</table>

	información.	redundancia suficiente para cumplir los requisitos de disponibilidad.	La información debería ser redundante con el fin de mantener la disponibilidad de los servicios y ser probadas en intervalos regulares.	
			IMPLEMENTA	
			SI	**NO**
			La organización no dispone de redundancia de la información.	

A.18	**CUMPLIMIENTO**			
A.18.1	**Cumplimiento de requisitos legales y contractuales**			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	**APLICA**	
			SI	**NO**
			Los administradores deberían identificar toda la información legislativa aplicable a la organización con el fin de cumplir con los requerimientos del negocio.	
			IMPLEMENTA	
			SI	**NO**

<table>
<tr><td></td><td></td><td></td><td colspan="2">Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.</td></tr>
<tr><td rowspan="5">A.18.1.2</td><td rowspan="5">Derechos de propiedad intelectual</td><td rowspan="5">Control: Se deberían 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.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían definir las políticas y procedimientos para controlar la propiedad intelectual.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se definen las políticas y procedimientos para controlar la propiedad intelectual.</td></tr>
<tr><td rowspan="5">A.18.1.3</td><td rowspan="5">Protección de registros</td><td rowspan="5">Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los registros deberían estar clasificados de acuerdo al esquema adoptado por la organización de acuerdo al nivel de confidencialidad.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe un nivel de clasificación formal de confidencialidad de los registros.</td></tr>
</table>

<table>
<tr><td rowspan="8">A.18.1.4</td><td rowspan="8">Privacidad y protección de datos personales</td><td rowspan="8">Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se debería documentar y definir políticas relativas a la protección de datos personales de acuerdo a las reglamentaciones que la ley exige.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Existe una política relativa a la protección de datos personales conforme a los requerimientos de la ley.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="8">A.18.1.5</td><td rowspan="8">Reglamentación de controles criptográficos</td><td rowspan="8">Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida y/o almacenada sea segura.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>A.18.2</td><td colspan="3">Revisiones de seguridad de la información</td></tr>
</table>

<table>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.</td></tr>
<tr><td rowspan="6">A.18.2.1</td><td rowspan="6">Revisión independiente de la seguridad de la información</td><td rowspan="6">Control: 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 deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían realizar auditorías de los procesos, procedimientos y sistemas por medio de entidades externas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se realizan auditorias con entidades externas.</td></tr>
<tr><td rowspan="6">A.18.2.2</td><td rowspan="6">Cumplimiento con las políticas y normas de seguridad</td><td rowspan="6">Control: Los directores deberían 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.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deberían realizar revisiones de las políticas de seguridad con el fin de verificar su cumplimiento.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No existen políticas de la seguridad de la información con la cual se permitan comparar los resultados.</td></tr>
<tr><td>A.18.2.3</td><td>Revisión del</td><td>Control: Los sistemas de</td><td colspan="2">APLICA</td></tr>
</table>

	cumplimiento técnico	información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	**SI**	**NO**
			Los test de penetración deben ser realizados por con herramientas automáticas, con personal calificado y en intervalos programados y acordados con el fin de verificar las políticas de seguridad así como los requerimientos.	
			IMPLEMENTA	
			SI	**NO**
			Aunque se realizan algunos test de penetración no hay políticas de seguridad o metodología de riesgo que permita comparar los resultados.	

ANEXO Nº 3

INVENTARIO Y CLASIFICACIÓN DE ACTIVOS INFORMÁTICOS

[D] DATOS/INFORMACIÓN

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
D_BCK	[backup]	Copias de Seguridad de los Sistemas de Información	Archivos de copias de seguridad de los diferentes Sistemas de Información y Aplicaciones.
D_CNT	[files]	Contratos	Contratos del personal administrativo.
D_GUI	[files]	Guía de usuario	Documento de comunicación técnica destinado a dar asistencia a las personas que utilizan un sistema en particular.
D_HCL	[files]	Historias Clínicas	Información clínica de los trabajadores con sus beneficios
D_HLB	[files]	Historial Laboral	Historial del tiempo laborado por el personal administrativo y de contratación.
D_PUB	[files]	Publicaciones	Publicaciones y comunicaciones oficiales de la empresa.
D_FPE	[files]	Formato de Préstamos de Equipos	Documento legal de la empresa que autoriza el préstamo de cualquier equipo.
D_LOG	[log]	Registros de Actividad	Archivos de registros de actividad de los diferentes Sistemas de Información y Aplicaciones.

D_SRC	[source]	Códigos Fuentes	Archivos de códigos fuentes de los diferentes Sistemas de Información propios desarrollados.

[S] SERVICIOS

CÓDIGO	SUBTIPO	DESCRIPCION	CONTENIDO
S_MAI	[email]	Correo Electrónico	Correo electrónico de uso empresarial para administrativos.
S_GID	[int]	Gestión de Identidades	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras organizacionales.
S_INT	[int]	Servicios Internos	Servicios de uso interno administrativo que cuentan con datos de acceso organizacionales. Software empresarial, Bases de Datos y Gestión Documental.
S_WWW	[www]	Páginas web de acceso público	Páginas que son disponibles para el personal administrativo y acceso público.

[SW] SOFTWARE

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
SW_SWP	[prp]	Software de Desarrollo Propio	Software desarrollado internamente por la empresa para cumplir sus necesidades a la medida.

SW_MAI	[email_client]	Software para Correo Electrónico	Software utilizado para el correo electrónico empresarial.
SW_DBS	[dbms]	Gestores de Bases de Datos	Administran y gestionan las bases de datos que se utilizan para soportar todo el software organizacional, administrativo y demás que apoyan a los demás procesos de la empresa.
SW_OFM	[office]	Ofimática	Software necesario para la realización de las actividades, así como la producción de recursos.
SW_AVS	[av]	Software de Antivirus	Software para prevenir y eliminar el malware.
SW_OPS	[os]	Sistemas Operativos	Software que administra los recursos de las computadoras de uso organizacional.

[HW] HARDWARE

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
HW_BCK	[backup]	Dispositivos de Respaldo	Dispositivos que almacenan la información y son útiles para la recuperación de desastres.
HW_FRW	[firewall]	Firewall	Controla el tráfico entrante/saliente de la red de datos aplicando reglas de seguridad.
HW_ANT	[host]	Antenas	Envío/Recepción de señales para la comunicación con los anexos de la empresa.
HW_HOS	[host]	Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes

			aplicaciones a través de la red.
HW_PCM	[mobile]	Computadoras Portátiles de Uso Organizacional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
HW_PCP	[pc]	Computadoras de Escritorio de Uso Organizacional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
HW_PRT	[print]	Impresoras	Dispositivos para la impresión en papel.
HW_LHD	[peripheral]	Lector de huella digital	Dispositivo que es capaz de leer, guardar e identificar las huellas dactilares.
HW_ROU	[router]	Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).
HW_SCN	[scan]	Escáner	Dispositivos para transformar la información en formato digital.
HW_STR	[peripheral]	Estabilizador	Equipos electrónicos responsables de la corrección de la tensión de la red eléctrica para proporcionar alimento estable y seguro a un equipo eléctrico.
HW_SWH	[switch]	Switch	Administra las VLANS que permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso organizacional.
HW_WAP	[wap]	Puntos de Acceso Inalámbrico	Amplían la cobertura de la red por medio de conexiones inalámbricas.

[COM] COMUNICACIONES

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
COM_INT	[internet]	Internet	Permite el acceso a recursos de la web.
COM_LAN	[LAN]	Red de Área Local	Permite la interconexión de las computadoras organizacionales así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.
COM_WIF	[wifi]	Conectividad Inalámbrica	Permite la conectividad inalámbrica de las computadoras organizacionales, así como amplía la cobertura.
COM_TEL	[PSTN]	Línea telefónica	Circuito eléctrico de un sistema de telecomunicaciones por teléfono.

[AUX] EQUIPO AUXILIAR

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
AUX_RCK	[furniture]	Rack	Aloja los servidores, *router*, *switches* y *firewall* protegiéndolos de la humedad, golpes o uso malintencionado.
AUX_PWR	[power]	Fuente de Alimentación	Provee y regula la energía a los Servidores.
AUX_UPS	[ups]	Sistema de Alimentación	Provee energía temporal a los Servidores y demás

		Ininterrumpida (UPS)	dispositivos vitales en caso de fallas eléctricas inesperadas.
AUX_WIR	[wire]	Cableado Eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.

[L] INSTALACIONES

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
L_SIT	[site]	Empresa Agroindustrial Pomalca S.A.A.	Estructura física que alberga la Empresa Agroindustrial Pomalca S.A.A.

[P] PERSONAL

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
P_ADM	[adm]	Administrador de Sistema	Persona encargada de administrar, gestionar, solucionar y ayudar en el correcto funcionamiento de los diferentes Sistemas de Información.
P_COM	[com]	Administrador de Comunicaciones	Persona encargada de administrar y gestionar el tráfico de datos en la red interna, así como configurar los diferentes dispositivos de comunicaciones que garanticen un óptimo rendimiento para el acceso a servicios y Sistemas de Información.
P_DBA	[dba]	Administrador de Bases de Datos	Persona que administra, configura y optimiza el rendimiento de las diferentes bases de datos que utilizan los Sistemas de Información para el soporte de los procesos

			organizacionales.
P_DES	[des]	Desarrolladores de Software	Persona que se encarga de programar el código fuente para los Sistemas de Información.
P_TEC	[op]	Responsable de soporte técnico	Personal capacitado para dar asistencia a los equipos defectuosos de la empresa.

ANEXO Nº 4

VALORACIÓN DE LOS ACTIVO DE ACUERDO AL IMPACTO

[D] DATOS/INFORMACIÓN

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
D_BCK	Copias de Seguridad de los Sistemas de Información	**MA**	Las copias de seguridad son determinantes para la recuperación de archivos ante un desastre.
D_CNT	Contratos	**M**	Los contratos son esenciales para los procesos jurídicos - administrativos
D_GUI	Guía de usuario	**M**	Las guías de usuario son importantes porque dan asistencia a las personas que utilizan un sistema.
D_HCL	Historias Clínicas	**M**	Archivos de historial clínico de enfermedades, tratamientos y suministros de medicamentos a los administrativos de la empresa.
D_HLB	Historial Laboral	**M**	Archivos esenciales para el historial laboral de los administrativos.
D_PUB	Publicaciones	**B**	Archivos de publicaciones organizacionales.
D_FPE	Formato de Préstamos de Equipos	**B**	Archivo legal de la empresa que autoriza el préstamo de cualquier equipo.
D_LOG	Registros de Actividad	**MA**	Los archivos de registro son esenciales para realizar seguimiento a los

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
			fallos de los Sistemas de Información y determinar posibles causas de mal funcionamiento o acceso no autorizado.
D_SRC	Códigos Fuentes	**MA**	Los archivos de código fuente contienen información de cómo se ejecutan los procesos internos en los Sistemas de Información desarrollados para la empresa.

[S] SERVICIOS

CÓDIGO	DESCRIPCION	IMPACTO	RAZÓN
S_MAI	Correo Electrónico	**A**	El correo electrónico se utiliza para la comunicación interna de los administrativos.
S_GID	Gestión de Identidades	**MA**	Acceso del personal administrativo a sus cuentas de usuario en el dominio organizacional.
S_INT	Servicios Internos	**MA**	Acceso a los servicios internos organizacionales para el desarrollo normal de los procesos.
S_WWW	Páginas web de acceso público	**M**	Acceso a la página web organizacional que ofrecen servicios al personal administrativo y al público en general.

[SW] SOFTWARE

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
SW_SWP	Software de Desarrollo Propio	**MA**	Utilizados para el normal desarrollo de los procesos organizacionales.
SW_MAI	Software para Correo Electrónico	**A**	Utilizado para la comunicación de administrativos.
SW_DBS	Gestores de Bases de Datos	**MA**	Almacena toda la información de los diferentes Sistemas de Información, así como el soporte para el desarrollo normal de los procesos y tomas de decisiones.
SW_OFM	Ofimática	**B**	Utilizado para la ejecución de tareas.
SW_AVS	Software de Antivirus	**A**	Utilizado para la prevención y eliminación de software malintencionado, así como evitar la propagación de malware por la red.
SW_OPS	Sistemas Operativos	**A**	Administra los recursos de software y hardware de las diferentes computadoras de uso organizacional.

[HW] HARDWARE

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
HW_BCK	Dispositivos de Respaldo	**MA**	Dispositivos que almacenan los archivos de las copias de seguridad necesarios para la recuperación en caso de desastres.

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
HW_FRW	Firewall	**MA**	Dispositivo que filtra los paquetes. Esencial para la configuración de seguridad de la red de datos.
HW_ANT	Antenas	**A**	Esencial para establecer los enlaces de comunicación con cada uno de los anexos de la empresa.
HW_HOS	Servidores	**MA**	Dispositivos esenciales para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos organizacionales.
HW_PCM	Computadoras Portátiles de Uso Organizacional	**M**	Dispositivos para la ejecución de tareas.
HW_PCP	Computadoras de Escritorio de Uso Organizacional	**M**	Dispositivos para la ejecución de tareas.
HW_PRT	Impresoras	**MB**	Dispositivos para realizar impresiones en papel.
HW_LHD	Lector de huella digital	**MB**	Dispositivo que es capaz de leer, guardar e identificar las huellas dactilares.
HW_ROU	Router	**A**	Esencial para direccionar el tráfico de datos interno y externo. A su vez, hace el papel de Gateway para dar salida a Internet.
HW_SCN	Escáner	**MB**	Dispositivos para digitalizar documentos.

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
HW_STR	Estabilizador	**MB**	Equipos electrónicos responsables de la corrección de la tensión de la red eléctrica para proporcionar alimento estable y seguro a un equipo eléctrico.
HW_SWH	Switch	**A**	Esencial para direccionar el tráfico de datos interno, administración de VLAN y segmentar el ancho de banda con el fin de optimizarla.
HW_WAP	Puntos de Acceso Inalámbrico	**B**	Amplían la cobertura de la red por medio de conexiones inalámbricas.

[COM] COMUNICACIONES

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
COM_INT	Internet	**A**	Permite el acceso a recursos de la web.
COM_LAN	Red de Área Local	**MA**	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos organizacionales. Incluye todo el cableado estructurado.
COM_WIF	Conectividad Inalámbrica	**B**	Amplía la cobertura y otorga acceso inalámbrico a ciertos dispositivos.
COM_TEL	Línea telefónica	**B**	Permite a comunicación interna entre las áreas administrativas de la organización.

[AUX] EQUIPO AUXILIAR

CÓDIGO	DESCRIPCIÓN	IMAPACTO	RAZÓN
AUX_RCK	Rack	**A**	Mantiene los dispositivos de red como el router, switches y servidores organizados y asegurados.
AUX_PWR	Fuente de Alimentación	**MA**	Esencial para el funcionamiento normal de todos los dispositivos que soportan los Sistemas de Información y procesos organizacional.
AUX_UPS	Sistema de Alimentación Ininterrumpida (UPS)	**A**	Esencial para mantener funcionando a los dispositivos en caso de una eventual falla en el suministro eléctrico, así como también evita el daño parcial o total del hardware.
AUX_WIR	Cableado Eléctrico	**MA**	Cableado esencial para mantener en funcionamiento los dispositivos y el normal desarrollo de los procesos organizacionales.

[L] INSTALACIONES

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
L_SIT	Empresa Agroindustrial Pomalca S.A.A.	**MA**	Esencial para el normal funcionamiento de todos los Sistemas de Información que soportan los procesos organizacionales.

[P] PERSONAL

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
P_ADM	Administrador de Sistema	**MA**	Personas encargadas de administrar los diferentes Sistemas de Información que dan soporte a los procesos organizacionales y sus servicios.
P_COM	Administrador de Comunicaciones	**MA**	Personas encargadas de administrar, configurar y operar las redes de comunicación de datos que dan soporte al normal funcionamiento de los servicios internos.
P_DBA	Administrador de Bases de Datos	**MA**	Persona encargada de administrar, configurar y optimizar el rendimiento de las bases de datos que contienen los datos de los diferentes Sistemas de Información, así como velar por la seguridad de que éstos se mantengan confidenciales, disponibles e íntegros.
P_DES	Desarrolladores de Software	**A**	Personas encargadas de desarrollar y/o programar el software que se ajuste a las necesidades de la organización.
P_TEC	Responsable de soporte técnico	**M**	Personal capacitado para dar asistencia a los equipos defectuosos de la empresa.

ANEXO Nº 5

VALORACIÓN DE LOS ACTIVO DE ACUERDO A LAS DIMENSIONES DE SEGURIDAD

[D] DATOS/INFORMACIÓN

CÓDIGO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D] DISPONIBILIDAD	[I] INTEGRIDAD	[C] CONFIDENCIALIDAD	[A] AUTENTICIDAD	[T] TRAZABILIDAD
D_BCK	Copias de Seguridad de los Sistemas de Información	**5**		**2**		
D_CNT	Contratos		**2**			
D_GUI	Guía de usuario	**3**			**6**	
D_HCL	Historias Clínicas		**6**	**7**	**6**	**6**
D_HLB	Historial Laboral		**3**	**2**		
D_PUB	Publicaciones	**1**				
D_FPE	Formato de Préstamos de Equipos		**2**			

D_LOG	Registros de Actividad			**2**		**3**
D_SRC	Códigos Fuentes		**3**	**5**		

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
D_BCK	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_CNT	[I]	2.pi1: Pudiera causar molestias a un individuo
D_GUI	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[A]	6.pi1: Probablemente afecte gravemente a un grupo de individuos
D_HCL	[I][A][T]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
D_HLB	[I]	3.lro: Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_PUB	[D]	1.pi1: Pudiera causar molestias a un individuo
D_FPE	[I]	2.pi1: Pudiera causar molestias a un individuo

D_LOG	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
D_SRC	[I]	3.olm: Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
	[C]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización

[S] SERVICIOS

CÓDIGO	**DESCRIPCIÓN**	**DIMENSIONES DE SEGURIDAD**				
		[D] DISPONIBILIDAD	**[I] INTEGRIDAD**	**[C] CONFIDENCIALIDAD**	**[A] AUTENTICIDAD**	**[T] TRAZABILIDAD**
S_MAI	Correo Electrónico	**3**		**2**		
S_GID	Gestión de Identidades	**5**	**2**	**2**		**4**
S_INT	Servicios Internos	**3**				
S_WWW	Páginas web de acceso público	**3**				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
S_MAI	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
S_GID	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	2.pi1: Pudiera causar molestias a un individuo
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
S_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
S_WWW	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización

[SW] SOFTWARE

CÓDIGO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D] DISPONIBILIDAD	[I] INTEGRIDAD	[C] CONFIDENCIALIDAD	[A] AUTENTICIDAD	[T] TRAZABILIDAD
SW_SWP	Software de Desarrollo Propio	**3**		**4**	**7**	**4**

SW_MAI	Software para Correo Electrónico	**5**				**1**
SW_DBS	Gestores de Bases de Datos	**7**	**7**	**7**	**7**	
SW_OFM	Ofimática	**1**				
SW_AVS	Software de Antivirus			**7**		
SW_OPS	Sistemas Operativos	**5**	**7**			

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
SW_SWP	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	4.pi1: Probablemente afecte a un grupo de individuos
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
SW_MAI	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	1.si: Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

SW_DBS	[D][I][A]	7.adm: Probablemente impediría la operación efectiva de la Organización
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
SW_OFM	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
SW_AVS	[C]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[HW] HARDWARE

CÓDIGO	**DESCRIPCIÓN**	**DIMENSIONES DE SEGURIDAD**				
		[D] DISPONIBILIDAD	**[I] INTEGRIDAD**	**[C] CONFIDENCIALIDAD**	**[A] AUTENTICIDAD**	**[T] TRAZABILIDAD**
HW_BCK	Dispositivos de Respaldo			**2**		**3**
HW_FRW	Firewall	**7**				
HW_ANT	Antenas	**3**				
HW_HOS	Servidores	**5**		**7**	**7**	
HW_PCM	Computadoras Portátiles de Uso Organizacional	**1**				

HW_PCP	Computadoras de Escritorio de Uso Organizacional	**1**				
HW_PRT	Impresoras	**1**				
HW_LHD	Lector de huella digital	**1**				
HW_ROU	Router	**5**			**7**	
HW_SCN	Escáner	**1**				
HW_STR	Estabilizador	**5**				
HW_SWH	Switch	**5**			**7**	
HW_WAP	Puntos de Acceso Inalámbrico	**1**				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
HW_BCK	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
HW_FRW	[D]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la

		investigación de incidentes graves
HW_ANT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
HW_HOS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[C][A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_PCM/ HW_PCP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
HW_PRT/ HW_SCN/ HW_LHD	[D]	1.pi1: Pudiera causar molestias a un individuo
HW_ROU/ HW_STR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_SWH	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_WAP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización

[COM] COMUNICACIONES

CÓDIGO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D] DISPONIBILIDAD	[I] INTEGRIDAD	[C] CONFIDENCIALIDAD	[A] AUTENTICIDAD	[T] TRAZABILIDAD
COM_INT	Internet	**3**				
COM_LAN	Red de Área Local	**5**				
COM_WIF	Conectividad Inalámbrica	**1**				
COM_TEL	Línea telefónica	**1**				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
COM_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
COM_LAN	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
COM_WIF/ COM_TEL	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización

[AUX] EQUIPO AUXILIAR

CÓDIGO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D] DISPONIBILIDAD	[I] INTEGRIDAD	[C] CONFIDENCIALIDAD	[A] AUTENTICIDAD	[T] TRAZABILIDAD
AUX_RCK	Rack	**5**				
AUX_PWR	Fuente de Alimentación	**5**				
AUX_UPS	Sistema de Alimentación Ininterrumpida (UPS)	**5**				
AUX_WIR	Cableado Eléctrico	**5**				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
AUX_RCK	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_PWR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_UPS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la

		Organización
AUX_WIR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización

[L] INSTALACIONES

CÓDIGO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D] DISPONIBILIDAD	[I] INTEGRIDAD	[C] CONFIDENCIALIDAD	[A] AUTENTICIDAD	[T] TRAZABILIDAD
L_SIT	Empresa Agroindustrial Pomalca S.A.A.	**7**				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
L_SIT	[D]	7.adm: Probablemente impediría la operación efectiva de la Organización

[P] PERSONAL

CÓDIGO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D] DISPONIBILIDAD	[I] INTEGRIDAD	[C] CONFIDENCIALIDAD	[A] AUTENTICIDAD	[T] TRAZABILIDAD

P_ADM	Administrador de Sistema	**5**				
P_COM	Administrador de Comunicaciones	**5**				
P_DBA	Administrador de Bases de Datos	**5**				
P_DES	Desarrolladores de Software	**3**				
P_TEC	Responsable de soporte técnico	**3**				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
P_ADM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_COM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_DBA	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_DES	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
P_TEC	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización

ANEXO Nº 6

IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

[D] DATOS/INFORMACIÓN

ACTIVOS	
Copias de Seguridad de los Sistemas de Información	**FRECUENCIA O PROBABILIDAD**
5.3.1. [E.1] Errores de los usuarios	**5**
5.3.2. [E.2] Errores del administrador	**5**
5.3.9. [E.14] Escapes de información	**5**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**5**
Contratos	**FRECUENCIA O PROBABILIDAD**
5.3.1. [E.1] Errores de los usuarios	**50**
5.3.9. [E.14] Escapes de información	**10**
5.3.10. [E.15] Alteración accidental de la información	**10**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**

5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**10**
Códigos Fuente	**FRECUENCIA O PROBABILIDAD**
5.3.4. [E.4] Errores de configuración	**10**
5.3.9. [E.14] Escapes de información	**5**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**5**
Formato de Préstamos de Equipos	**FRECUENCIA O PROBABILIDAD**
5.3.1. [E.1] Errores de los usuarios	**50**
5.3.9. [E.14] Escapes de información	**10**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**10**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**10**

Guía de Usuario	FRECUENCIA O PROBABILIDAD
5.3.9. [E.14] Escapes de información	**10**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**10**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**10**
Historias Clínicas	**FRECUENCIA O PROBABILIDAD**
5.3.9. [E.14] Escapes de información	**10**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**10**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**10**
Historial Laboral	**FRECUENCIA O PROBABILIDAD**
5.3.9. [E.14] Escapes de información	**10**
5.3.11. [E.18] Destrucción de información	**5**

5.3.12. [E.19] Fugas de información	**10**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**10**
Publicaciones	**FRECUENCIA O PROBABILIDAD**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de información	**5**
Registros de Actividad	**FRECUENCIA O PROBABILIDAD**
5.3.3. [E.3] Errores de monitorización (log)	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.4.1. [A.3] Manipulación de los registros de actividad (log)	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**

[S] SERVICIOS

ACTIVOS	
Correo Electrónico	**FRECUENCIA O PROBABILIDAD**
5.3.1. [E.1] Errores de los usuarios	**50**
5.3.9. [E.14] Escapes de información	**50**
5.3.10. [E.15] Alteración accidental de la información	**10**
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	**50**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.8. [A.10] Alteración de secuencia	**5**
5.4.9. [A.11] Acceso no autorizado	**10**
5.4.11. [A.13] Repudio	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de la información	**10**
5.4.18. [A.24] Denegación de servicio	**5**
Gestión de Identidades	**FRECUENCIA O PROBABILIDAD**
5.3.9. [E.14] Escapes de información	**50**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	**50**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.9. [A.11] Acceso no autorizado	**5**

5.4.11. [A.13] Repudio	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de la información	**5**
5.4.18. [A.24] Denegación de servicio	**5**
Páginas Web de Acceso Público	**FRECUENCIA O PROBABILIDAD**
5.3.10. [E.15] Alteración accidental de la información	**10**
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	**50**
5.4.14. [A.18] Destrucción de información	**5**
5.4.18. [A.24] Denegación de servicio	**5**
Servicios Interno	**FRECUENCIA O PROBABILIDAD**
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	**50**
5.4.18. [A.24] Denegación de servicio	**5**

[SW] SOFTWARE

ACTIVOS	
Gestores de Base de Datos	**FRECUENCIA O PROBABILIDAD**
5.2.6. [I.5] Avería de origen físico o lógico	**5**
5.3.1. [E.1] Errores de los usuarios	**10**
5.3.2. [E.2] errores de administrador	**10**
5.3.6. [E.8] Difusión de software dañino	**5**
5.3.9. [E.14] Escapes de información	**5**

5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.3.13. [E.20] Vulnerabilidades de los programas (software)	**10**
5.4.3. [A.5] Suplantación de identidad del usuario	**10**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.5. [A.7] Uso no previsto	**5**
5.4.6. [A.8] Difusión de software dañino	**5**
5.4.7. [A.9] [Re-]encaminamiento de mensajes	**5**
5.4.8. [A.10] Alteración de secuencia	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de la información	**5**
5.4.16. [A.22] Manipulación de programas	**5**
Ofimática	**FRECUENCIA O PROBABILIDAD**
5.2.6. [I.5] Avería de origen físico o lógico	**10**
5.3.1. [E.1] Errores de los usuarios	**50**
5.3.6. [E.8] Difusión de software dañino	**10**
5.3.13. [E.20] Vulnerabilidades de los programas (software)	**50**
5.4.5. [A.7] Uso no previsto	**50**
5.4.6. [A.8] Difusión de software dañino	**5**
5.4.9. [A.11] Acceso no autorizado	**5**

Sistemas Operativos	FRECUENCIA O PROBABILIDAD
5.2.6. [I.5] Avería de origen físico o lógico	**5**
5.3.1. [E.1] Errores de los usuarios	**10**
5.3.2. [E.2] errores de administrador	**10**
5.3.6. [E.8] Difusión de software dañino	**10**
5.3.9. [E.14] Escapes de información	**5**
5.3.10. [E.15] Alteración accidental de la información	**10**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.3.13. [E.20] Vulnerabilidades de los programas (software)	**5**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.5. [A.7] Uso no previsto	**5**
5.4.6. [A.8] Difusión de software dañino	**5**
5.4.7. [A.9] [Re-]encaminamiento de mensajes	**5**
5.4.8. [A.10] Alteración de secuencia	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de la información	**5**
5.4.16. [A.22] Manipulación de programas	**5**
Software de antivirus	**FRECUENCIA O PROBABILIDAD**
5.2.6. [I.5] Avería de origen físico o lógico	**5**

5.3.1. [E.1] Errores de los usuarios	**50**
5.3.6. [E.8] Difusión de software dañino	**10**
5.3.13. [E.20] Vulnerabilidades de los programas (software)	**10**
5.4.5. [A.7] Uso no previsto	**5**
5.4.6. [A.8] Difusión de software dañino	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
Software para Correo Electrónico	**FRECUENCIA O PROBABILIDAD**
5.2.6. [I.5] Avería de origen físico o lógico	**10**
5.3.1. [E.1] Errores de los usuarios	**70**
5.3.2. [E.2] errores de administrador	**10**
5.3.6. [E.8] Difusión de software dañino	**5**
5.3.9. [E.14] Escapes de información	**5**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**1**
5.3.12. [E.19] Fugas de información	**50**
5.3.13. [E.20] Vulnerabilidades de los programas (software)	**10**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.5. [A.7] Uso no previsto	**5**
5.4.6. [A.8] Difusión de software dañino	**5**
5.4.7. [A.9] [Re-]encaminamiento de mensajes	**5**
5.4.8. [A.10] Alteración de secuencia	**5**
5.4.9. [A.11] Acceso no autorizado	**5**

5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de la información	**5**
5.4.16. [A.22] Manipulación de programas	**5**
Software de Desarrollo Propio	**FRECUENCIA O PROBABILIDAD**
5.2.6. [I.5] Avería de origen físico o lógico	**5**
5.3.1. [E.1] Errores de los usuarios	**50**
5.3.2. [E.2] errores de administrador	**10**
5.3.6. [E.8] Difusión de software dañino	**10**
5.3.9. [E.14] Escapes de información	**10**
5.3.10. [E.15] Alteración accidental de la información	**5**
5.3.11. [E.18] Destrucción de información	**5**
5.3.12. [E.19] Fugas de información	**5**
5.3.13. [E.20] Vulnerabilidades de los programas (software)	**50**
5.4.3. [A.5] Suplantación de identidad del usuario	**5**
5.4.4. [A.6] Abuso de privilegios de acceso	**5**
5.4.5. [A.7] Uso no previsto	**5**
5.4.6. [A.8] Difusión de software dañino	**10**
5.4.7. [A.9] [Re-]encaminamiento de mensajes	**5**
5.4.8. [A.10] Alteración de secuencia	**5**
5.4.9. [A.11] Acceso no autorizado	**5**
5.4.13. [A.15] Modificación deliberada de la información	**5**
5.4.14. [A.18] Destrucción de información	**5**
5.4.15. [A.19] Divulgación de la información	**5**

5.4.16. [A.22] Manipulación de programas	**5**

[HW] HARDWARE

ACTIVOS	
Antenas	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	5
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	5
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.5. [A.7] Uso no previsto	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Computadoras de Escritorio de uso Organizacional	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.2. [E.2] Errores del administrador	20

5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Computadoras Portátiles de uso Organizacional	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.2. [E.2] Errores del administrador	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5

5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Dispositivos de Respaldo	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.2. [E.2] Errores del administrador	5
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Escáner	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5

5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.17. [E.25] Pérdida de equipos	5
5.4.19. [A.25] Robo	5
Estabilizador	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.17. [E.25] Pérdida de equipos	5
5.4.19. [A.25] Robo	5
Firewall	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10

5.3.2. [E.2] Errores del administrador	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Impresoras	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.17. [E.25] Pérdida de equipos	5
5.4.19. [A.25] Robo	5
Lector de Huella Digital	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5

5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.17. [E.25] Pérdida de equipos	5
5.4.19. [A.25] Robo	5
Puntos de Acceso Inalámbrico	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.2. [E.2] Errores del administrador	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5

Router	FRECUENCIA O PROBABILIDAD
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.2. [E.2] Errores del administrador	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Servidores	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10

5.3.2. [E.2] Errores del administrador	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
Switch	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.2. [E.2] Errores del administrador	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5

5.4.9. [A.11] Acceso no autorizado	5
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5

[COM] COMUNICACIONES

ACTIVOS	
Conectividad Inalámbrica	**FRECUENCIA O PROBABILIDAD**
5.3.2. [E.2] Errores del administrador	10
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	50
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5
5.4.18. [A.24] Denegación de servicio	70
Línea telefónica	**FRECUENCIA O PROBABILIDAD**
5.3.2. [E.2] Errores del administrador	10
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	10
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5

5.4.9. [A.11] Acceso no autorizado	5
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5
5.4.18. [A.24] Denegación de servicio	10
Internet	**FRECUENCIA O PROBABILIDAD**
5.3.2. [E.2] Errores del administrador	5
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	10
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	10
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5
5.4.18. [A.24] Denegación de servicio	10
Red de Área Local	**FRECUENCIA O PROBABILIDAD**
5.3.2. [E.2] Errores del administrador	10
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	50
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5

5.4.18. [A.24] Denegación de servicio	70

[AUX] EQUIPO AUXILIAR

ACTIVOS	
Cableado Eléctrico	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	5
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.4.19. [A.25] Robo	5
5.4.20. [A.26] Ataque destructivo	5
Fuente de Alimentación	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.4.19. [A.25] Robo	5
5.4.20. [A.26] Ataque destructivo	5

Rack	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.4.19. [A.25] Robo	5
5.4.20. [A.26] Ataque destructivo	5
Sistema de Alimentación Ininterrumpida (UPS)	**FRECUENCIA O PROBABILIDAD**
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	20
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.4.19. [A.25] Robo	5
5.4.20. [A.26] Ataque destructivo	5

[L]INSTALACIONES

ACTIVOS	
Empresa Agroindustrial Pomalca S.A.A.	**FRECUENCIA O**

	PROBABILIDAD
5.1.3. [N.*] Desastres Naturales	5
5.2.12. [I.11] Emanaciones electromagnéticas	5
5.3.10. [E.15] Alteración accidental de la información	5
5.3.11. [E.18] Destrucción de información	5
5.3.12. [E.19] Fugas de información	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	5
5.4.20. [A.26] Ataque destructivo	5

[P] PERSONAL

ACTIVOS	
Administrador de Base de Datos	**FRECUENCIA O PROBABILIDAD**
5.3.5. [E.7] Deficiencias en la organización	5
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.4.22. [A.28] Indisponibilidad del personal	5
Administrador de Comunicaciones	**FRECUENCIA O PROBABILIDAD**
5.3.5. [E.7] Deficiencias en la organización	5
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10

5.4.22. [A.28] Indisponibilidad del personal	5
Administrador de Sistema	**FRECUENCIA O PROBABILIDAD**
5.3.5. [E.7] Deficiencias en la organización	5
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.4.22. [A.28] Indisponibilidad del personal	5
Desarrolladores de Software	**FRECUENCIA O PROBABILIDAD**
5.3.5. [E.7] Deficiencias en la organización	5
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.4.22. [A.28] Indisponibilidad del personal	5
Responsable de Soporte Técnico	**FRECUENCIA O PROBABILIDAD**
5.3.5. [E.7] Deficiencias en la organización	5
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.4.22. [A.28] Indisponibilidad del personal	5

ANEXO Nº 7

RIESGO POTENCIAL

[D] DATOS/INFORMACIÓN

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
D_BCK	Copias de Seguridad de los Sistemas de Información	**MA**	**MB**	**E*, A***	R_D_BCK	**A**
D_CNT	Contratos	**M**	**M**	**E*, A***	R_D_CNT	**M**
D_GUI	Guía de usuario	**M**	**B**	**E*, A***	R_D_GUI	**M**
D_HCL	Historias Clínicas	**M**	**B**	**E*, A***	R_D_HCL	**M**
D_HLB	Historial Laboral	**M**	**B**	**E*, A***	R_D_HLB	**M**
D_PUB	Publicaciones	**B**	**MB**	**E*, A***	R_D_PUB	**MB**
D_FPE	Formato de Préstamos de Equipos	**B**	**M**	**E*, A***	R_D_FPE	**B**
D_LOG	Registros de Actividad	**MA**	**MB**	**E*, A***	R_D_LOG	**A**
D_SRC	Códigos Fuentes	**MA**	**B**	**E*, A***	R_D_SRC	**MA**

[S] SERVICIOS

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
S_MAI	Correo Electrónico	**A**	**M**	**E*, A***	R_S_MAI	**A**
S_GID	Gestión de Identidades	**MA**	**M**	**E*, A***	R_S_GID	**MA**
S_INT	Servicios Internos	**MA**	**M**	**E*, A***	R_S_INT	**MA**
S_WWW	Páginas web de acceso público	**M**	**M**	**E*, A***	R_S_WWW	**M**

[SW] SOFTWARE

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
SW_SWP	Software de Desarrollo Propio	**MA**	**M**	**I*, E*, A***	R_SW_SWP	**MA**
SW_MAI	Software para Correo Electrónico	**A**	**A**	**I*, E*, A***	R_SW_MAI	**MA**
SW_DBS	Gestores de Bases de Datos	**MA**	**B**	**I*, E*, A***	R_SW_DBS	**MA**
SW_OFM	Ofimática	**B**	**M**	**I*, E*, A***	R_SW_OFM	**B**
SW_AVS	Software de Antivirus	**A**	**M**	**I*, E*, A***	R_SW_AVS	**A**
SW_OPS	Sistemas Operativos	**A**	**B**	**I*, E*, A***	R_SW_OPS	**A**

[HW] HARDWARE

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
HW_BCK	Dispositivos de Respaldo	**MA**	**M**	**I*, E*, A***	R_HW_BCK	**MA**
HW_FRW	Firewall	**MA**	**M**	**I*, E*, A***	R_HW_FRW	**MA**
HW_ANT	Antenas	**A**	**MB**	**I*, E*, A***	R_HW_ANT	**M**
HW_HOS	Servidores	**MA**	**M**	**I*, E*, A***	R_HW_HOS	**MA**
HW_PCM	Computadoras Portátiles de Uso Organizacional	**M**	**M**	**I*, E*, A***	R_HW_PCM	**M**
HW_PCP	Computadoras de Escritorio de Uso Organizacional	**M**	**M**	**I*, E*, A***	R_HW_PCP	**M**
HW_PRT	Impresoras	**MB**	**M**	**I*, E*, A***	R_HW_PRT	**MB**
HW_LHD	Lector de huella digital	**MB**	**M**	**I*, E*, A***	R_HW_LHD	**MB**
HW_ROU	Router	**A**	**M**	**I*, E*, A***	R_HW_ROU	**A**
HW_SCN	Escáner	**MB**	**M**	**I*, E*, A***	R_HW_SCN	**MB**
HW_STR	Estabilizador	**MB**	**M**	**I*, E*, A***	R_HW_STR	**MB**
HW_SWH	Switch	**A**	**M**	**I*, E*, A***	R_HW_SWH	**A**

HW_WAP	Puntos de Acceso Inalámbrico	**B**	**M**	**I*, E*, A***	R_HW_WAP	**B**

[COM] COMUNICACIONES

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
COM_INT	Internet	**A**	**A**	**E*, A***	R_COM_INT	**MA**
COM_LAN	Red de Área Local	**MA**	**A**	**E*, A***	R_COM_LAN	**MA**
COM_WIF	Conectividad Inalámbrica	**B**	**A**	**E*, A***	R_COM_WIF	**M**
COM_TEL	Línea telefónica	**B**	**B**	**E*, A***	R_COM_TEL	**B**

[AUX] EQUIPO AUXILIAR

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
AUX_RCK	Rack	**A**	**M**	**I*, E*, A***	R_AUX_RCK	**A**
AUX_PWR	Fuente de Alimentación	**MA**	**M**	**I*, E*, A***	R_AUX_PWR	**MA**
AUX_UPS	Sistema de Alimentación Ininterrumpida (UPS)	**A**	**M**	**I*, E*, A***	R_AUX_UPS	**A**
AUX_WIR	Cableado Eléctrico	**MA**	**M**	**I*, E*, A***	R_AUX_WIR	**MA**

[L] INSTALACIONES

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
L_SIT	Empresa Agroindustrial Pomalca S.A.A.	**MA**	**MB**	**N*, I*, E*, A***	R_L_SIT	**A**

[P] PERSONAL

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
P_ADM	Administrador de Sistema	**MA**	**B**	**E*, A***	R_P_ADM	**MA**
P_COM	Administrador de Comunicaciones	**MA**	**B**	**E*, A***	R_P_COM	**MA**
P_DBA	Administrador de Bases de Datos	**MA**	**B**	**E*, A***	R_P_DBA	**MA**
P_DES	Desarrolladores de Software	**A**	**B**	**E*, A***	R_P_DES	**A**
P_TEC	Responsable de soporte técnico	**M**	**B**	**E*, A***	R_P_TEC	**M**

Clasificación de los riesgos según la Zona de Riesgos:

RIESGO		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	R_D_BCK, R_D_LOG, R_L_SIT	R_D_SRC, R_SW_DBS, R_P_ADM, R_P_COM, R_P_DBA	R_S_GID, R_S_INT, R_SW_SWP, R_HW_BCK, R_HW_FRW, R_HW_HOS, R_AUX_PWR, R_AUX_WIR	R_COM_LAN	
	A	R_HW_ANT	R_SW_OPS, R_P_DES	R_S_MAI, R_HW_ROU, R_HW_SWH,R_SW_AVS, R_AUX_RCK, R_AUX_UPS	R_SW_MAI, R_COM_INT	
	M		R_D_GUI, R_D_HCL, R_D_HLB, R_P_TEC	R_D_CNT, R_S_WWW, R_HW_PCM, R_HW_PCP		
	B	R_D_PUB	R_COM_TEL	R_D_FPE, R_SW_OFM, R_HW_WAP	R_COM_WIF	
	MB			R_HW_LHD, R_HW_STR,R_HW_PRT, R_HW_SCN		

ANEXO Nº 8

APLICABILIDAD DE CONTROLES PARA LA EMPRESA AGROINDUSTRIAL POMALCA S.A.A.

Núm.	Control	Aplicable	Justificación
5	**Políticas de seguridad de la información**		
5.1	Directrices establecidas por la dirección para la seguridad de la información		
5.1.1	Políticas para la seguridad de la información	SI	Se redactan y documentan las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables. Este documento se pone a disposición de los empleados y público en general.
5.1.2	Revisión de las políticas para seguridad de la información	SI	Las políticas de seguridad de la información deben ser revisadas y evaluadas periódicamente y/o cuando sea necesario. Se deben documentar los cambios y las justificaciones de los mismos.
6	**Organización de la seguridad de la información**		
6.1	Organización interna		
6.1.1	Roles y responsabilidades para la seguridad de información	SI	Los roles y responsabilidades de la seguridad de la información están definidas.
6.1.2	Separación de deberes	SI	El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su

Núm.	Control	Aplicable	Justificación
			trabajo.
6.1.3	Contacto con las autoridades	SI	Es recomendable que el jefe de la oficina de Sistemas y Cómputo mantenga contactos actualizados para incidentes de seguridad.
6.1.4	Contacto con grupos de interés especial	SI	Es recomendable que el jefe de la oficina de Sistemas y Cómputo mantenga contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.
6.1.5	Seguridad de la información en la gestión de proyectos	SI	El Jefe de la oficina de Sistemas y Cómputo es el encargado de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos de TI.
6.2	Dispositivos móviles y teletrabajo		
6.2.1	Política para dispositivos móviles	SI	Es necesario documentar una política de seguridad apropiada para los móviles. Los dispositivos móviles deberían ser configurados bajo las condiciones de seguridad aplicables antes de realizar cualquier conexión a la red institucional.
6.2.2	Teletrabajo	NO	
7	**Seguridad de los recursos humanos**		
7.1	Antes de asumir el empleo		
7.1.1	Selección	SI	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
7.1.2	Términos y condiciones del empleo	SI	Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.

Núm.	Control	Aplicable	Justificación
7.2	Durante la ejecución del empleo		
7.2.1	Responsabilidades de la dirección	SI	La empresa comprende la importancia de la seguridad de la información y soporta el diseño del SGSI.
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	El jefe de la oficina de Sistemas y Cómputo debería realizar campañas y talleres de formación y educación en la seguridad de la información de forma periódica al personal administrativo.
7.2.3	Proceso disciplinario	SI	Es recomendable que los trabajadores sean sometidos a procesos disciplinarios en caso de incumplimiento con las políticas de seguridad de la información de forma deliberada.
7.3	Terminación o cambio de empleo		
7.3.1	Terminación o cambio de responsabilidades de empleo	SI	El jefe de la oficina de Sistemas y Cómputo debe procurar que el empleado que termine el contrato o cambie de responsabilidades, se le sean reasignados los permisos y condiciones de seguridad de la información.
8	**Gestión de activos**		
8.1	Responsabilidad por los activos		
8.1.1	Inventario de activos	SI	El jefe de la oficina de Sistemas y Cómputo junto a los empleados, realizan el inventario de activos y se documentan con su clasificación.
8.1.2	Propiedad de los activos	SI	Es recomendable que los activos inventariados tengan asignados a los trabajadores responsables.
8.1.3	Uso aceptable de los activos	SI	Es necesario que los empleados se comprometan a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de

Núm.	Control	Aplicable	Justificación
			información generales.
8.1.4	Devolución de activos	SI	Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.
8.2	Clasificación de la información		
8.2.1	Clasificación de la información	SI	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo a los niveles de seguridad establecidos.
8.2.2	Etiquetado de la información	SI	Cada uno de los activos inventariados están etiquetados con la clasificación de la información asociada.
8.2.3	Manejo de activos	SI	Es recomendable que el jefe de la oficina de Sistemas y Cómputo junto a los empleados realicen y documenten los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
8.3	Manejo de los soportes de almacenamiento		
8.3.1	Gestión de medios removibles	SI	Existe una política para la gestión de los medios removibles y se clasifican y protegen de acuerdo a su tipo.
8.3.2	Disposición de los medios	SI	Los medios removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
8.3.3	Transferencia de medios físicos	NO	
9	**Control de acceso**		
9.1	Requisitos del negocio para control de		

Núm.	Control	Aplicable	Justificación
	acceso		
9.1.1	Política de control de acceso	SI	La política de control de acceso está documentada en las Políticas de la Seguridad de Información.
9.1.2	Política sobre el uso de los servicios de red	SI	Las redes están segmentadas y el acceso a ella está protegido a personas no autorizadas.
9.2	Gestión de acceso de usuarios		
9.2.1	Registro y cancelación del registro de usuarios	NO	
9.2.2	Suministro de acceso de usuarios	NO	
9.2.3	Gestión de derechos de acceso privilegiado	SI	A los empleados se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo. Estos privilegios son documentados y los empleados son agrupados bajo Perfiles de Usuario.
9.2.4	Gestión de información de autenticación secreta de usuarios	SI	La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
9.2.5	Revisión de los derechos de acceso de usuarios	SI	Es recomendable que el Jefe de la oficina de Sistemas y Cómputo junto a los empleados encargados verifiquen que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación se debe realizar de forma periódica y cualquier anormalidad debe ser debidamente documentada.
9.2.6	Retiro o ajuste de los derechos de acceso	SI	Es necesario que el jefe de la oficina de Sistemas y Cómputo verifique y elimine los permisos asignados al personal que sea retirado.

Núm.	Control	Aplicable	Justificación
9.3	Responsabilidades de los usuarios		
9.3.1	Uso de la información de autenticación secreta	SI	La información de autenticación del empleado en los sistemas y acceso a información es confidencial.
9.4	Control de acceso a sistemas y aplicaciones		
9.4.1	Restricción de acceso Información	SI	Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del trabajador en la organización.
9.4.2	Procedimiento de ingreso seguro	SI	Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.
9.4.3	Sistema de gestión de contraseñas	SI	Es recomendable que se implementen mecanismos de recuperación de contraseñas de forma automática y se garantice que la nueva contraseña del trabajador cumpla con los requisitos de seguridad expuestos en la Política de Seguridad.
9.4.4	Uso de programas utilitarios privilegiados	SI	Se recomienda que el jefe de la oficina de Sistemas y Cómputo verifique que a los sistemas y activos críticos sólo se les instalen los programas estrictamente necesarios y licenciados
9.4.5	Control de acceso a códigos fuente de programas	SI	El Jefe de la oficina de Sistemas y Cómputo verifica que los códigos fuentes de los programas permanecen de forma confidencial.
10	**Criptografía**		
10.1	Controles criptográficos		
10.1.1	Política sobre el uso de controles criptográficos	SI	Existe una política de seguridad que se encarga del uso de los controles criptográficos y justificación de los algoritmos de cifrado y su aplicación

Núm.	Control	Aplicable	Justificación
			en los servicios que la requieran.
10.1.2	Gestión de llaves	NO	
11	**Seguridad física y del entorno**		
11.1	Áreas seguras		
11.1.1	Perímetro de seguridad física	SI	Existe un perímetro físico, así como personal de seguridad.
11.1.2	Controles físicos de entrada	SI	Es recomendable que se implemente el control de acceso físico por medio de algún dispositivo como tarjetas inteligentes que permitan el acceso a sólo al personal autorizado y registren la fecha y hora de acceso.
11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	Las oficinas y lugares de trabajo claves están protegidas por medios físicos para controlar el acceso a personas no autorizadas.
11.1.4	Protección contra amenazas externas y ambientales	SI	Es recomendable que se implemente un plan de protección física contra desastres naturales, ataques maliciosos o accidentes.
11.1.5	Trabajo en áreas seguras	NO	
11.1.6	Áreas de despacho y carga	SI	Es necesario que implemente la creación de un área diseñada para recibir el descargue de los equipos y que impidan el acceso al interior de la oficina e infraestructura que contiene el hardware de las operaciones críticas.
11.2	Equipos		
11.2.1	Ubicación y protección de los equipos	SI	Es recomendable que los equipos se protejan físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc.

Núm.	Control	Aplicable	Justificación
11.2.2	Servicios de suministro	SI	Los servicios de suministros como energía, agua, ventilación y gas están acordes a la manufacturación de los equipos.
11.2.3	Seguridad del cableado	SI	El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.
11.2.4	Mantenimiento de equipos	SI	Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.
11.2.5	Retiro de activos	SI	El retiro de los equipos, eliminación de software e información sólo es realizada por el personal autorizado.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	NO	
11.2.7	Disposición segura o reutilización de equipos	SI	Se realiza un procedimiento seguro para la disposición o reutilización de equipos.
11.2.8	Equipos de usuario desatendidos	SI	Los usuarios son conscientes y aplican la seguridad apropiada (como protección del equipo con contraseñas) cuando el equipo está en desuso.
11.2.9	Política de escritorio limpio y pantalla limpia	SI	El jefe de la oficina de Sistemas y Cómputo garantiza que la información confidencial física es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.
12	**Seguridad de las operaciones**		
12.1	Procedimientos operacionales y responsabilidades		
12.1.1	Procedimientos de operación	SI	Es recomendable que el Jefe de la oficina de Sistemas y Cómputo y los

Núm.	Control	Aplicable	Justificación
	documentados		trabajadores documenten los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.
12.1.2	Gestión de cambios	SI	Los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.
12.1.3	Gestión de capacidad	SI	Se les realiza un monitoreo continuo a los recursos y la adquisición de los nuevos se proyecta de acuerdo a las necesidades críticas de la empresa.
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	El jefe de la oficina de Sistemas y Cómputo es el encargado de asegurar que los ambientes de desarrollo, pruebas y operación están debidamente separados y no pongan en riesgo la información.
12.2	Protección contra códigos maliciosos		
12.2.1	Controles contra códigos maliciosos	SI	Es recomendable que implementen un plan de capacitación y concientización a los trabajadores sobre la seguridad de la información y los riesgos a los que están expuestos los activos de la empresa, especialmente sobre el software de código malicioso.
12.3	Copias de respaldo		
12.3.1	Respaldo de información	SI	Las copias de seguridad se realizan a intervalos programados de forma manual, sólo por el personal autorizado.
12.4	Registro y seguimiento		
12.4.1	Registro de eventos	SI	Se mantienen los registros de los eventos ocurridos en los sistemas.
12.4.2	Protección de la información de registro	SI	Los registros de eventos están protegidos contra el acceso no autorizado.

Núm.	Control	Aplicable	Justificación
12.4.3	Registros del administrador y del operador	SI	Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
12.4.4	Sincronización de relojes	SI	Todos los sistemas están acordes y ajustados en una referencia de tiempo única y sincronizada.
12.5	Control de software operacional		
12.5.1	Instalación de software en sistemas operativos	SI	Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y software, que cumpla con las políticas de seguridad de la información.
12.6	Gestión de la vulnerabilidad técnica		
12.6.1	Gestión de las vulnerabilidades técnicas	SI	Existe una metodología de análisis y evaluación de riesgos.
12.6.2	Restricciones sobre la instalación de software	SI	Es recomendable que la instalación de software sea realizada sólo por el personal autorizado y con software probado y licenciado, además de otorgar el principio del menor privilegio.
12.7	Consideraciones sobre auditorias de sistemas de información		
12.7.1	Información controles de auditoría de sistemas	SI	Es necesario que las auditorías de los sistemas se acuerden, planeen y controlen sin interferir en el desarrollo normal de los procesos.
13	**Seguridad de las comunicaciones**		
13.1	Gestión de la seguridad de las redes		
13.1.1	Controles de redes	SI	Se recomienda que implementen una Infraestructura de Llave Pública (PKI) mediante algoritmos de cifrado que garanticen la confidencialidad e

Núm.	Control	Aplicable	Justificación
			integridad de la información que se transmite a través de las redes.
13.1.2	Seguridad de los servicios de red	SI	El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.
13.1.3	Separación en las redes	SI	Los usuarios y servicios están separados a través de dominios y VLANS.
13.2	Transferencia de información		
13.2.1	Políticas y procedimientos de transferencia de información	SI	Se recomienda la implementación y documentación sobre los procedimientos y controles a implementar para la transferencia segura de la información.
13.2.2	Acuerdos sobre transferencia de información	SI	Es recomendable que se documenten los acuerdos sobre los algoritmos de cifrado a utilizar para la transferencia de información que garanticen su confidencialidad e integridad.
13.2.3	Mensajería electrónica	SI	Es necesario que se implemente una Infraestructura de Llave Pública (PKI) mediante algoritmos de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	En los documentos y acuerdos contractuales de los trabajadores se estipula el compromiso con la confidencialidad de la información.
14	**Adquisición, desarrollo y mantenimientos de sistemas**		
14.1	Requisitos de seguridad de los sistemas de información		
14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	Existe una política que establece los requisitos relativos a la seguridad de la información para la adquisición de los nuevos equipos.

Núm.	Control	Aplicable	Justificación
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	SI	Se recomienda que implementen una Infraestructura de Llave Pública (PKI) mediante algoritmos de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	Se recomienda que implementen una Infraestructura de Llave Pública (PKI) mediante algoritmos de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
14.2	Seguridad en los procesos de desarrollo y soporte		
14.2.1	Política de desarrollo seguro	SI	Las políticas y controles de seguridad son aplicados en el desarrollo de software.
14.2.2	Procedimientos de control de cambios en sistemas	SI	El procedimiento formal de los cambios en el desarrollo de software es documentado para garantizar la integridad del sistema o aplicación.
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	Las aplicaciones y plataformas de operación son revisadas y probadas antes de implementarse.
14.2.4	Restricciones en los cambios a los paquetes de software	SI	Las modificaciones de software sólo se hacen a lo estrictamente necesario.
14.2.5	Principios de construcción de sistemas seguros	SI	Se establecen y documentan los principios de desarrollo de software seguro.
14.2.6	Ambiente de desarrollo seguro	SI	Los ambientes de desarrollo de software están protegidos de acceso no autorizado o de ejecución de software malicioso.
14.2.7	Desarrollo contratado externamente	NO	

Núm.	Control	Aplicable	Justificación
14.2.8	Pruebas de seguridad de sistemas	NO	
14.2.9	Prueba de aceptación de sistemas	SI	Es recomendable que se realicen pruebas de seguridad a los sistemas y se documenten los procedimientos.
14.3	Datos de prueba		
14.3.1	Protección de datos de prueba	SI	Los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.
15	**Relación con los proveedores**		
15.1	Seguridad de la información en las relaciones con los proveedores		
15.1.1	Política de seguridad de la información para las relaciones con proveedores	SI	Es necesario que se implemente una política de seguridad de la información relacionada con los proveedores.
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	SI	Es recomendable que se implementen acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	Es recomendable que se implementen acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
15.2	Gestión de la prestación de servicios con los proveedores		
15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	Es recomendable que se implementen acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.

Núm.	Control	Aplicable	Justificación
15.2.2	Gestión de cambios en los servicios de proveedores	SI	Es recomendable que se implementen acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
16	**Gestión de incidentes de seguridad de la información**		
16.1	Gestión de incidentes y mejoras en la seguridad de la información		
16.1.1	Responsabilidad y procedimientos	SI	Es recomendable que el jefe de la oficina de Sistemas y Cómputo y los trabajadores correspondientes tengan documentado los procesos y procedimientos para los incidentes de la seguridad de la información.
16.1.2	Reporte de eventos de seguridad de la información	SI	Los trabajadores están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados. Se establecen los procedimientos a seguir.
16.1.3	Reporte de debilidades de seguridad de la información	SI	Existen los formatos documentados disponibles para que los trabajadores reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el jefe de la oficina de Sistemas y Cómputo.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	Existen los formatos documentados disponibles para que los trabajadores reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el jefe de la oficina de Sistemas y Cómputo.
16.1.5	Respuesta a incidentes de seguridad de la información	SI	Se recomienda que el jefe de la oficina de Sistemas y Cómputo y los trabajadores correspondientes tengan documentado los procesos y procedimientos para los incidentes de la seguridad de la información.

Núm.	Control	Aplicable	Justificación
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	Los incidentes de la seguridad de la información son documentados especificando los riesgos, vulnerabilidades y amenazas, y los posibles controles de seguridad a implementar.
16.1.7	Recolección de evidencia	SI	Existen formatos y documentos para recolectar la evidencia y emitirlos a las autoridades correspondientes.
17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**		
17.1	Continuidad de seguridad de la información		
17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Es recomendable que el jefe de la oficina de Sistemas y Cómputo y los trabajadores correspondientes tengan documentado los procesos y procedimientos para la continuidad de la seguridad de la información.
17.1.2	Implementación de la continuidad de la seguridad de la información	SI	Se recomienda que el jefe de la oficina de Sistemas y Cómputo y los trabajadores correspondientes tengan documentado los procesos y procedimientos para la continuidad de la seguridad de la información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	Es necesario que el jefe de la oficina de Sistemas y Cómputo y los trabajadores correspondientes tengan documentado los procesos y procedimientos para la verificación, revisión y evaluación de la continuidad de seguridad de la información.
17.2	Redundancias		
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	SI	Es recomendable que se establezca la instalación e infraestructura disponible para el procesamiento de información.

Núm.	Control	Aplicable	Justificación
18	**Cumplimiento**		
18.1	Cumplimiento de requisitos legales y contractuales		
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
18.1.2	Derechos de propiedad intelectual	SI	Se definen las políticas y procedimientos para controlar la propiedad intelectual.
18.1.3	Protección de registros	SI	Es necesario que se clasifique de manera forma la confidencialidad de los registros.
18.1.4	Privacidad y protección de datos personales	SI	Existe una política relativa a la protección de datos personales conforme a los requerimientos de la ley.
18.1.5	Reglamentación de controles criptográficos	SI	Se recomienda que implementen una Infraestructura de Llave Pública (PKI) mediante algoritmos de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
18.2	Revisiones de seguridad de la información		
18.2.1	Revisión independiente de la seguridad de la información	SI	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información.
18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información con el fin de verificar el nivel de cumplimiento, controles y políticas de seguridad de la información.
18.2.3	Revisión del cumplimiento técnico	SI	Exista la documentación para la realización periódica de los test de

Núm.	Control	Aplicable	Justificación
			penetración y verificación de resultados e informes.

ANEXO Nº 9

APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA EL TRATAMIENTO DE RIESGOS

[D] DATOS/INFORMACIÓN

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
D_BCK	Copias de Seguridad de los Sistemas de Información	**E*, A***	R_D_BCK	**A**	**DC**	✓ D Protección de la Información. ✓ D.A Copias de seguridad de los datos (backup). ✓ D.C Cifrado de la información.	✓ A.8.2. ✓ A.12.3.1 ✓ A.10.1.
D_CNT	Contratos	**E*, A***	R_D_CNT	**M**	**DC**	✓ D.C Cifrado de la información. ✓ D.DS Uso de firmas electrónicas. ✓ D.I Aseguramiento de la integridad.	✓ A.10.1.
D_GUI	Guía de usuario	**E*, A***	R_D_GUI	**M**	**DC**	✓ D.A Copias de seguridad de los datos (backup).	✓ A.12.3.1
D_HCL	Historias Clínicas	**E*, A***	R_D_HCL	**M**	**DC**	✓ D.C Cifrado de la información. ✓ D.DS Uso de firmas	✓ A.10.1.

						electrónicas. ✓ D.I Aseguramiento de la integridad.	
D_HLB	Historial Laboral	**E*, A***	R_D_HLB	**M**	**DC**	✓ D.C Cifrado de la información. ✓ D.DS Uso de firmas electrónicas. ✓ D.I Aseguramiento de la integridad.	✓ A.10.1.
D_PUB	Publicaciones	**E*, A***	R_D_PUB	**MB**	**DC**	✓ D.A Copias de seguridad de los datos (backup).	✓ A.12.3.1
D_FPE	Formato de Préstamos de Equipos	**E*, A***	R_D_FPE	**B**	**DC**	✓ D.C Cifrado de la información. ✓ D.DS Uso de firmas electrónicas. ✓ D.I Aseguramiento de la integridad.	✓ A.10.1.
D_LOG	Registros de Actividad	**E*, A***	R_D_LOG	**A**	**DC**	✓ D Protección de la Información. ✓ D.C Cifrado de la información.	✓ A.8.2. ✓ A.10.1.
D_SRC	Códigos Fuentes	**E*, A***	R_D_SRC	**MA**	**DC**	✓ D Protección de la Información. ✓ D.C Cifrado de la información.	✓ A.8.2. ✓ A.10.1.

[S] SERVICIOS

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
S_MAI	Correo Electrónico	**E*, A***	R_S_MAI	**A**	**DC**	✓ S.email Protección del correo electrónico ✓ S.www Protección de servicios y aplicaciones web	✓ A.13.2.3 ✓ A.12.5.1
S_GID	Gestión de Identidades	**E*, A***	R_S_GID	**MA**	**DC**	✓ S.A Aseguramiento de la disponibilidad ✓ S.dir Protección del directorio ✓ S.SC Se aplican perfiles de seguridad	✓ A.17.1. ✓ A.8.2. ✓ A.9.4.3
S_INT	Servicios Internos	**E*, A***	R_S_INT	**MA**	**DC**	✓ S.A Aseguramiento de la disponibilidad ✓ S.dns Protección del servidor de nombres de dominio (DNS)	✓ A.17.1. ✓ A.9.4.
S_WWW	Páginas web de acceso publico	**E*, A***	R_S_WWW	**M**	**DC**	✓ S.A Aseguramiento de la disponibilidad ✓ S.www Protección de servicios y aplicaciones web	✓ A.17.1. ✓ A.12.5.1

[SW] SOFTWARE

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
SW_SWP	Software de Desarrollo Propio	**I*, E*, A***	R_SW_SWP	**MA**	**DC**	✓ SW Protección de las Aplicaciones Informáticas ✓ SW.A Copias de seguridad (backup) ✓ SW.SC Se aplican perfiles de seguridad ✓ SW.start Puesta en producción	✓ A.14.2. ✓ A.12.3.1
SW_MAI	Software para Correo Electrónico	**I*, E*, A***	R_SW_MAI	**MA**	**DC**	✓ SW Protección de las Aplicaciones Informáticas ✓ SW.SC Se aplican perfiles de seguridad	✓ A.14.2.
SW_DBS	Gestores de Bases de Datos	**I*, E*, A***	R_SW_DBS	**MA**	**DC**	✓ SW Protección de las Aplicaciones Informáticas ✓ SW.A Copias de seguridad (backup) ✓ SW.CM Cambios (actualizaciones y mantenimiento) ✓ SW.SC Se aplican perfiles de seguridad	✓ A.14.2. ✓ A.12.3.1

SW_OFM	Ofimática	**I*, E*, A***	R_SW_OFM	**B**	**DC**	✓ SW Protección de las Aplicaciones Informáticas ✓ SW.A Copias de seguridad (backup) ✓ SW.SC Se aplican perfiles de seguridad	✓ A.14.2. ✓ A.12.3.1
SW_AVS	Software de Antivirus	**I*, E*, A***	R_SW_AVS	**A**	**DC**	✓ SW Protección de las Aplicaciones Informáticas ✓ SW.SC Se aplican perfiles de seguridad	✓ A.12.2.1
SW_OPS	Sistemas Operativos	**I*, E*, A***	R_SW_OPS	**A**	**DC**	✓ SW Protección de las Aplicaciones Informáticas ✓ SW.A Copias de seguridad (backup) ✓ SW.SC Se aplican perfiles de seguridad	✓ A.14.2. ✓ A.12.3.1 ✓ A.12.2.1 ✓ A.12.5.1 ✓ A.12.6.

[HW] HARDWARE

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
HW_BCK	Dispositivo de Respaldo	**I*, E*, A***	R_HW_BCK	**MA**	**DC**	✓ HW Protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1

							✓ A.12.3.1
HW_FRW	Firewall	**I*, E*, A***	R_HW_FRW	**MA**	**DC**	✓ HW Protección de los Equipos Informáticos ✓ HW.A Aseguramiento de la disponibilidad ✓ HW.SC Se aplican perfiles de seguridad	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_ANT	Antenas	**I*, E*, A***	R_HW_ANT	**M**	**DC**	✓ HW Protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_HOS	Servidores	**I*, E*, A***	R_HW_HOS	**MA**	**DC**	✓ HW Protección de los Equipos informáticos ✓ HW.A Aseguramiento de la disponibilidad ✓ HW.SC se aplican perfiles de seguridad	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_PCM	Computadoras Portátiles de Uso Organizacional	**I*, E*, A***	R_HW_PCM	**M**	**DC**	✓ HW protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_PCP	Computadoras de Escritorio de Uso Organizacional	**I*, E*, A***	R_HW_PCP	**M**	**DC**	✓ HW protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1

HW_PRT	Impresoras	**I*, E*, A***	R_HW_PRT	**MB**	**AS**	✓ HW Protección de los Equipos Informáticos ✓ HW.print Reproducción de documentos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_LHD	Lector de huella digital	**I*, E*, A***	R_HW_LHD	**MB**	**AS**	✓ HW Protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_ROU	Router	**I*, E*, A***	R_HW_ROU	**A**	**DC**	✓ HW Protección de los Equipos Informáticos ✓ HW.A Aseguramiento de la disponibilidad ✓ HW.SC Se aplican perfiles de seguridad	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_SCN	Escáner	**I*, E*, A***	R_HW_SCN	**MB**	**AS**	✓ HW Protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_STR	Estabilizador	**I*, E*, A***	R_HW_STR	**MB**	**AS**	✓ HW Protección de los Equipos Informáticos	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1
HW_SWH	Switch	**I*, E*, A***	R_HW_SWH	**A**	**DC**	✓ HW Protección de los Equipos Informáticos ✓ HW.A Aseguramiento de la disponibilidad ✓ HW.SC Se aplican perfiles de seguridad	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1

HW_WAP	Puntos de Acceso inalámbrico	**I*, E*, A***	R_HW_WAP	**B**	**DC**	✓ HW Protección de los Equipos Informáticos ✓ HW.A Aseguramiento de la disponibilidad	✓ A.11.1.1 ✓ A.11.1.2 ✓ A.11.2.1

[COM] COMUNICACIONES

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
COM_INT	Internet	**E*, A***	R_COM_INT	**MA**	**DC**	✓ COM Protección de las Comunicaciones ✓ COM.A Aseguramiento de la disponibilidad ✓ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	✓ A.9.1.2 ✓ A.10.1.1 ✓ A.11.2.3 ✓ A.13.1. ✓ A.13.2.1 ✓ A.13.2.2
COM_LAN	Red de Área Local	**E*, A***	R_COM_LAN	**MA**	**DC**	✓ COM Protección de las Comunicaciones ✓ COM.A Aseguramiento de la disponibilidad ✓ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	✓ A.9.1.2 ✓ A.10.1.1 ✓ A.11.2.3 ✓ A.13.1. ✓ A.13.2.1 ✓ A.13.2.2

COM_WIF	Conectividad inalámbrica	**E*, A***	R_COM_WIF	**M**	**DC**	✓ COM Protección de las Comunicaciones ✓ COM.A Aseguramiento de la disponibilidad ✓ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados ✓ COM.wifi Seguridad Wireless (WiFi)	✓ A.9.1.2 ✓ A.10.1.1 ✓ A.13.1. ✓ A.13.2.1 ✓ A.13.2.2
COM_TEL	Línea telefónica	**E*, A***	R_COM_TEL	**B**	**DC**	✓ COM Protección de las Comunicaciones ✓ COM.A Aseguramiento de la disponibilidad ✓ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	✓ A.9.1.2 ✓ A.10.1.1 ✓ A.13.1. ✓ A.13.2.1 ✓ A.13.2.2

[AUX] EQUIPO AUXILIAR

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
AUX_RCK	Rack	**I*, E*, A***	R_AUX_RCK	**A**	**DC**	✓ AUX.A Aseguramiento de la disponibilidad ✓ AUX.AC Climatización ✓ AUX.power Suministro	✓ A.11.2.2 ✓ A.11.2.3

						eléctrico	✓ A.13.2.1
AUX_PWR	Fuente de Alimentación	**I*, E*, A***	R_AUX_PWR	**MA**	**DC**	✓ AUX.A Aseguramiento de la disponibilidad ✓ AUX.AC Climatización ✓ AUX.power Suministro eléctrico	✓ A.11.2.2 ✓ A.11.2.3 ✓ A.13.2.1
AUX_UPS	Sistema de Alimentación ininterrumpida (UPS)	**I*, E*, A***	R_AUX_UPS	**A**	**DC**	✓ AUX.A Aseguramiento de la disponibilidad ✓ AUX.AC Climatización ✓ AUX.power Suministro eléctrico	✓ A.11.2.2 ✓ A.11.2.3 ✓ A.13.2.1
AUX_WIR	Cableado Eléctrico	**I*, E*, A***	R_AUX_WIR	**MA**	**DC**	✓ AUX.A Aseguramiento de la disponibilidad ✓ AUX.power Suministro eléctrico ✓ AUX.wires Protección del cableado	✓ A.11.2.2 ✓ A.11.2.3 ✓ A.11.2.6 ✓ A.13.2.1

[L] INSTALACIONES

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
L_SIT	Empresa Agroindustrial Pomalca S.A.A.	**N*, I*, E*, A***	R_L_SIT	**A**	**AS**	✓ Instalaciones ✓ L.A Aseguramiento de la disponibilidad ✓ L.AC Control	✓ A.11.1. ✓ A.17.

[P] PERSONAL

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
P_ADM	Administrador de Sistema	**E*, A***	R_P_ADM	**MA**	**TT**	✓ PS Gestión del Personal ✓ PS.A Aseguramiento de la disponibilidad ✓ PS.AT Formación y concienciación	✓ A.7.

P_COM	Administrador de Comunicaciones	**E*, A***	R_P_COM	**MA**	**TT**	✓ PS Gestión del Personal ✓ PS.A Aseguramiento de la disponibilidad ✓ PS.AT Formación y concienciación	✓ A.7.
P_DBA	Administrador de Bases de Datos	**E*, A***	R_P_DBA	**MA**	**TT**	✓ PS Gestión del Personal ✓ PS.A Aseguramiento de la disponibilidad ✓ PS.AT Formación y concienciación	✓ A.7.
P_DES	Desarrollador de Software	**E*, A***	R_P_DES	**A**	**TT**	✓ PS Gestión del Personal ✓ PS.A Aseguramiento de la disponibilidad ✓ PS.AT Formación y concienciación	✓ A.7.
P_TEC	Responsable de soporte técnico	**E*, A***	R_P_TEC	**M**	**TT**	✓ PS Gestión del Personal ✓ PS.A Aseguramiento de la disponibilidad ✓ PS.AT Formación y concienciación	✓ A.7.