# UNIVERSIDAD TÉCNICA DE AMBATO


## FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

## MAESTRÍA EN GESTIÓN DE BASE DE DATOS III VERSIÓN

---

**TEMA:** Normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de las empresas de desarrollo de software, basada en la Norma Internacional ISO 27001.

---

Trabajo de Investigación, previo a la obtención del Grado Académico de Magíster en Gestión de Base de Datos

**Autora**: Ing. Gabriela María Quintanilla Guerrero

**Director:** Ing. Franklin Mayorga Mayorga, Mg.

Ambato – Ecuador

2018

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor de Trabajo de Investigación presidido por la Ingeniera Pilar Urrutia, Magister, e integrado por los señores Ingeniero Edison Homero Álvarez Mayorga, Magister., Clay Fernando Aldás Flores, Magister., Carlos Israel Núñez Miranda, Magister, designados por la Unidad Académica de Titulación de Posgrado de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS DATOS EN LOS SISTEMAS INFORMÁTICOS DE LAS EMPRESAS DE DESARROLLO DE SOFTWARE, BASADA EN LA NORMA INTERNACIONAL ISO 27001", elaborado y presentado por la señorita Ingeniera Gabriela María Quintanilla Guerrero, para optar por el Grado Académico de Magíster en Gestión de Bases de Datos; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Ingeniera Pilar Urrutia, Mg.
Presidente del Tribunal

Ing. Edison Homero Álvarez Mayorga, Mg.
Miembro del Tribunal

Ing. Clay Fernando Aldás Flores, Mg.
Miembro del Tribunal

Ing. Carlos Israel Núñez Miranda, Mg.
Miembro del Tribunal

## AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS DATOS EN LOS SISTEMAS INFORMÁTICOS DE LAS EMPRESAS DE DESARROLLO DE SOFTWARE, BASADA EN LA NORMA INTERNACIONAL ISO 27001, le corresponden exclusivamente a la Ingeniera Gabriela María Quintanilla Guerrero, autora bajo la Dirección del Ingeniero Franklin Mayorga Mayorga, Mg. Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ing. Gabriela María Quintanilla Guerrero
c.c.: 0604231449
**AUTORA**

Ing. Franklin Mayorga Mayorga, Mg.
c.c.: 1802503993
**DIRECTOR**

## DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Gabriela María Quintanilla Guerrero
c.c.: 0604231449

# ÍNDICE GENERAL DE CONTENIDOS

# ÍNDICE DE GRÁFICOS

# ÍNDICE DE CUADROS

# ÍNDICE DE TABLAS

**AGRADECIMIENTO**

A Dios, a mi familia.

A Nelson Fernando.

A la empresa de tecnologías STD S. A.

Al Ing. Franklin Mayorga.

Y a la Universidad Técnica de Ambato.

*Gabriela María Quintanilla Guerrero*

**DEDICATORIA**

A, Mariana, Verónica y Andrés

Por ser mi guía, mi apoyo incondicional y mi razón de vida.

*Gabriela María Quintanilla Guerrero*

**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL/DIRECCIÓN DE POSGRADO**

**MAESTRÍA EN GESTIÓN DE BASES DE DATOS**

**TEMA:**

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS DATOS EN LOS SISTEMAS INFORMÁTICOS DE LAS EMPRESAS DE DESARROLLO DE SOFTWARE, BASADA EN LA NORMA INTERNACIONAL ISO 27001.

**Autor:** Ing. Gabriela María Quintanilla Guerrero.
**Director:** Ing. Franklin Mayorga Mayorga, Mg.
**Fecha:** 24 de noviembre de 2017

## RESUMEN EJECUTIVO

La investigación Normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de las empresas de desarrollo de software, basada en la norma internacional ISO 27001 (ISO: Organización Internacional de Normalización), tiene como objetivo implementar directrices para gestionar todos los recursos que intervienen en el manejo de la información física y digital dentro de los entornos tecnológicos empresariales.

La Norma Internacional empleada para determinar las directrices de seguridad de la información en una empresa de desarrollo de software, es la ISO 27001:2013, que está organizada por 14 dominios (capítulos), 35 categorías y 114 criterios (controles), el planteamiento de la normativa determina los lineamientos que se deben aplicar en lo relativo a políticas de seguridad de la información, organización de la seguridad de la información, seguridad de los recursos humanos, gestión de activos, control de accesos, criptografía, seguridad física y ambiental, seguridad de las operaciones, seguridad en las comunicaciones, adquisición, desarrollo y mantenimientos de sistemas, relación con

proveedores, gestión de incidentes de seguridad de la información, aspectos de seguridad de la información dentro de la continuidad del negocio.

La seguridad de la información se consigue mediante la implementación de un conjunto de controles, que se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y del negocio de la empresa.

**Keywords:** ISO 27001:2013, Seguridad de la información, Vulnerabilidades, Criterios de seguridad, Directrices de seguridad, Sistemas informáticos, Protección de datos, Normativa de seguridad, Información, Sistemas de gestión de seguridad de la información.

**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL**

**MAESTRÍA EN GESTIÓN DE BASES DE DATOS**

**TEMA:**

INFORMATION SAFETY REGULATIONS FOR THE PROTECTION OF DATA IN COMPUTER SYSTEMS OF SOFTWARE DEVELOPMENT COMPANIES, BASED ON INTERNATIONAL STANDARD ISO 27001.

**Author:** Ing. Gabriela María Quintanilla Guerrero.
**Directed by:** Ing. Franklin Mayorga Mayorga, Mg.
**Date:** 24 de octubre de 2017

## EXECUTIVE SUMARY

The research Information security regulations for data protection in computer systems of software development companies, based on the international standard ISO 27001, aims to implement guidelines to manage all resources involved in the management of the physical and digital information within the technological technological environments.

The International Standard used to determine information security guidelines in a software development company is ISO 27001: 2013, which is organized by 14 domains (chapters), 35 categories and 114 criteria (controls), the regulations determine the guidelines to be applied in relation to information security policies, organization of information security, human resources security, asset management, access control, cryptography, physical and environmental security, security of operations, security in communications, acquisition, development and maintenance of systems, relationship with suppliers, management of information security incidents, security aspects of information within business continuity.

Information security is achieved through the implementation of a set of controls, which should be established, implemented, monitored, reviewed and improved, when necessary, to ensure that the company's specific security and business objectives are met.

**Descriptors:** ISO 27001: 2013, Information Security, Vulnerabilities, Security Criteria, Security Guidelines, Computer Systems, Data Protection, Security Regulations, Information, Information Security Management Systems.

## INTRODUCCIÓN

El desarrollo del presente proyecto de investigación está estructurado por capítulos, en los cuales constan definiciones y conceptos de los términos utilizados y los datos utilizados a lo largo de la investigación están presentados en tablas, gráficos, cuadros, a continuación, un resumen de cada capítulo:

El **capítulo I** denominado "**EL PROBLEMA DE INVESTIGACIÓN**", se describe el problema que es el objeto de la investigación, que contempla el tema de investigación, el planteamiento del problema, la contextualización macro, meso y micro, el análisis crítico, la prognosis, la formulación del problema, las interrogantes, la delimitación del objeto de investigación, la justificación y los objetivos generales y específicos.

El **capítulo II** denominado "**MARCO TEÓRICO**", está estructurado por los antecedentes de la investigación, la fundamentación filosófica y legal, las categorías fundamentales y el señalamiento de variables.

El **capítulo III** denominado "**METODOLOGÍA**", se describe el enfoque, la modalidad básica de investigación, nivel o tipo de investigación, la población y muestra, la operacionalización de variables, plan de recolección de información y el plan de procesamiento de la información

El **capítulo IV** denominado "**ANÁLISIS E INTERPRETACIÓN DE RESULTADOS**", se describe el análisis de resultados, la verificación de la prueba de hipótesis que se realizó utilizando el estadístico Chi – Cuadrado.

El **capítulo V** denominado "**CONCLUSIONES Y RECOMENDACIONES**", se presentan las conclusiones y recomendaciones de la investigación del problema planteado, están basados en la información y el análisis realizado en los capítulos anteriores.

El **capítulo VI** denominado "**DESARROLLO DE LA PROPUESTA**" (basada en la NORMA Internacional ISO 27001:2013, ISO 27002/2013), contempla la información detallada de la Normativa de Seguridad de la información; tema, datos informativos, antecedentes de la propuesta, la justificación, los objetivos, el análisis de factibilidad, la fundamentación científica y técnica, propuesta de la normativa que incluye las fases:

situación actual, diseño de la normativa de seguridad, haciendo énfasis en los criterios: políticas de desarrollo seguro, principios de construcción de sistemas seguros y ambiente de desarrollo seguro y la proyección de resultados por la aplicación de la normativa de seguridad.

Finalizando con los **Anexos**, que contiene la encuesta aplicada, la ficha de observación utilizada en la recolección de la información y procesamiento de la información de las encuestas por empresa.

# CAPÍTULO I

# EL PROBLEMA DE INVESTIGACIÓN

## 1.1. Tema de Investigación

Normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de las empresas de desarrollo de software basada en la Norma Internacional ISO 27001.

## 1.2. Planteamiento de problema

### 1.2.1. Contextualización

En la actualidad la Seguridad de la Información tiene más atención dentro de las organizaciones a nivel mundial; los gobiernos, las empresas públicas y privadas, y las personas están obligadas a tomar las medidas necesarias en materia de gestión de seguridad para los datos y la información, como principal activo para garantizar su permanecía en el sector donde actúan.

Según la Encuesta Global de Seguridad de la Información 2015 de PwC (PwC: Prince Waterhouse Coopers), en el período comprendido entre los años 2013 y 2014 hubo aproximado del 48% de la detección de incidentes de seguridad, que se vio reflejado en pérdidas financiera por fuga de información y nuevas inversiones en medidas para evitar incidentes relacionados a la seguridad. Empresas de países como Brasil y Francia son las más propensas a sufrir una violación de datos y empresas de países como Alemania y Canadá son las menos propensas a sufrir ataques. El número de registros corrompidos por incidentes en las empresas en el mismo período fue en aumento de 4300 a 88100, por lo que el tamaño promedio de una violación de datos o el número de registros perdidos o robados subió en un 2%. (Techtarget, 2015)

A nivel de Latinoamérica existen grandes abismos si se habla de seguridad de la información en la empresas, en el año 2012 los tipos de fallas de Seguridad de la Información más comunes fueron la manipulación de aplicaciones de software (15,55%), instalación de software no autorizado (50,55%), accesos no autorizados a la web (24,16%), fraudes (12,77%), virus (caballos de Troya, 43,88%), robo de datos (7,5), monitoreo no autorizado de tráfico (8,88%), negación de servicio (11,94%), pérdida de

integridad (12,77), pérdida/fuga de información crítica (10,55%), suplantación de identidad (9,72), phishing (22,77), pharming (4,16%), robos de hardware (20%), ingeniería social (11,94%), espionaje (3,05), ataques de aplicaciones web (18,05) y ninguno (111,66%); todas las fallas de seguridad se deben a que los empleados no tienen una cultura de seguridad de la información. Según la IV Encuesta Latinoamericana. (Rosero, 2015, pág. 9)

El Ecuador es uno de los países que está inmerso en este cambio hacia la seguridad de la información, es por eso que, las empresas del sector público y privado están tomando las medidas para proteger sus datos y su información.

Según Rosero (2015) afirma que "En Ecuador, para el año 2012 reporto ser uno de los países con mayor incidencia de malware en Latinoamérica con el 77,88% (tasa de infección de malware)" (pág. 11).

Encuesta ESET 2012, además se evidencia la falta de interés por optar a certificaciones basadas en seguridad de la información (falta de difusión y falta de conocimiento) para el personal del departamento de sistemas de las empresas, lo que les hace un país vulnerable con respecto a otros. Otro problema para la gestión de la información en las empresas ecuatorianas es la falta de apoyo e interés de la gerencia, por lo que uno de los principales desafíos es concienciar e involucrar a la gerencia en este campo, y también; cambiar la forma de pensar de los empleados en materia de seguridad de la información, para así poder alinear los objetivos del negocio con los de las Tecnologías de la Información (TI). (Rosero, 2015, pág. 13-14)

Por su parte, las empresas del sector tecnológico están conscientes de incrementar sus medidas de protección, sensatos de que su información es muy importante y es necesario asegurarla; pero lo que no hacen es destinar los recursos suficientes; en Ecuador solo la banca incrementa su presupuesto cada año, ya que la información que maneja es susceptible y la perdida de información traería problemas monetarios y legales. En el sector tecnológico, la seguridad de la información aun no es una realidad, por la falta de normativas para gestión de la seguridad de los datos y de la información, ya sea por el desconocimiento de los beneficios que los sistemas de gestión de seguridad de la información aportan a la empresa (certificación), falta de difusión de Normas de

Seguridad aplicadas en otros sectores y países, solo se cuenta con políticas de seguridad y privacidad internas básicas, planes de contingencia de riesgos muy generales que en muchas veces no se aplican.

Por lo que el propósito de implantar una normativa es, garantizar que los riesgos a los que están expuestos los datos sean conocidos, asumidos, gestionados y minimizados por la empresa de forma documentada, sistemática, estructurada, repetible, eficiente: VER GRÁFICO 1.

### 1.2.2. Análisis crítico

El bajo nivel de la seguridad de la información no garantiza la confidencialidad, integridad y confiabilidad de los datos, ya que en muchos casos las políticas de seguridad no son parte de los objetivos del negocio y tampoco están alineadas con dichos objetivos, por lo tanto, su cumplimiento en mucho de los casos es nulo. Una debilidad para toda organización es la falta de valoración de riesgos de seguridad a los que está expuesta la información lo que desemboca en una constante exposición a pérdidas y alteraciones no autorizadas. Además, en la definición de políticas para la seguridad, comúnmente no se tiene la participación activa toda la empresa, por lo que el desconocimiento, la falta de concienciación y apropiación en temas de seguridad de la información por parte de los actores (personal) es una debilidad que requiere atención inmediata, ya que también se constituye en una desventaja frente a las empresas que ya aplican modelos, metodologías, normativas nacionales e internacionales que favorezcan el crecimiento empresarial en ámbitos de seguridad de la información. Las casi nulas o pocas medidas de seguridad físicas y lógicas a los sistemas informáticos, bases de datos y demás activos, en un momento crítico pueden generar pérdidas económicas, afecciones legales, y hasta el quiebre de la empresa. Hoy en día la información es un activo estratégico para los negocios, su perdida, alteración y daños puede llegar a ser muy perjudicial; por lo que, las empresas del sector tecnológico deben proveer fuertes medidas de seguridad a fin de que los elementos utilizados para brindar sus servicios y desarrollar sus productos sean seguros y confiables. Normar y controlar la seguridad de la información empresarial en todo su ciclo de vida y formatos, se consigue con la implementación de medidas de seguridad preventivas, detectivas, de respuesta, de recuperación que contribuyan a garantizar la **confidencialidad, integridad y disponibilidad** de los datos en su estado

natural, que a su vez permitan dar cumplimientos a los objetivos empresariales, la incorporación de la Norma Internacional ISO 27001en la gestión de seguridad de la información garantiza el éxito y continuidad del negocio.

### 1.2.3. Prognosis

En el caso que no se tome una acción correctiva ocurrirá que: los datos estarán expuestos a ser vulnerables ante fallos de seguridad, lo que implica a las empresas pérdidas económicas, pérdidas reputacionales que finaliza con la quiebra de la organización.

### 1.2.4. Formulación del problema

¿La seguridad de la información incide en la protección de los datos de los sistemas informáticos de las empresas de desarrollo de software?

### 1.2.5. Interrogantes

**Pregunta 1:** ¿Cómo se gestiona la seguridad de la información de los sistemas informáticos de las empresas de desarrollo de software?

**Pregunta 2:** ¿Cuál es el nivel de confianza que determina la protección de los datos en las empresas de desarrollo de software?

**Pregunta 3:** ¿Se puede proponer una normativa de seguridad de la información para las empresas dedicadas al desarrollo de software?

### 1.2.6. Delimitación del objeto de investigación

**Campo:** Bases de datos
**Área:** Escalabilidad de las bases de datos.
**Aspecto:** Normativa para la seguridad de la información.

#### 1.2.6.1. Delimitación espacial

**Provincia:** Chimborazo

**Ciudad:** Riobamba

**Empresa:** Empresas de desarrollo de software

#### 1.2.6.2. Delimitación temporal

Junio 2017 – noviembre 2017

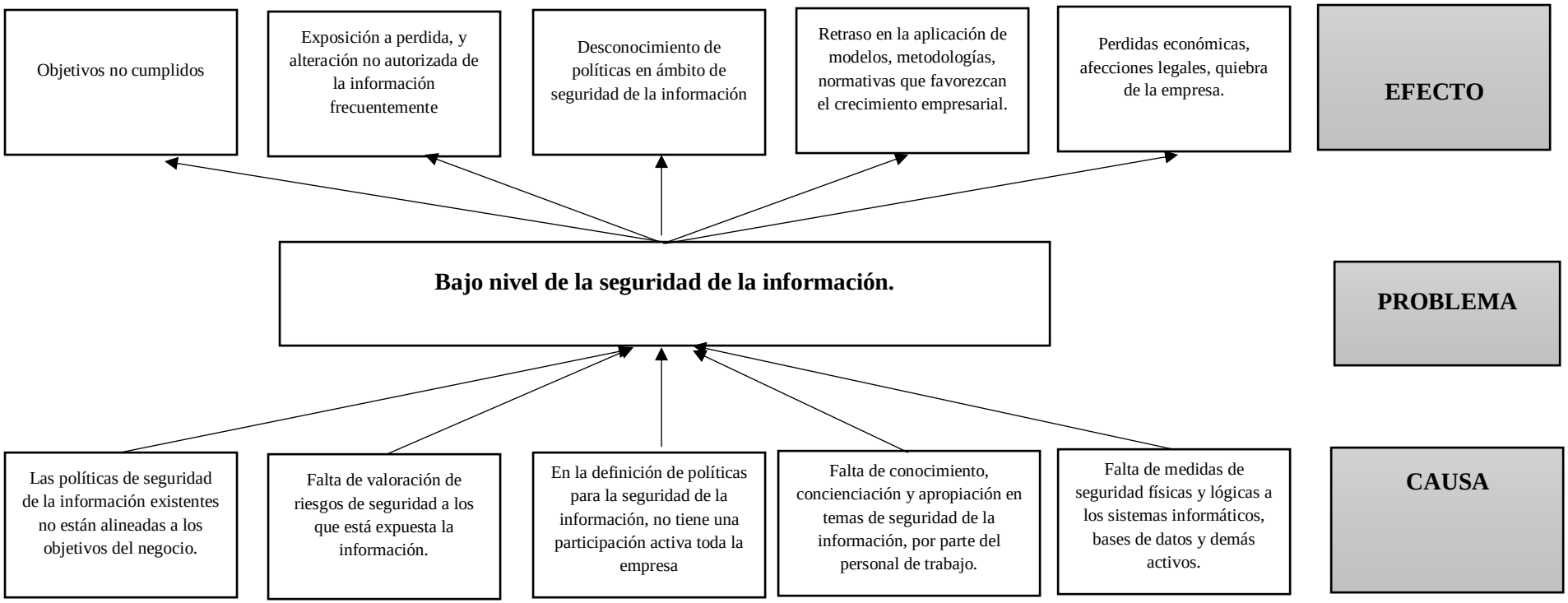



**Gráfico 1:** Árbol de problemas

**Elaborado por:** Investigador

## 1.3. Justificación

Tomando como base lo expuesto surge la necesidad que las empresas de desarrollo de software deban contar con normativas y/o sistemas de gestión de seguridad de la información, el cual permita administrar toda su información y datos, garantizando los aspectos de confidencialidad, integridad, disponibilidad que esta deba cumplir.

Se justifica así, la factibilidad de analizar, diseñar, desarrollar e implantar una normativa de seguridad de la información con la Norma Internacional ISO 27001:2013 (Sistemas de gestión de Seguridad de la Información) ayudando a minimizar los riesgos de daño, robo o fuga de información; su uso optimizará las garantías que las empresas ofrece en sus sistemas y procedimientos, lo que contribuye a generar más confianza en sus clientes y usuarios.

La implantación de una Normativa de Seguridad de la Información demuestra el compromiso de las empresas hacia la Seguridad de su activo más valioso (datos convertidos en información), además que proporciona las herramientas y elementos para alcanzar sus objetivos de seguridad de manera efectiva.

## 1.4. Objetivos

### Objetivo general

Implementar una normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de las empresas de desarrollo de software, basada en la Norma ISO 27001.

### Objetivos Específicos

- Analizar la situación referente a la seguridad de la información de las empresas de desarrollo de software.
- Establecer los parámetros de protección de la información para los sistemas informáticos de las empresas de desarrollo de software basado en la norma ISO 27001.
- Implementar una normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de la empresa de desarrollo de software (STD caso práctico).

# CAPÍTULO II

# MARCO TEÓRICO

## 2.1. Antecedentes de la Investigación

La seguridad de la información y la protección de los datos son temas de mayor importancia para entidades públicas y privadas, más aún para las empresas que hacen del manejo de la información digital su regla del negocio. Asegurar la integridad, disponibilidad y confidencialidad de los datos que se convierten en información por el tratamiento que se les da, es un reto para los especialistas informáticos; se evidencia la implantación de soluciones técnicas/legales y de calidad en las instituciones públicas**.**

Según (Guaman, 2015) en su trabajo de grado **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES MILITARES,** realizado en la Escuela Politécnica Nacional, facultad de Ingeniería de Sistemas, concluye que "Las Instituciones Militares, actualmente no disponen de un Sistema de Gestión de Seguridad de la Información para resguardar los activos de información que posee la institución, lo que dificulta mantener información de acuerdo a las normas de la ISO 27001:2005 " **y** "se estableció el diseño de un Sistema de Gestión de Seguridad de la información para Instituciones Militares; así como la identificación del riesgo, amenazas y vulnerabilidades; el cálculo del riesgo amenaza y vulnerabilidades; tratamiento de riesgo; revisión de riesgo y reevaluación de los riesgos de los activos de información de la Dirección de Tecnologías de la Información y Comunicaciones, lo que permitió aplicar para el diseño del SGSI la cláusula 4.2.1 de la norma 27001:2005 literales a) a la j)".

En el trabajo de titulación **DISEÑO DEL PLAN DE GESTIÓN DE SEGURIDADES DE LA INFORMACIÓN PARA CEPSA S.A.**, realizado en la Escuela Politécnica Nacional, facultad de Ingeniería de Sistemas, se afirma que "Las empresas más vulnerables son las que no poseen documentación y políticas de seguridad de la información, ya que hay varias vías por donde puede haber fugas de información, como durante el cambio de información, ya sea por medios físicos y electrónicos. Estos riegos pueden ser mitigados emitiendo una política para el intercambio de información. Las principales vulnerabilidades que posee una empresa es cómo sus empleados manejan la información por lo que es muy importante concienciar al

personal sobre la importancia de correcta gestión de la seguridad de la información". (Rosero, 2015)

La Secretaría Nacional de la Administración Pública (2014), en el proyecto titulado Implementación, Control y Seguimiento de la Seguridad de la Información en entidades de la Administración pública Central e Institucional, concluye que "Con relación a la Normativa y protocolos de Seguridad de la Información, el 61% de las instituciones no conoce la existencia de la familia de las Normas Técnicas Ecuatorianas INEN de Seguridad de la Información. El 70% de las instituciones no dispone de una política documentada de Gestión de Seguridad de la Información." (pág. 33)

## 2.2. Fundamentación Filosófica

La presente investigación se enmarca en el paradigma Crítico Propositivo, critico porque realiza un análisis crítico del problema y es propositivo porque busca poner una solución factible del problema.

## 2.3. Fundamentación Legal

En el VIII congreso Iberoamericano de Seguridad de la Información, se resaltó la importancia de la Seguridad de la Información para el gobierno ecuatoriano, dentro de su política de construir un Ecuador diferente, seguro, incluyente y equitativo, ha implementado cambios que motivan a la población hacia un mejor futuro. Una de las políticas consiste en que las instituciones públicas y privadas otorguen mayor atención a la protección de sus activos de información, con el fin de generar confianza en la ciudadanía y minimizar los riesgos derivados de vulnerabilidades informáticas. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2011)

En la constitución del Ecuador, en el artículo 4 de la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los datos personales del Sistema Nacional de Registro de Datos Públicos se establece que "las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos público, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo".

El Acuerdo Ministerial N°. 166, publicado mediante Registro Oficial N°. 88 del 25 de septiembre de 2013, dispone que las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva, la implementación del Esquema Gubernamental de Seguridad de la información EGSI, Norma Técnica Ecuatoriana INEN ISO/IEC 27002 "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información". En concordancia con el Plan de Gobierno Electrónico 2014-2017 del Ecuador, el EGSI es un instrumento de vital importancia para todos los actores del Plan Nacional: ciudadanos, servidores, empresas y gobierno y otros actores del estado. (Agencia de Control y Regulación de Electricidad, 2013)

## 2.4. Categorías fundamentales

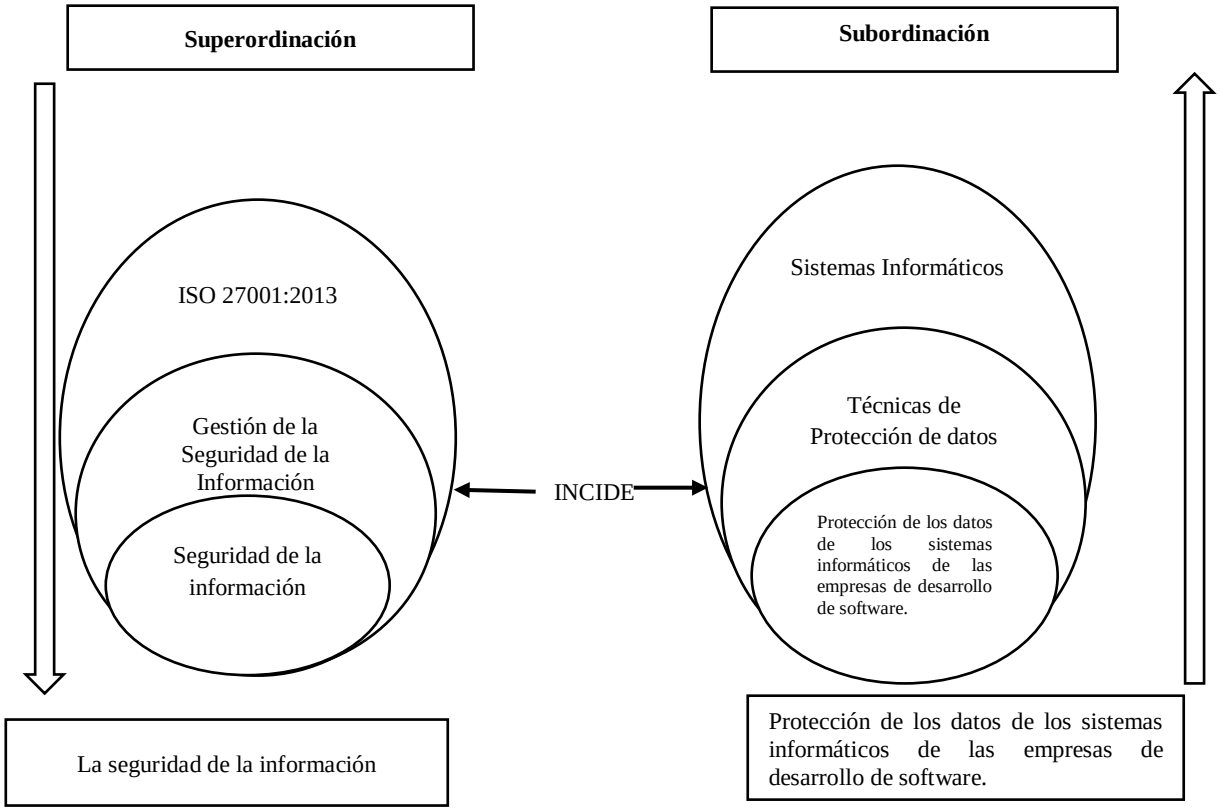



**Gráfico 2:** Superordinación conceptual

**Elaborado por:** Investigador

**Constelación de Ideas Variable Independiente**

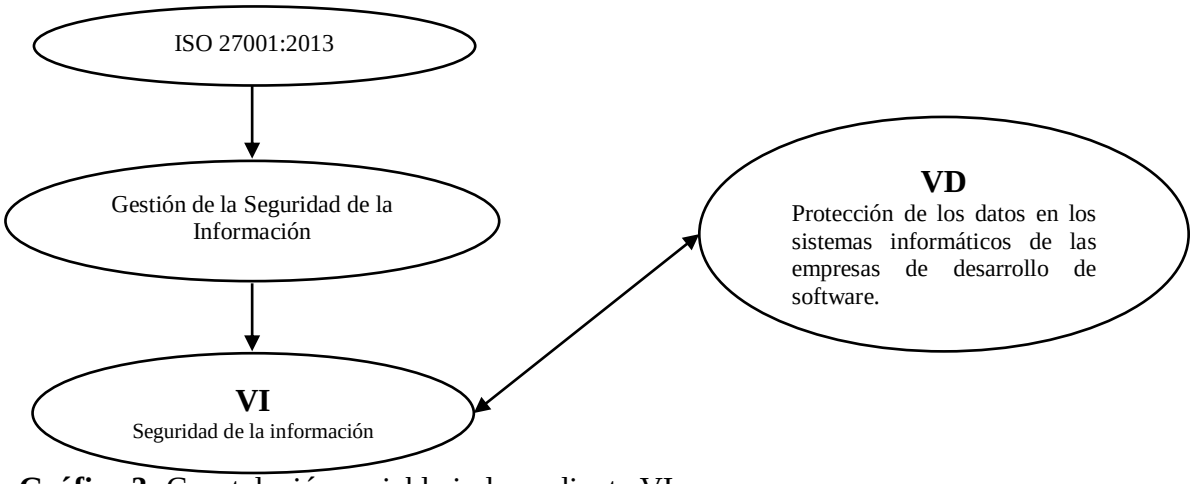



**Gráfico 3:** Constelación variable independiente VI.

**Elaborado por:** Investigador

**Constelación de Ideas Variable Dependiente**

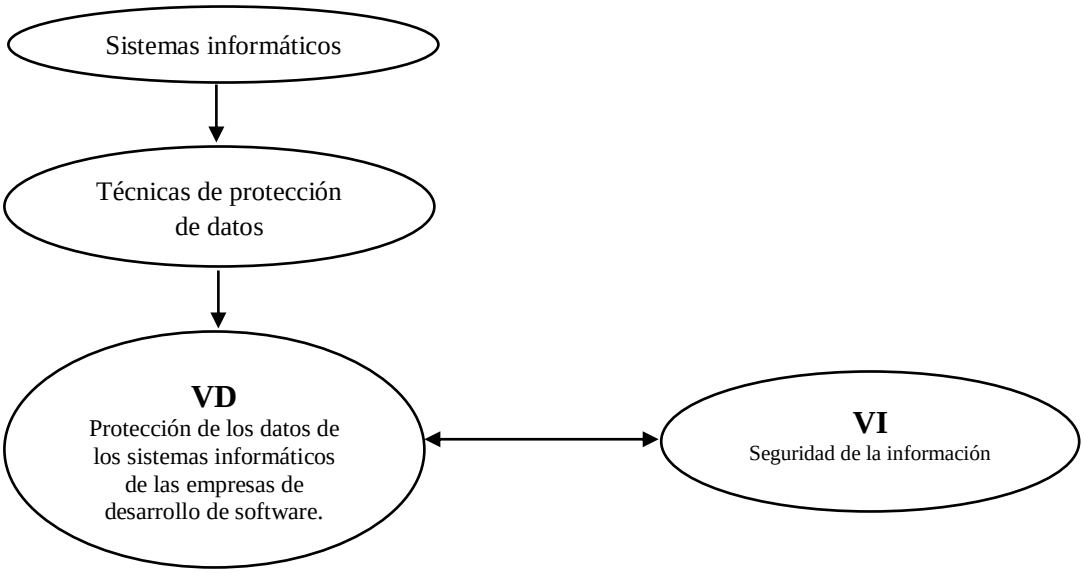



**Gráfico 4:** Constelación variable dependiente VD

**Elaborado por:** Investigador

## 2.5. Hipótesis

La seguridad de la información SI incide en la protección de los datos de los sistemas informáticos de las empresas de desarrollo de software.

## 2.6. Señalamiento de variables

**Variable independiente:** La seguridad de la información.

- **La seguridad de la información:** es una disciplina de reciente aparición que trata de la protección de la información frente a revelaciones accidentales o intencionales, a usuarios no autorizados, frente a modificaciones indebidas o frente a destrucciones.
- **Ámbitos de la seguridad de la información:** Integridad, disponibilidad, confidencialidad y el control de accesos:

  **Confidencialidad:** es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. (Guindel, 2009, pág. 20)

  **Integridad:** que la información permanezca exacta y completa. (Guindel, 2009, pág. 20)

  **Disponibilidad:** que solo los usuarios autorizados puedan utilizar la información en la forma y tiempo previstos. (Guindel, 2009, pág.20)
- **Medidas de seguridad de la información:** las medidas de protección pueden ser de prevención, de detección, de corrección y de recuperación; que se constituyen en medidas técnicas, administrativas y organizativas, y físicas.

  **Medidas de seguridad técnicas:** se materializan en mecanismos que se implementan en el interior de los sistemas de información y tratan de contrarrestar las amenazas que desde dentro de los sistemas acechan a los programas y datos.

  **Medidas de seguridad administrativas y organizativas:** se instrumentan mediante reglas y procedimientos que involucran a gestores que dictan las normas y pautas de alto nivel que incumben a la seguridad, técnicos que formulan los procedimientos que se deducen de las anteriores y usuarios responsables de cumplirlas; por lo tanto, son medidas que se refieren a la gestión de la seguridad.

  **Medidas de seguridad físicas:** pretenden proteger los equipos de amenazas provenientes del medio natural, del entorno operativo o y acciones humanas (incendios, inundaciones, hurtos de soporte y equipos, sabotajes materiales, cortes de fluido eléctrico, etc.).

- **Sistemas de gestión de seguridad de la información:** el SGSI (Sistema de gestión de seguridad de la información) es el concepto central sobre el que se construye ISO 27001.

  La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, además que podría considerarse, por analogía con una norma conocida como ISO 9001, como sistema de calidad para la seguridad de la información. (ISO 27000).

  El modelo ISO 27001:005 define a un Sistema de Gestión de Seguridad de la información como ***la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.*** (ISO/IEC 27001:2005. Estándar Internacional. Tecnología de la información - Técnicas de Seguridad de la información – Requerimientos)

  **ISO/IEC 27002:2013:** Esta norma internacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Información (SGSI) basado en la Norma ISO/IEC 27001 (IEC: Comisión Electrónica Internacional) o bien como un documento guía para organizaciones que implementen controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de seguridad de la información en industria y organizaciones específicas, teniendo en cuenta sus entornos específicos de riesgo de seguridad de la información. (Asociación Española de Normalización y Certificación, 2015)

**Variable dependiente:** Protección de los datos en los sistemas informáticos de las empresas de desarrollo de software.

**Protección de los datos:** Trata de mantener el derecho de los individuos/objetos y actores a determinar cuándo, cómo, a quién, qué y para qué información sobre ellos puede ser cedida a terceros.

- **Técnicas de protección de datos:** autenticación, control de acceso, cifrado de datos, registros de auditorías y borrado seguro.
- **Sistemas informáticos de las empresas de desarrollo de software:** Conjunto de soluciones tecnológicas dedicadas a resolver problemas de la sociedad, mediante la automatización de procesos manuales y mediante la utilización de software y hardware que ofrecen las mejores prestaciones para cumplir con los objetivos empresariales.

# CAPÍTULO III

# METODOLOGÍA

## 3.1. Modalidad básica de investigación

Las modalidades básicas de investigación serán bibliográficas y de campo.

La investigación será bibliográfica por que utilizará fuentes como: libros, revistas, documentos, artículos para la construcción de marco teórico acerca de la seguridad de la información y de la protección de los datos los sistemas informáticos de las empresas de desarrollo de software.

La investigación también tendrá la modalidad de campo porque se buscará obtener la información de la variable independiente: Seguridad de la información y de la variable dependiente: Protección de los datos de los sistemas informáticos de las empresas de desarrollo de software, en el mismo lugar que ocurre.

## 3.2. Nivel o tipo de investigación

Experimental porque se va obtener información por medio de la observación de los hechos.

La investigación será de nivel exploratoria porque se va analizar los problemas fundamentales de la Seguridad de la Información y su incidencia en la protección de los datos de los sistemas informáticos de las empresas de desarrollo de software.

La investigación será descriptiva porque se utilizará métodos para describir los datos y las características de la población de estudio. Además, será explicativa porque se encontrará las razones para determinar el nivel de confianza que determina la protección de los datos en las empresas de desarrollo de software, utilizando el método deductivo.

También es correlacional porque buscara medir el grado de relación entre la variable independiente: La seguridad de la información y de la variable dependiente: protección de los datos de los sistemas informáticos de las empresas de desarrollo de software.

### 3.3. Población y muestra

El proyecto trabajara con la población de 3 empresas dedicadas al desarrollo de software:

| EMPRESA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| Empresa 3 | 5 | 22,73 % |
| Empresa 2 | 5 | 22,73 % |
| Empresa 1 | 12 | 54,54 % |
| **TOTAL** | **3** | **100%** |

**Cuadro N° 1:** Población
**Elaborado por:** Investigador

No se trabajará con una muestra, directamente con la población.

### 3.4. Operacionalización de variables

VER CUADRO N° 3 y CUADRO N° 4

### 3.5. Plan de recolección de información

| PREGUNTAS BÁSICAS | EXPLICACIÓN |
|---|---|
| ¿Para qué? | Para analizar los objetivos del a investigación. |
| ¿De qué personas u objetos? | Personal encargado del proceso. |
| ¿Sobre qué aspectos? | Sobre los indicadores expuestos en la matriz. |
| ¿Quién, Quiénes? | Gabriela María Quintanilla Guerrero |
| ¿Cuándo? | Tercer trimestre del 2017 |
| ¿Dónde? | Riobamba, Empresas de desarrollo de Software. |
| ¿Cuántas veces? | Una |
| ¿Qué técnicas de recolección? | Encuesta/Observación/Revisión de documentos |
| ¿Con qué? | Cuestionario/Guía de Entrevista/Inspecciones |
| ¿En qué situación? | En el momento del proceso. |

**Cuadro N° 2:** Recolección de la Información
Elaborado por: Investigador

### 3.6. Plan de procesamiento de la información

1) Revisión crítica de la información recogida; es decir, limpieza de la información defectuosa: contradictoria, incompleta, no pertinente, etc.
2) Repetición de la recolección, para corregir fallas de contestación.
3) Tabulación o cuadros según variables de cada hipótesis: cuadros de una sola variable, cuadro con cruce de variables, etc.
4) Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente, que no influyen significativamente en los análisis).

**Variable independiente: Seguridad de la información**

| CONCEPTUALIZACIÓN | DIMENSIONES | INDICADORES | ITEMS BÁSICOS | TÉCNICAS E INSTRUMENTOS |
|---|---|---|---|---|
| **La seguridad de la información:** es una disciplina de reciente aparición, que hace referencia a la confidencialidad, integridad y disponibilidad de la información y datos independientemente de la forma que los datos puedan tener. (Ribagorda , 2008) | Confidencialidad de la información.<br><br>Integridad de la información.<br><br>Disponibilidad de la información.<br><br>Trazabilidad de la información. | Efectividad de los procedimientos de confidencialidad.<br>Eficiencia de los procedimientos de confidencialidad.<br><br>Precisión<br>Validez<br>Coherencia<br>Calidad<br><br>Garantizar su almacenamiento<br>Garantizar su accesibilidad<br>Garantizar su mantenimiento | ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?<br>¿El computador asignado para el desarrollo de sus funciones posee un antivirus?<br>¿La empresa posee software legal en su totalidad?<br>¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado?<br>¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa?<br>¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información?<br>¿La empresa capacita al personal en temas de seguridad de la información?<br>¿Existe algún control para navegar en internet?<br>¿Existe control sobre el uso del correo electrónico?<br>¿Existe alguna política para el cambio regular de las contraseñas?<br>¿Antes y después de la contratación del personal se hace entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información?<br><br>¿La información disponible en los repositorios de datos se mantiene exacta?<br><br>¿La información disponible en los repositorios de datos es completa?<br><br>¿La información solo está disponible para accesos autorizados? | Encuesta – Guía de encuesta<br>Dirigido a profesionales de Tecnologías de la información y comunicación: directores de proyectos.<br>Supervisores de proyectos.<br>Desarrolladores de software.<br>Administradores de bases de datos.<br>Técnicos de comunicaciones. |

| | | | | |
|---|---|---|---|---|
| | Autenticidad de la información. | Eficiencia de los procedimientos de trazabilidad.<br><br>Veracidad<br>Exactitud<br>Autenticidad | ¿Se garantiza el almacenamiento de la información?<br><br>¿Se garantiza el acceso oportuno hacia la información?<br><br>¿La información está disponible para actualizaciones constantes?<br>¿Se identifica quién realiza cambios en la información?<br>¿Se conoce en qué momento se cambió la información?<br>¿El contenido de la información que está disponible es comprobable?<br><br>¿La información disponible es verdadera?<br><br>¿Se realiza respaldos de los datos?<br><br>¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?<br><br>¿Existen zonas restringidas de acceso de personal?<br><br>¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?<br><br>¿Se cuenta con sistemas de alarma como detectores de humo, humedad?<br><br>¿Existe vigilancia en la entrada del edificio? | |

**Cuadro N° 3:** Operacionalización de la variable independiente
**Elaborado Por:** Investigador

**Variable dependiente: Protección de los datos de los sistemas informáticos de la empresa de desarrollo de software**

| CONCEPTUALIZACIÓN | DIMENSIONES | INDICADORES | ITEMS BÁSICOS | TÉCNICAS E INSTRUMENTOS |
|---|---|---|---|---|
| **Protección de los datos de los sistemas informáticos de las empresas de desarrollo de software:** Es el conjunto de procesos que prevalecen para proteger el activo más importante empresarial que son los datos; mantener su estado natural y legalmente constituido dentro de los sistemas existentes. (Investigador, 2017) | **Políticas de seguridad de la información.** | Directrices establecidas por la dirección para la seguridad de la información. | Políticas para la seguridad de la información.<br>Revisión de políticas para la seguridad de la información. | Ficha de observación. |
| | **Organización de la seguridad de la información.** | Organización interna | Roles y responsabilidades para la seguridad de la información.<br>Separación de deberes.<br>Contacto con las autoridades.<br>Contacto con grupos de interés especial.<br>Seguridad de la información en la gestión de proyectos. | |
| | | Dispositivos móviles y teletrabajo. | Políticas para dispositivos móviles.<br>Teletrabajo. | |
| | **Seguridad de los recursos humanos.** | Antes de asumir el empleo.<br>Durante la ejecución del empleo. | Selección.<br>Términos y condiciones de empleo.<br>Responsabilidades de la dirección.<br>Toma de conciencia, educación y formación en la seguridad de la información.<br>Proceso disciplinario. | |
| | | Terminación o cambio de empleo. | Terminación o cambio de responsabilidades de empleo. | |
| | **Gestión de Activos** | Responsabilidad por los activos. | Inventario de activos.<br>Propiedad de los activos.<br>Uso aceptable de los activos.<br>Devolución de los activos. | |
| | | Clasificación de la información. | Clasificación de la información.<br>Etiquetado de la información.<br>Manejo de activos | |

| | | | | |
|---|---|---|---|---|
| | | | Gestión de medios removibles.<br>Disposición de los medios.<br>Transferencia de medios físicos. | |
| | **Control de Accesos** | Requisitos del negocio para el control de acceso. | Política de control de acceso.<br>Política sobre el uso de los servicios de red. | |
| | | Gestión de accesos de usuarios. | Registro y cancelación del registro de usuarios.<br>Suministro de acceso de usuarios.<br>Gestión de derechos de acceso de privilegiado.<br>Gestión de información de autenticación secreta de usuarios.<br>Revisión de los derechos de acceso de usuarios.<br>Retiro o ajuste de los derechos de acceso. | |
| | | Responsabilidad de los usuarios. | Uso de la información de autenticación secreta. | |
| | | Control de acceso a sistemas y aplicaciones. | Restricción de acceso a la información.<br>Procedimiento de ingreso seguro.<br>Sistemas de gestión de contraseñas.<br>Uso de programas utilitarios privilegiados.<br>Control de acceso a código fuente de programas. | |
| | **Criptografía** | Controles criptográficos | Política sobre el uso de controles criptográficos.<br>Gestión de llaves. | |
| | **Seguridad Física y Ambiental** | Áreas seguras | Perímetro de seguridad física.<br>Controles físicos de entrada.<br>Seguridad de oficinas, recintos e instalaciones.<br>Protección contra amenazas externas y ambientales.<br>Trabajo en áreas seguras.<br>Áreas de despacho y carga. | |
| | | Equipos | Ubicación y protección de los equipos.<br>Servicios de suministro.<br>Seguridad de cableado.<br>Mantenimiento de equipos. | |

| | | | | |
|---|---|---|---|---|
| | | | Retiro de activos.<br>Seguridad de equipos y activos fuera de las instalaciones.<br>Disposición segura o reutilización de equipos.<br>Equipos de usuarios desatendidos.<br>Política de escritorio limpio y pantalla limpia. | |
| | | Procedimientos operaciones y responsabilidades. | Procedimientos de operación documentados.<br>Gestión de cambios.<br>Gestión de capacidad.<br>Separación de los ambientes de desarrollo, pruebas y operación. | |
| | **Seguridad de las Operaciones** | Protección contra códigos maliciosos. | Controles contra códigos maliciosos. | |
| | | Copias de respaldo. | Respaldos de información. | |
| | | Registro y seguimiento. | Registro de eventos.<br>Protección de la información de registro.<br>Registros del administrador y del operador.<br>Sincronización de relojes. | |
| | | Control de software operacional. | Instalación de software en sistemas operativos. | |
| | | Gestión de la vulnerabilidad técnica. | Gestión de las vulnerabilidades técnicas.<br>Restricciones sobre la instalación de software. | |
| | | Consideraciones sobre auditorias de sistemas de información. | Información controles de auditoria de sistemas. | |
| | | Gestión de la seguridad de las redes. | Controles de redes.<br>Seguridad de los servicios de red.<br>Separación en las redes. | |
| | | Transferencia de información. | Políticas y procedimientos de transferencia de información. | |

| | | | | |
|---|---|---|---|---|
| | | | Acuerdos sobre transferencia de información.<br>Mensajería electrónica.<br>Acuerdos de confidencialidad o de no divulgación. | |
| | **Seguridad en las comunicaciones** | Requisitos de seguridad de los sistemas de información. | Análisis y especificación de requisitos de seguridad de la información.<br>Seguridad de servicios de las aplicaciones en redes públicas.<br>Protección de transacciones de los servicios de las aplicaciones. | |
| | **Adquisición, desarrollo y mantenimientos de sistemas** | Seguridad en los procesos de desarrollo y soporte. | Política de desarrollo seguro.<br>Procedimientos de control de cambios en sistemas.<br>Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.<br>Restricciones en los cambios a los paquetes de software.<br>Principios de construcción de sistemas seguros.<br>Ambiente de desarrollo seguro.<br>Desarrollo contratado externamente.<br>Pruebas de seguridad de sistemas.<br>Pruebas de aceptación de sistemas. | |
| | | Datos de prueba | Protección de datos de prueba. | |
| | **Relación con proveedores** | Seguridad de la información en las relaciones con los proveedores. | Política de seguridad de la información para las relaciones con los proveedores.<br>Tratamiento de la seguridad dentro de los acuerdos con proveedores.<br>Cadena de suministro de tecnología de información y comunicación. | |
| | | Gestión de la prestación de servicios con los proveedores. | Seguimiento y revisión de los servicios de los proveedores.<br>Gestión de cambios en los servicios de proveedores. | |
| | | Gestión de incidentes y mejoras en la seguridad de la información. | Responsabilidad y procedimientos.<br>Reporte de eventos de seguridad de la información.<br>Reporte de debilidades de seguridad de la información. | |

| | | | | |
|---|---|---|---|---|
| | | | Evaluación de eventos de seguridad de la información y decisiones sobre ellos.<br>Respuesta a incidentes de seguridad de la información.<br>Aprendizaje obtenido de los incidentes de seguridad de la información.<br>Recolección de evidencia. | |
| | **Gestión de incidentes de seguridad de la información** | Continuidad de seguridad de la información. | Planificación de la continuidad de la seguridad de la información.<br>Implementación de la continuidad de la seguridad de la información.<br>Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | |
| | | Redundancias. | Identificación de la legislación aplicable y los requisitos contractuales.<br>Derechos de propiedad intelectual.<br>Protección de registros.<br>Privacidad y protección de datos personales.<br>Reglamentación de controles criptográficos. | |
| | **Aspectos de seguridad de la información dentro de la continuidad del negocio.** | Revisión de seguridad de la información. | Revisión independiente de la seguridad de la información.<br>Cumplimiento con las políticas y normas de seguridad.<br>Revisión del cumplimiento técnico. | |

**Cuadro N° 4:** Operacionalización de la variable dependiente
**Elaborado por:** Investigador

# CAPÍTULO IV

# ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

## 4.1. Análisis e interpretación de los resultados

El análisis y la interpretación de resultados, se considera a partir de la encuesta realizada a 22 profesionales de TICs (TICs: Tecnologías de la información y comunicación) de las empresas de desarrollo de software, y su aplicación generó la siguiente información:

**Pregunta 1.** ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?

**Tabla 1:** Resultados de la Pregunta 1

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 11 | 11 | 22 |
| **Porcentaje (%)** | 50 % | 50 % | 100% |

**Elaborado por:** Investigador

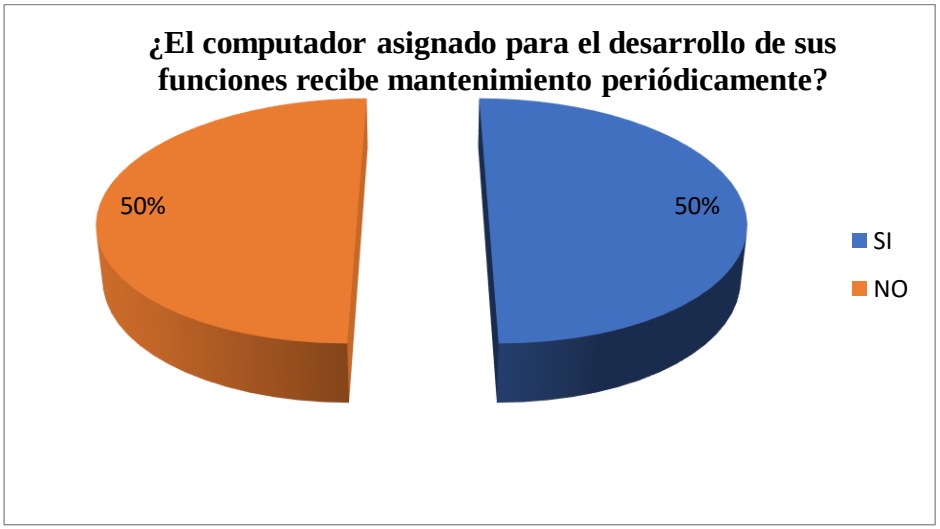



**Gráfico 5:** Pregunta 1
**Elaborado por:** Investigador

**Interpretación:** De un total de 22 encuestas realizadas, se evidencia que 11 encuestados afirman que el computador asignado para el desarrollo de sus funciones SI recibe mantenimiento periódicamente. Mientras que los 11 encuestados restantes afirman que el computador asignado para el desarrollo de sus funciones NO recibe mantenimiento periódicamente.

**Análisis:** Se concluye que en las empresas de desarrollo de software el mantenimiento periódico de los equipos de cómputo es regular.

**Pregunta 2:** ¿El computador asignado para el desarrollo de sus funciones posee un antivirus?

**Tabla 2:** Resultados de la Pregunta 2

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 21 | 1 | 22 |
| **Porcentaje (%)** | 95,45 % | 4,55 % | 100% |

**Elaborado por:** Investigador


**Gráfico 6:** Pregunta 2
**Elaborado por:** Investigador

**Interpretación:** De un total de 22 encuestados, 21encuestados afirma que el computador asignado para el desarrollo de sus funciones SI posee un antivirus.

**Análisis:** Se concluye que las empresas de desarrollo de software cuentan con la protección de software antivirus para sus equipos y para la información.

**Pregunta 3:** ¿La empresa posee software legal en su totalidad?

**Tabla 3:** Resultados de la Pregunta 3

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 4 | 18 | 22 |
| **Porcentaje (%)** | 18,18 % | 81,82 % | 100 % |

**Elaborado por:** Investigador

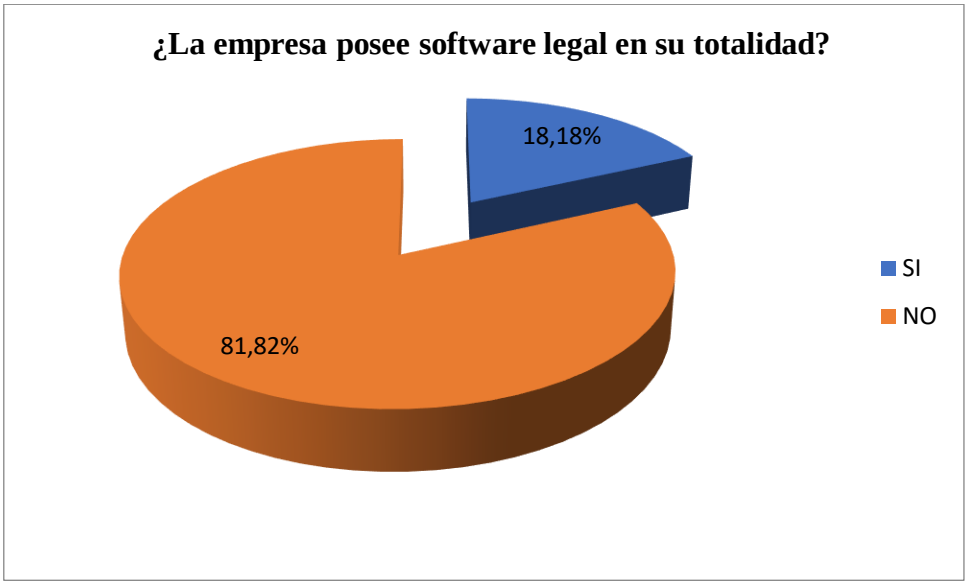



**Gráfico 7:** Pregunta 3
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que, de 22 encuestados, 18 encuestados afirman que en la empresa la totalidad del software no es legal y 4 encuestados afirman que la empresa si posee software legal en su totalidad.

**Análisis:** Se evidencia que las empresas aun no conocen los riesgos al adquirir, descargar, reproducir, instalar y utilizar software sin licencia, demostrando que existe una pobre valoración de las consecuencias técnicas, financieras y legales a las que están expuestas por el uso ilícito de estos productos.

**Pregunta 4:** ¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado?

**Tabla 4:** Resultados de la Pregunta 4

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 12 | 10 | 22 |
| **Porcentaje (%)** | 54,55 % | 45,45 % | 100 % |

**Elaborado por:** Investigador

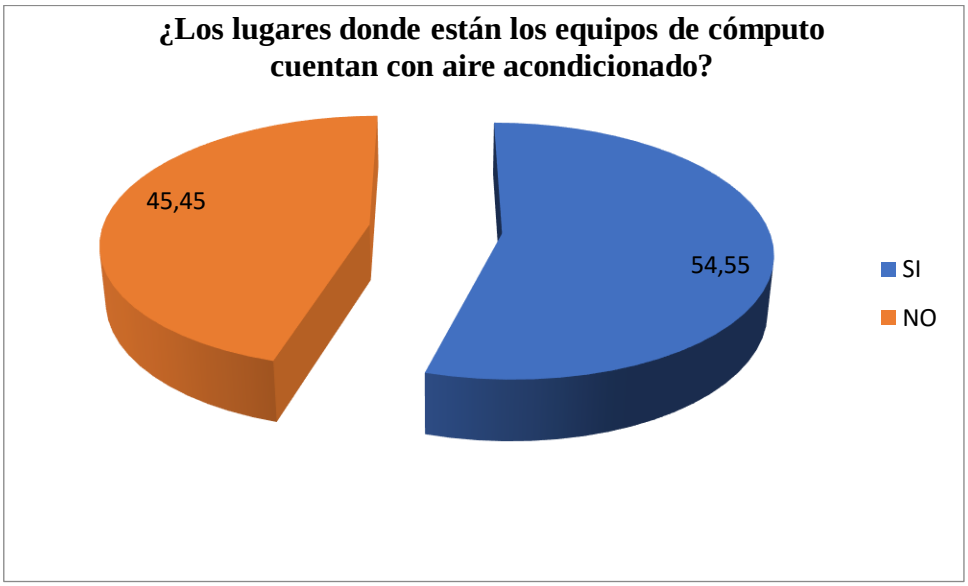



**Gráfico 8:** Pregunta 4
**Elaborado por:** Investigador

**Interpretación:** En un total de 22 encuestados, 12 afirman que los equipos de cómputo en la empresa donde laboran SI cuentan con aire acondicionado, mientras tanto 10 encuestados afirman que NO cuentan con aire acondicionado en el lugar donde está su equipo de cómputo asignado para su trabajo.

**Análisis:** De forma parcial las empresas de desarrollo de software proporcionan soluciones de enfriamiento para sus equipos; en parte cuentan con un diseño, instalación y funcionamiento de un sistema de enfriamiento para mantener la temperatura adecuada de los equipos tecnológicos.

**Pregunta 5:** ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa?

**Tabla 5:** Resultados de la Pregunta 5

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 11 | 11 | 22 |
| **Porcentaje (%)** | 50 % | 50 % | 100 % |

**Elaborado por:** Investigador

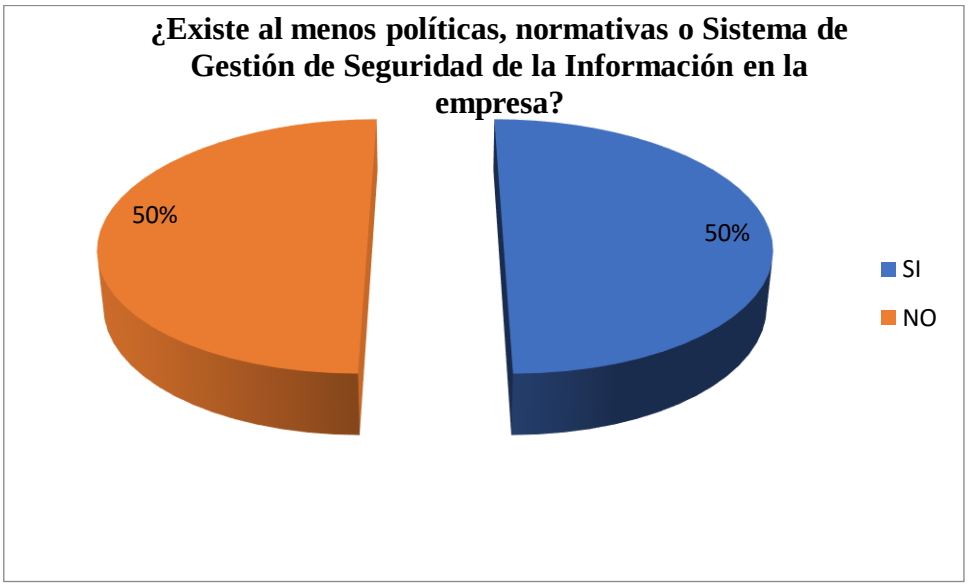



**Gráfico 9:** Pregunta 5
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que de 11 de 22 encuestados conocen la existencia de al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa donde laboran; mientras que el resto de encuestados (11) no conocen acerca de su existencia.

**Análisis:** El conocimiento parcial por parte de los empleados en una empresa de desarrollo de software en temas de seguridad de la información hace que la aplicación de las políticas, normativas y/o de los sistemas de seguridad de la información que posee no se efectiva, ya que el personal de trabajo desconoce todas aquellas responsabilidades y prácticas que ejerce la alta dirección empresarial en materia de seguridad.

**Pregunta 6:** ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información?

**Tabla 6:** Resultados de la Pregunta 6

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 20 | 2 | 22 |
| **Porcentaje (%)** | 90,91 % | 9,09 % | 100 % |

**Elaborado por:** Investigador

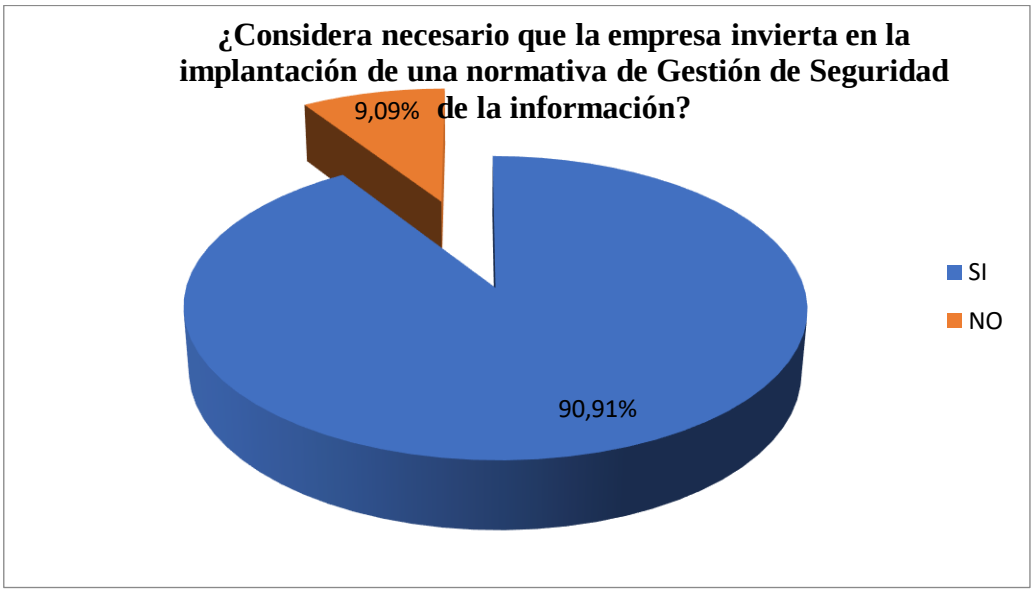



**Gráfico 10:** Pregunta 6
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que 20 encuestados están de acuerdo en que, en las empresas de desarrollo de software es necesario invertir en la implantación de una normativa de Gestión de Seguridad de la información.

**Análisis:** Las empresas de desarrollo de software en conjunto con sus empleados están poniendo mayor atención en sus activos más valiosos, que son los datos que manejan, por lo que invertir en una normativa de seguridad de la información traerá ventajas económicas, se garantizará la seguridad, confidencialidad, e integridad de los datos, además de permitir alcanzar los objetivos empresariales.

**Pregunta 7:** ¿La empresa capacita al personal en temas de seguridad de la información?

**Tabla 7:** Resultados de la Pregunta 7

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 6 | 16 | 22 |
| **Porcentaje (%)** | 27,27 % | 72,73 % | 100 % |

**Elaborado por:** Investigador

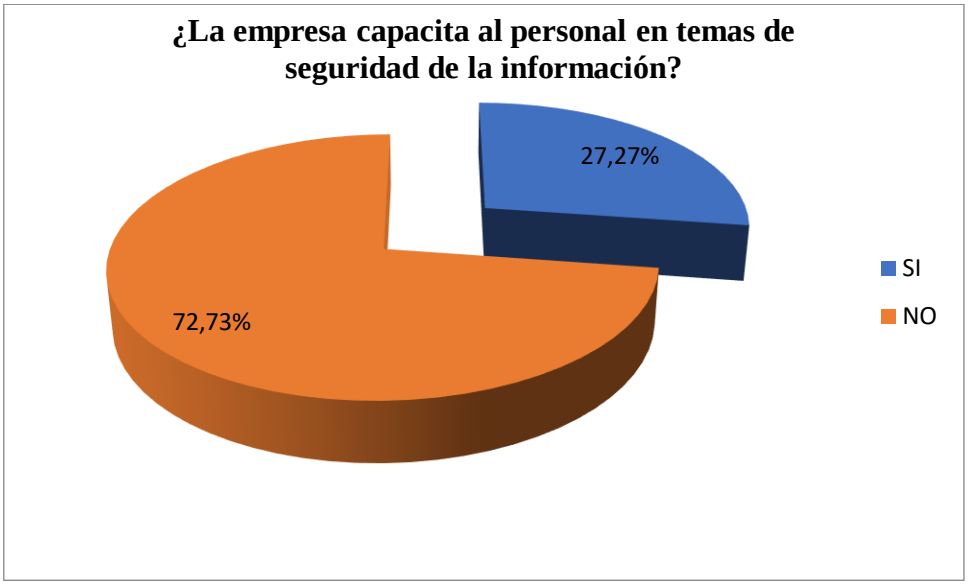



**Gráfico 11:** Pregunta 7
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que solo 6 encuestados de un total de 22 aseguran que la empresa de desarrollo de software capacita al personal en temas de seguridad de la información; 16 encuestados no aseguran haber accedido a capacitación alguna.

**Análisis:** Capacitar y concienciar a las personas que están relacionadas con la seguridad de la información es una empresa es de gran importancia, ya que la falta de este indicador es uno de los motivos y fracasos de los proyectos de seguridad de la información en las empresas.

**Pregunta 8:** ¿Existe algún control para navegar en internet?

**Tabla 8:** Resultados de la Pregunta 8

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 5 | 17 | 22 |
| **Porcentaje (%)** | 22,73% | 77,27% | 100 % |

**Elaborado por:** Investigador

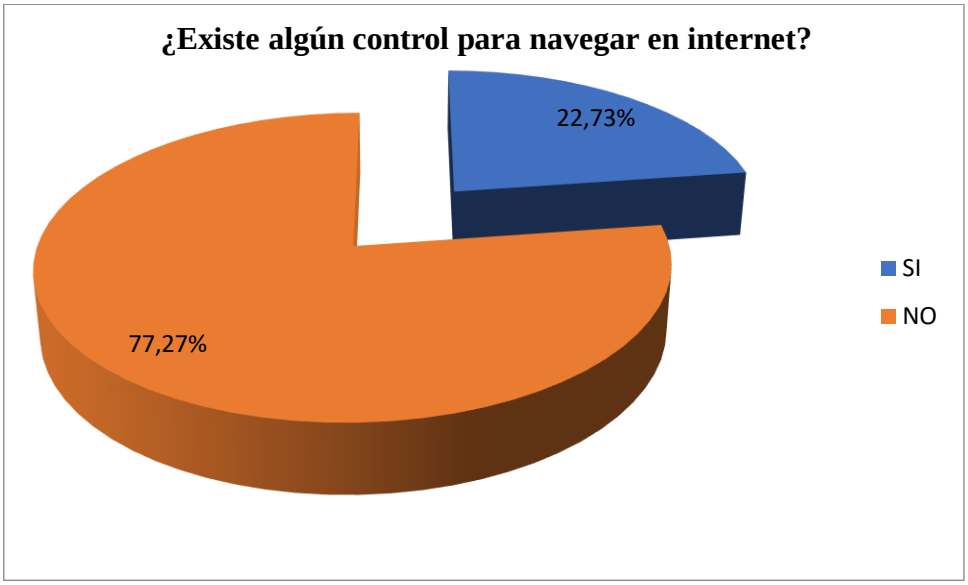



**Gráfico 12:** Pregunta 8
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que 17 encuestados de un total de 22 encuestados, afirman que en las empresas donde laboran no existe control para navegar en internet; y los 5 encuestados restantes afirman que si existe control.

**Análisis:** La ausencia de un control al momento de navegar por internet hace que involuntariamente la información, el personal de trabajo, los recursos empresariales sean utilizados/manejados de manera no segura; afectando la privacidad, siendo cada vez más vulnerables a los delitos informáticos.

**Pregunta 9:** ¿Existe control sobre el uso del correo electrónico?

**Tabla 9:** Resultados de la Pregunta 9

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 5 | 17 | 22 |
| **Porcentaje (%)** | 22,73% | 77,27% | 100 % |

**Elaborado por:** Investigador

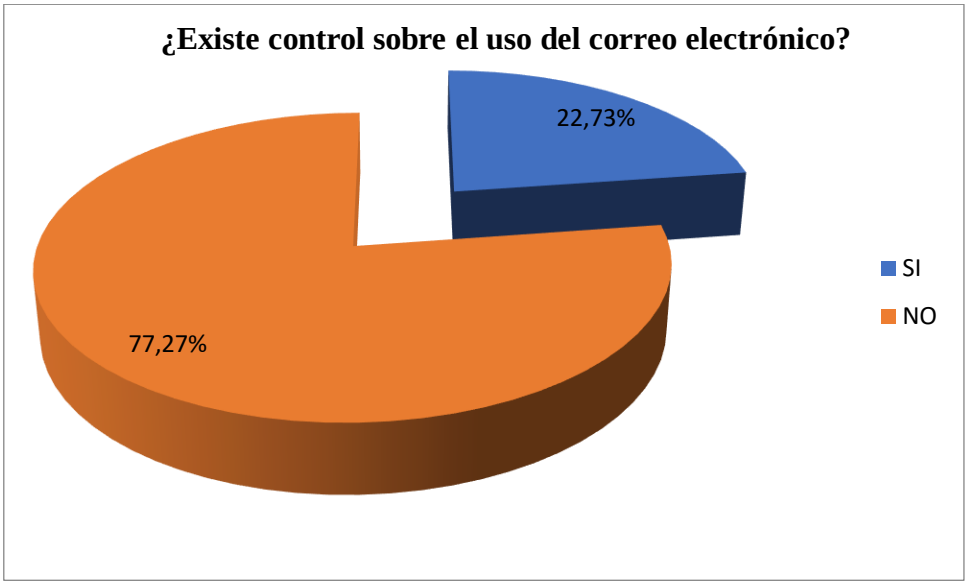



**Gráfico 13:** Pregunta 9
**Elaborado por:** Investigador

**Interpretación:** De un total de 22 encuestados, 17 afirman que en la empresa no existe control alguno del uso del correo electrónico corporativo y 5 encuestados aseguran que si se les aplica controles al momento de usar su correo electrónico corporativo.

**Análisis:** Regular y controlar el uso del correo electrónico en el ámbito laboral constituye ser una buena práctica que contribuye a ofrecer más seguridad, sobre todo en el derecho de proteger los datos de carácter personal y de terceras personas; por lo que no aplicar normas para el uso del correo electrónico es una amenaza/debilidad para la empresa y para el personal que labora.

**Pregunta 10:** ¿Existe alguna política para el cambio regular de las contraseñas?

**Tabla 10:** Resultados de la Pregunta 10

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 2 | 20 | 22 |
| **Porcentaje (%)** | 9,09 % | 90,91 % | 100 % |

**Elaborado por:** Investigador

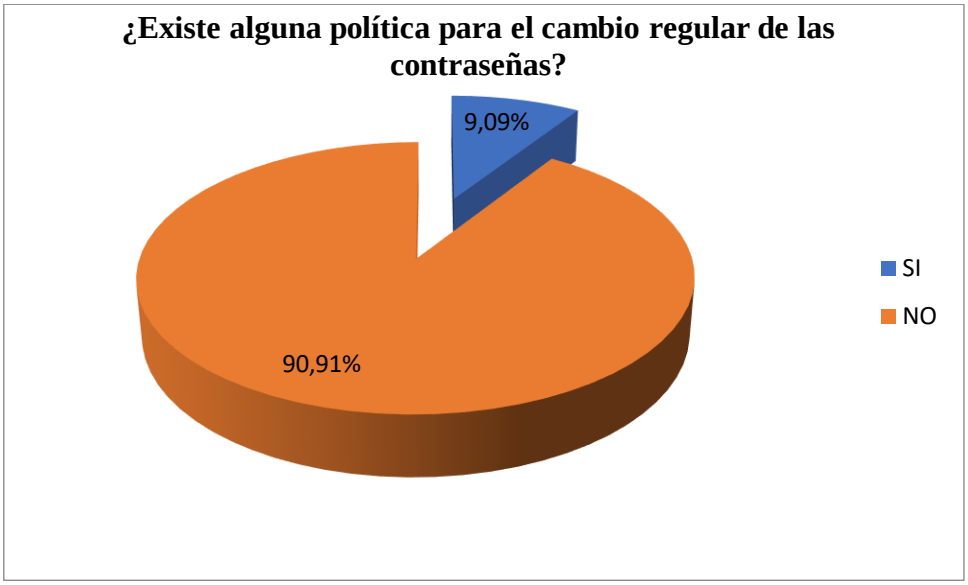



**Gráfico 14:** Pregunta 10
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que, de un total de 22 encuestados, 20 afirman que NO existe alguna política para el cambio regular de las contraseñas en la empresa de desarrollo de software donde laboran y 2 encuestados afirman que SI existe alguna política para el cambio regular de las contraseñas.

**Análisis:** La ausencia de política alguna para el cambio regular de contraseña en una empresa hace que la confidencialidad de dicha contraseña sea no segura, exponiendo el acceso a su información personal, laboral y empresarial en cualquier instante de tiempo. Es necesario disponer de políticas para con frecuencia cambiar las contraseñas de las cuentas de usuario.

**Pregunta 11:** ¿Antes y después de la contratación del personal se hace entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información?

**Tabla 11:** Resultados de la Pregunta 11

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 4 | 18 | 22 |
| **Porcentaje (%)** | 18,18 % | 81,82 % | 100 % |

**Elaborado por:** Investigador

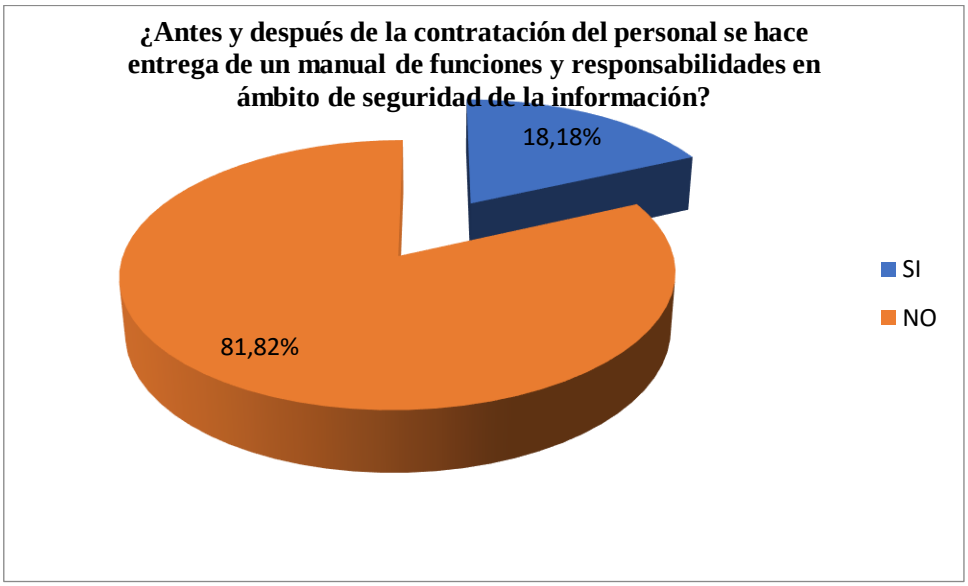



**Gráfico 15:** Pregunta 11
**Elaborado por:** Investigador

**Interpretación:** 18 encuestados de un total de 22 encuestados afirman que antes y después de la contratación del personal NO se hace entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información y solo 4 encuestados aseguran que SI.

**Análisis:** Se concluye que antes y después de la contratación del personal no siempre se entrega algún manual de funciones y responsabilidades en ámbito de seguridad de la información al personal de trabajo.

**Pregunta 12:** ¿La información disponible en los repositorios de datos se mantiene exacta?

**Tabla 12:** Resultados de la Pregunta 12

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 9 | 13 | 22 |
| **Porcentaje (%)** | 40,91 % | 59,09 % | 100 % |

**Elaborado por:** Investigador

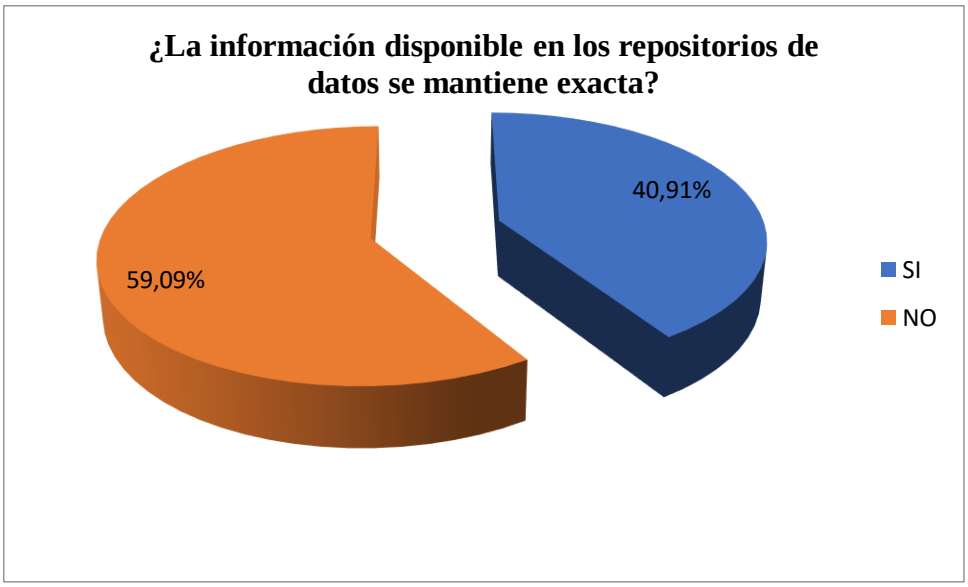



**Gráfico 16:** Pregunta 12
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que 13 encuestados que laboran en al menos una empresa de desarrollo de software aseguran que la información disponible en los repositorios de datos NO se mantiene exacta y contra posición de 9 encuestados que aseguran que la información disponible en los repositorios de datos SI se mantiene exacta.

**Análisis:** La exactitud de la información es un indicador que determina que en los repositorios de datos existe alteración del estado de la información.

**Pregunta 13:** ¿La información disponible en los repositorios de datos es completa?

**Tabla 13:** Resultados de la Pregunta 13

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 8 | 14 | 22 |
| **Porcentaje (%)** | 36,36 % | 63,64 % | 100 % |

**Elaborado por:** Investigador

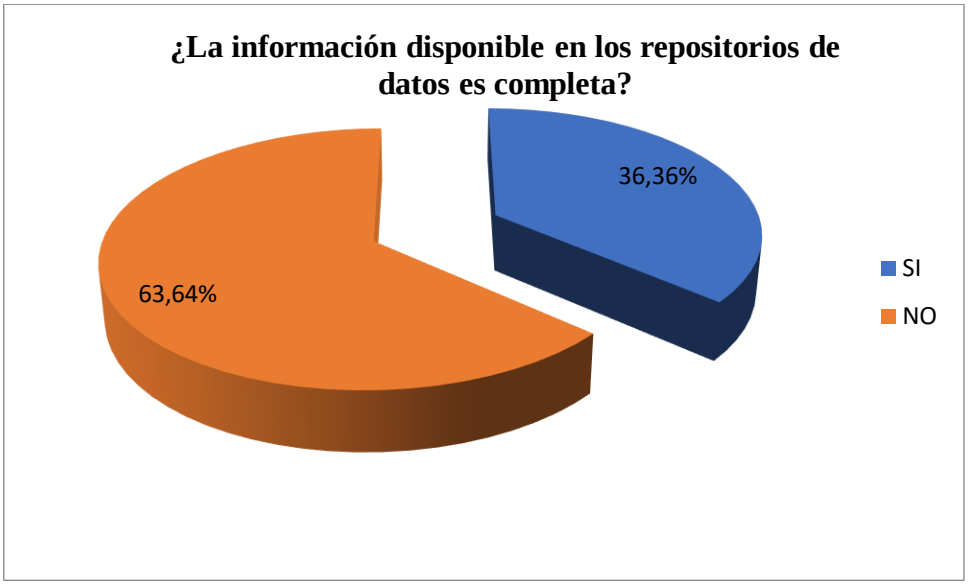



**Gráfico 17:** Pregunta 13
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que 14 encuestados que laboran en al menos una empresa de desarrollo de software aseguran que la información disponible en los repositorios de datos NO es completa y contra posición de 8 encuestados que aseguran que la información disponible en los repositorios de datos es completa**.**

**Análisis:** Se concluye que en los repositorios de datos la información disponible no es completa, por lo que dificulta su tratamiento en las transacciones que se realizan desde los sistemas de información.

**Pregunta 14:** ¿La información solo está disponible para accesos autorizados?

**Tabla 14:** Resultados de la Pregunta 14

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 14 | 8 | 22 |
| **Porcentaje (%)** | 63,64 % | 36,36 % | 100 % |

**Elaborado por:** Investigador

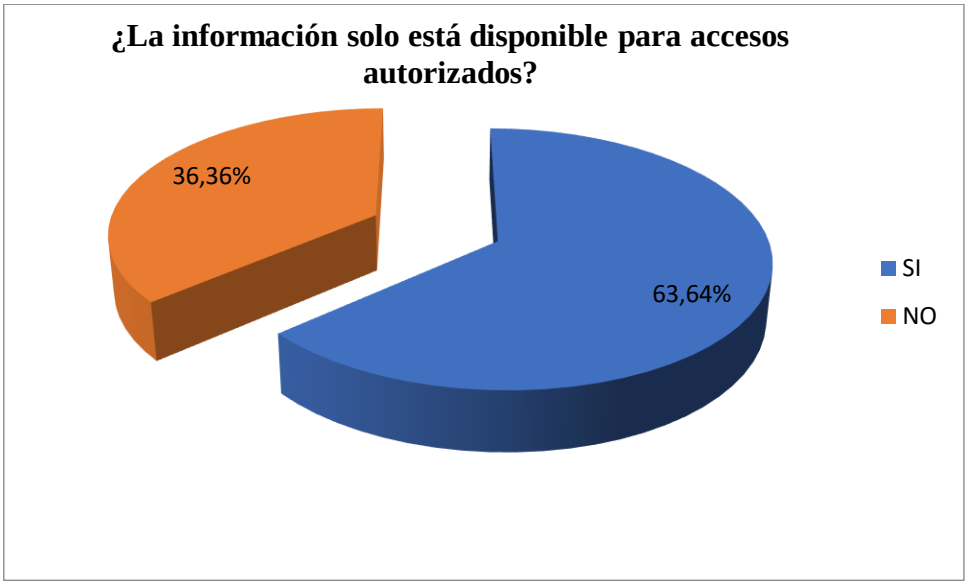



**Gráfico 18:** Pregunta 14
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que 8 encuestados que laboran en al menos una empresa de desarrollo de software aseguran que la información NO solo está disponible para accesos autorizados y contra posición de 14 encuestados que aseguran que la información SI está disponible solo para accesos autorizados.

**Análisis:** Se concluye que el acceso a la información mayoritariamente es solo para el personal autorizado, usuarios que cuentan con los permisos y roles que les permiten la lectura/escritura de los datos.

**Pregunta 15:** ¿Se garantiza el almacenamiento de la información?

**Tabla 15:** Resultados de la Pregunta 15

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 11 | 11 | 22 |
| **Porcentaje (%)** | 50 % | 50 % | 100 % |

**Elaborado por:** Investigador

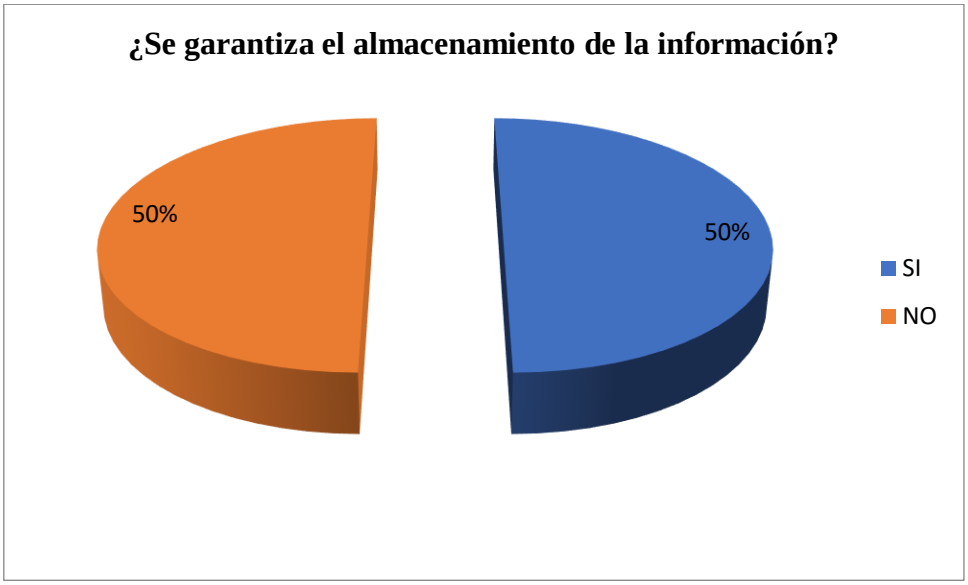



**Gráfico 19:** Pregunta 15
**Elaborado por:** Investigador

**Interpretación:** De un total de 22 encuestados, 11 encuestados que corresponden al 50% manifiestan que en la empresa donde trabajan SI se garantiza el almacenamiento de la información; mientras que el 50% restante determina que NO se garantiza el almacenamiento de la información.

**Análisis:** Se concluye que el almacenamiento de la información como indicador de la seguridad de la información es parcialmente garantizado.

**Pregunta 16:** ¿Se garantiza el acceso oportuno hacia la información?

**Tabla 16:** Resultados de la Pregunta 16

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 10 | 12 | 22 |
| **Porcentaje (%)** | 45,45 % | 54,55 % | 100 % |

**Elaborado por:** Investigador

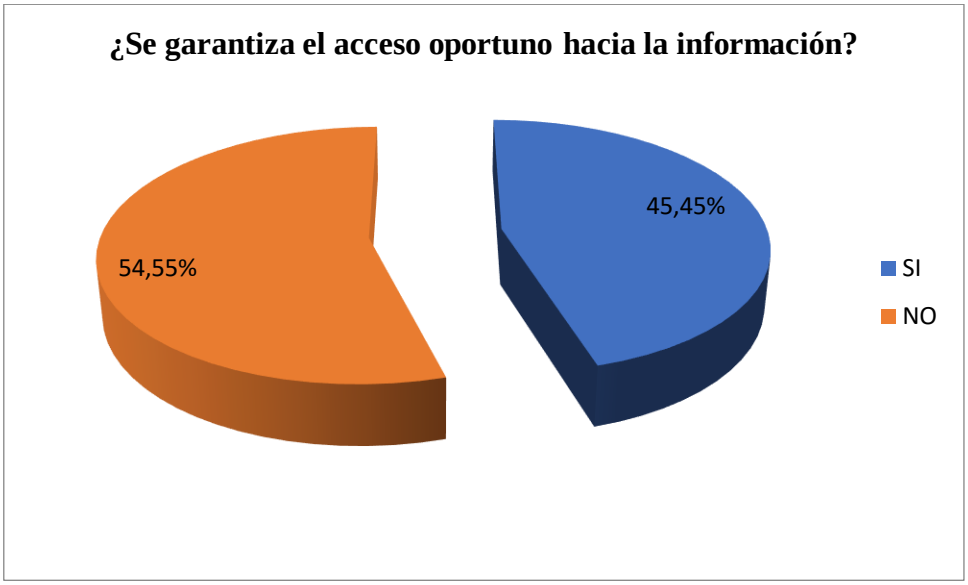



**Gráfico 20:** Pregunta 16
**Elaborado por:** Investigador

**Interpretación:** Se determina que 12 encuestados de un total de 22 encuestados, indican que en su lugar de trabajo NO se garantiza el acceso oportuno hacia la información y 10 encuestados indican que SI se garantiza el acceso oportuno hacia la información.

**Análisis:** Se concluye que el acceso oportuno a la información no está garantizado, aunque el acceso se garantice solo al personal autorizado, la disponibilidad de la información debe garantizarse en acceso oportuno y en accesos autorizados.

**Pregunta 17:** ¿La información está disponible para actualizaciones constantes?

**Tabla 17:** Resultados de la Pregunta 17

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 14 | 8 | 22 |
| **Porcentaje (%)** | 63,64 % | 36,36 % | 100 % |

**Elaborado por:** Investigador

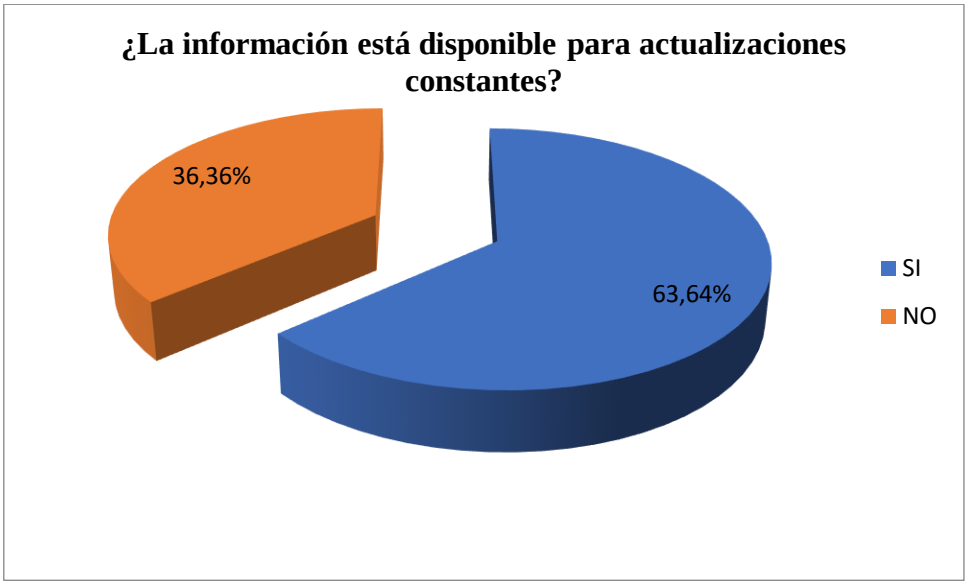



**Gráfico 21:** Pregunta 17
**Elaborado por:** Investigador

**Interpretación:** El 63,64% de encuestados afirma que en las empresas de desarrollo de software la información SI está disponible para actualizaciones constantes y con un 36,36% se afirma que la información NO está disponible para actualizaciones constantes.

**Análisis:** Se concluye que la información está disponible para actualizaciones constantes, dichas transacciones para actualizar la información deben reflejar la integridad de la información.

**Pregunta 18:** ¿Se identifica quién realiza cambios en la información?

**Tabla 18:** Resultados de la Pregunta 18

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 7 | 15 | 22 |
| **Porcentaje (%)** | 31,82 % | 68,18 % | 100 % |

**Elaborado por:** Investigador

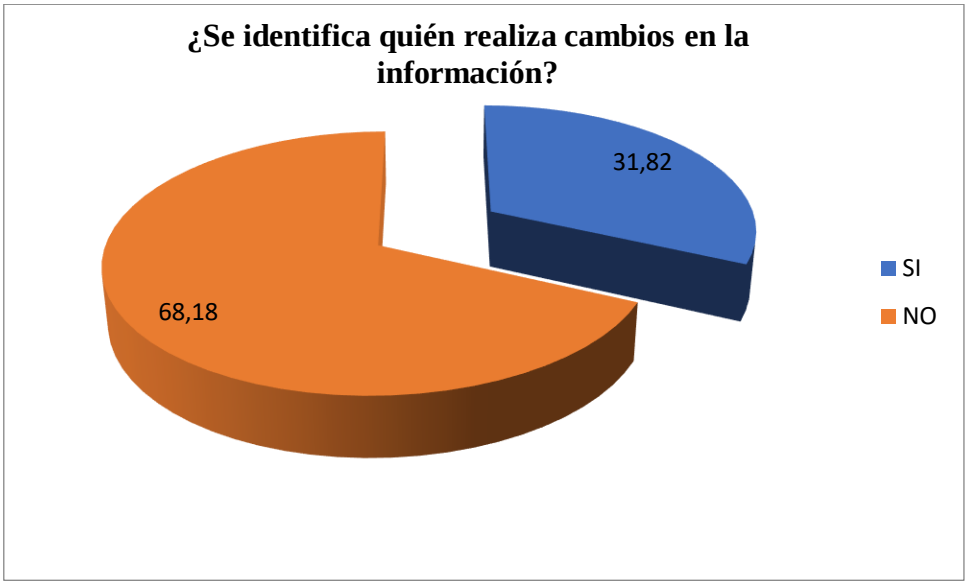



**Gráfico 22:** Pregunta 18
**Elaborado por:** Investigador

**Interpretación:** De un total de 22 encuestados, 15 encuestados aseguran que en la empresa donde laboran NO se identifica quién realiza cambios en la información cuando estos suceden; mientras tanto que 7 encuestados aseguran que SI se identifica quién realiza cambios en la información.

**Análisis:** Se concluye mayoritariamente que no se identifica quien realiza los cambios en la información, aunque los accesos en su mayoría son solo para el personal autorizado; evidenciando debilidades en la administración y seguridad de los sistemas informáticos.

**Pregunta 19:** ¿Se conoce en qué momento se cambió la información?

**Tabla 19:** Resultados de la Pregunta 19

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 6 | 16 | 22 |
| **Porcentaje (%)** | 27,27 % | 72,73 % | 100 % |

**Elaborado por:** Investigador

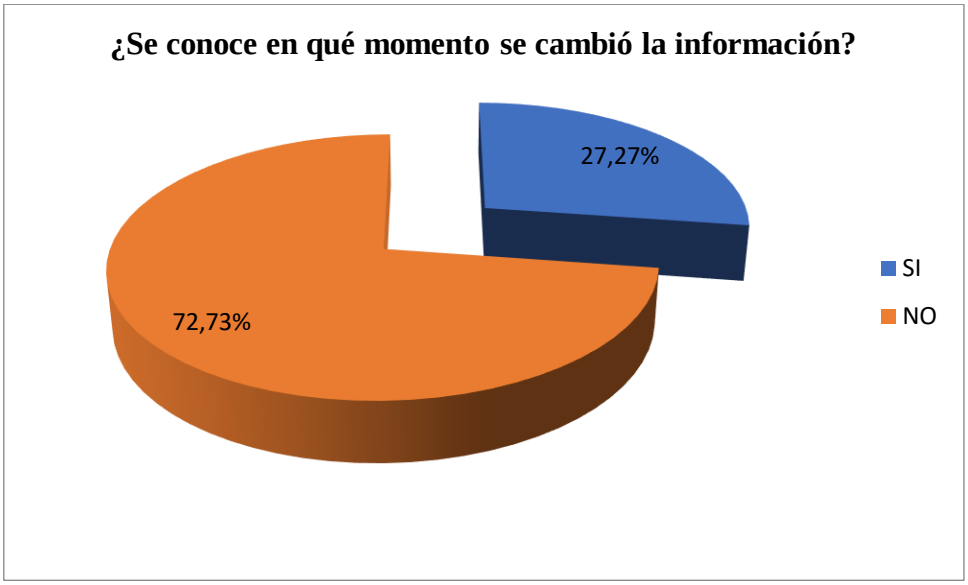



**Gráfico 23:** Pregunta 19
**Elaborado por:** Investigador

**Interpretación:** De un total de 22 encuestados, 16 encuestados aseguran que en la empresa donde laboran NO se conoce en qué momento se cambió la información en caso de que suceda; mientras tanto que 6 encuestados aseguran que SI se conoce en qué momento se cambió la información.

**Análisis:** Se concluye que parcialmente se identifica el momento exacto en el que se cambió la información, para cubrir esta debilidad es necesario llevar un registro del log de transacciones desde la administración y seguridad de los sistemas.

**Pregunta 20:** ¿El contenido de la información que está disponible es comprobable?

**Tabla 20:** Resultados de la Pregunta 20

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 7 | 15 | 22 |
| **Porcentaje (%)** | 31,82 % | 68,18% | 100 % |

**Elaborado por:** Investigador

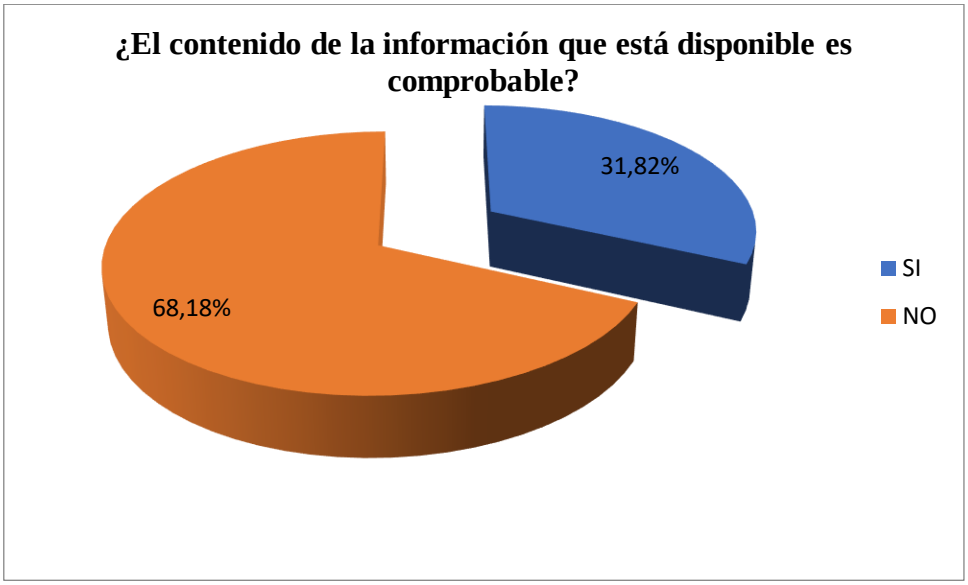



**Gráfico 24:** Pregunta 20
**Elaborado por:** Investigador

**Interpretación:** Con una frecuencia de 15 encuestados del total determinan que NO es comprobable en contenido de la información que está disponible y a su alcance; mientras que 7 encuestados determinan que SI es comprobable en contenido de la información que está disponible.

**Análisis:** Se concluye que casi no siempre el contenido de la información disponible es comprobable.

**Pregunta 21:** ¿La información disponible es verdadera?

**Tabla 21:** Resultados de la Pregunta 21

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 11 | 11 | 22 |
| **Porcentaje (%)** | 50 % | 50 % | 100 % |

**Elaborado por:** Investigador

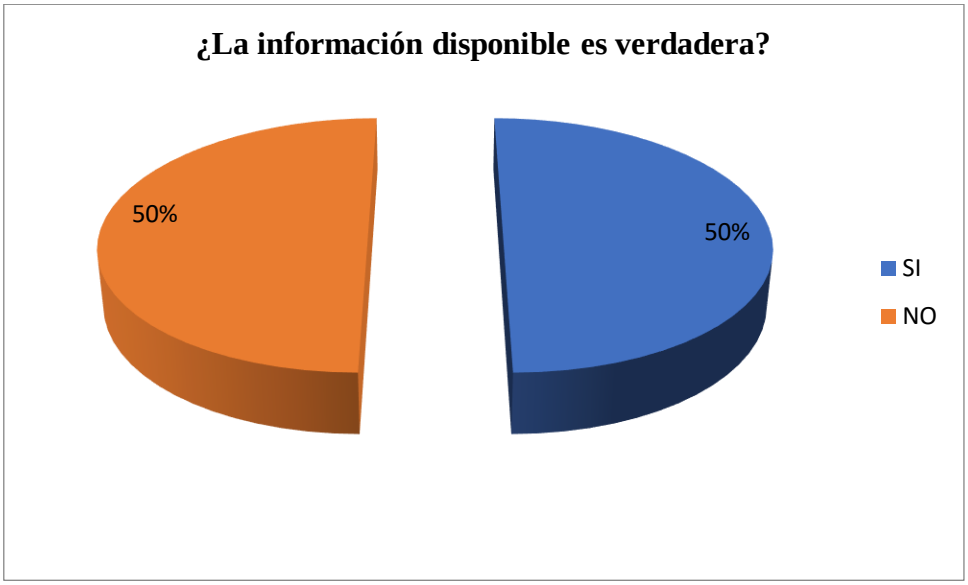



**Gráfico 25:** Pregunta 21
**Elaborado por:** Investigador

**Interpretación:** Igualitariamente los encuestados determinan que la información disponible es verdadera y también que no es verdadera, en su lugar de trabajo.

**Análisis:** Se concluye que parcialmente la información disponible es verdadera, si no es posible comprobar la información en su totalidad, asegurar que es verdadera no se puede determinar en su totalidad.

**Pregunta 22:** ¿Se realiza respaldos de los datos?

**Tabla 22:** Resultados de la Pregunta 22

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 17 | 5 | 22 |
| **Porcentaje (%)** | 77,27 % | 22,73 % | 100 % |

**Elaborado por:** Investigador

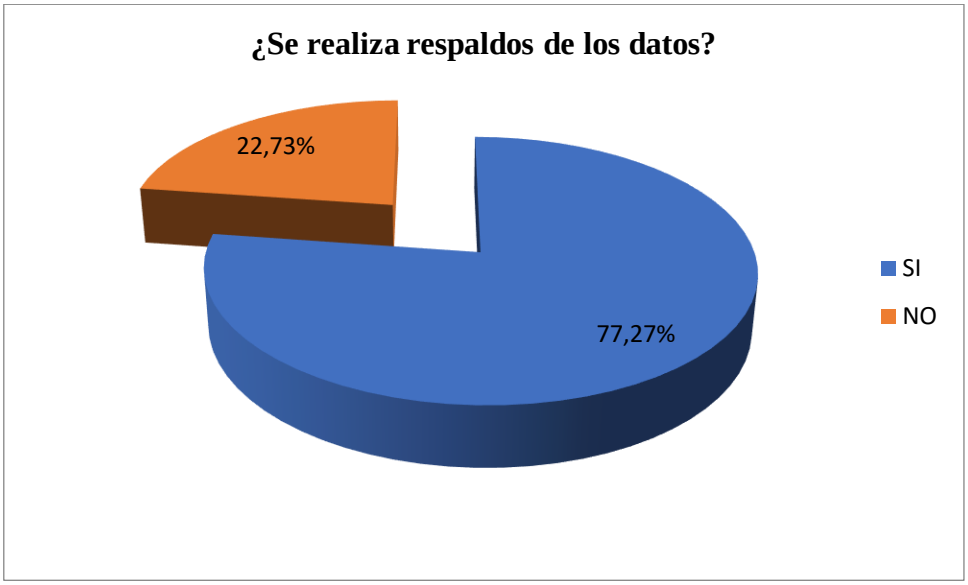



**Gráfico 26:** Pregunta 22
**Elaborado por:** Investigador

**Interpretación:** Respaldar los datos en su diferentes estados y presentación en evidente en las empresas de desarrollo de software; por lo que el 77,27% de encuestados aseguran que si se respalda los datos y tan solo el 22,73% aseguran que no.

**Análisis:** Se concluye que, de la información disponible en los repositorios de datos, casi siempre se realiza respaldos.

**Pregunta 23:** ¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?

**Tabla 23:** Resultados de la Pregunta 23

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 13 | 9 | 22 |
| **Porcentaje (%)** | 59,09 % | 40, 91 % | 100 % |

**Elaborado por:** Investigador

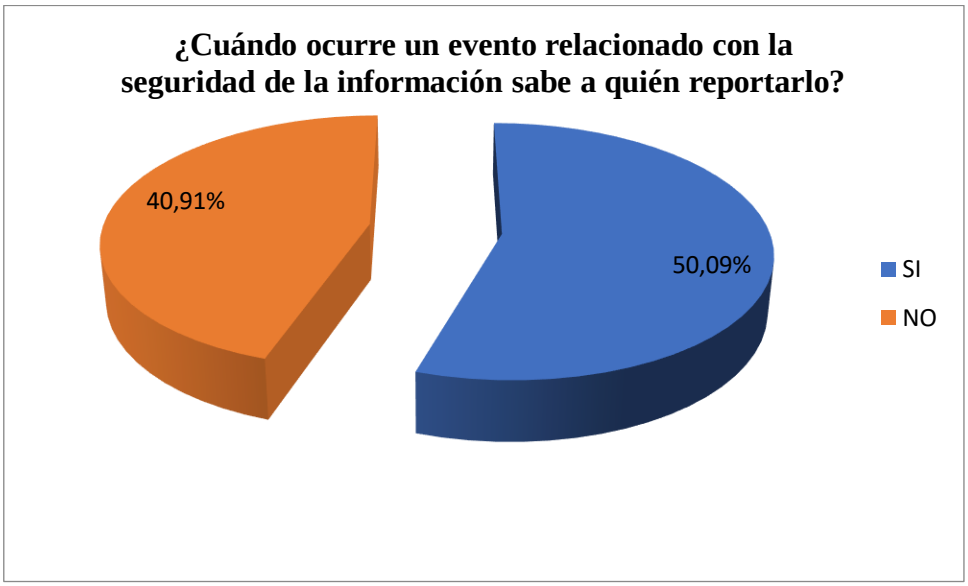



**Gráfico 27:** Pregunta 23
**Elaborado por:** Investigador

**Interpretación:** Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo, el 40,91% de los encuestados aseguran que si saben a quién reportarlo; mientras que el 50,09% no sabe a quién reportarlo en su lugar de trabajo.

**Análisis:** Se concluye que cuando ocurre un evento relacionado con la seguridad de la información no siempre se sabe a quién reportarlo.

**Pregunta 24:** ¿Existen zonas restringidas de acceso de personal?

**Tabla 24:** Resultados de la Pregunta 24

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 7 | 15 | 22 |
| **Porcentaje (%)** | 31,82% | 68,18 % | 100 % |

**Elaborado por:** Investigador

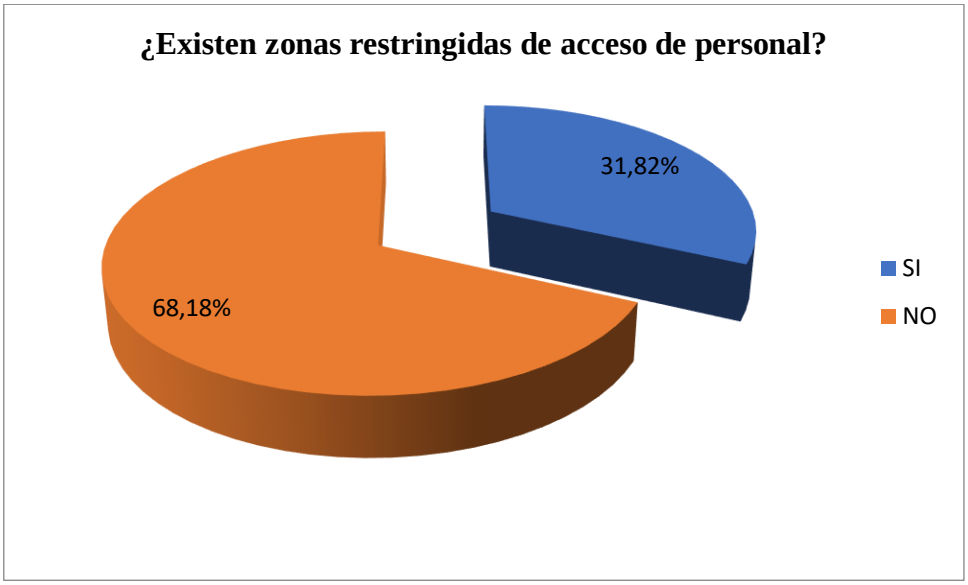



**Gráfico 28:** Pregunta 24
**Elaborado por:** Investigador

**Interpretación:** En las empresas de desarrollo de software en 68,18% de los empleados (encuestados) determinan que no existen zonas restringidas de acceso de personal; y el 31,82% de empleados determinan que si existen zonas restringidas de acceso de personal.

**Análisis:** Se concluye que parcialmente si existen zonas restringidas de acceso de personal en las empresas.

**Pregunta 25:** ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?

**Tabla 25:** Resultados de la Pregunta 25

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 8 | 14 | 22 |
| **Porcentaje (%)** | 18,18 % | 81,82 % | 100 % |

**Elaborado por:** Investigador

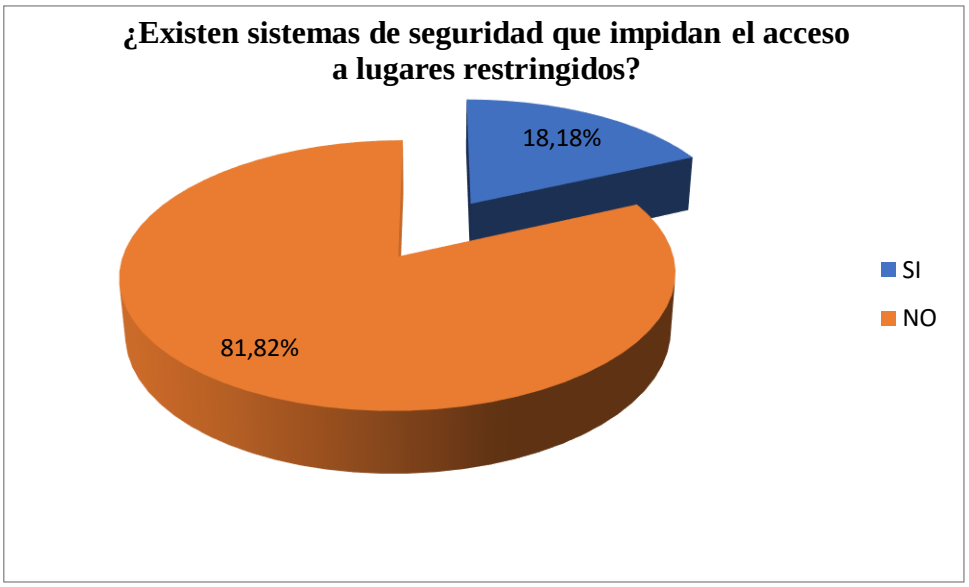



**Gráfico 29:** Pregunta 25
**Elaborado por:** Investigador

**Interpretación:** El 81,82% de encuestados aseguran que en su lugar de trabajo NO existen sistemas de seguridad que impidan el acceso a lugares restringidos y el 18,18% aseguran que si existen sistemas de seguridad que impidan el acceso a lugares restringidos.

**Análisis:** Se concluye que parcialmente existen sistemas de seguridad que impidan el acceso a lugares restringidos en las empresas.

**Pregunta 26:** ¿Se cuenta con sistemas de alarma como detectores de humo, humedad?

**Tabla 26:** Resultados de la Pregunta 26

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 14 | 8 | 22 |
| **Porcentaje (%)** | 18,18 % | 81,82 % | 100 % |

**Elaborado por:** Investigador

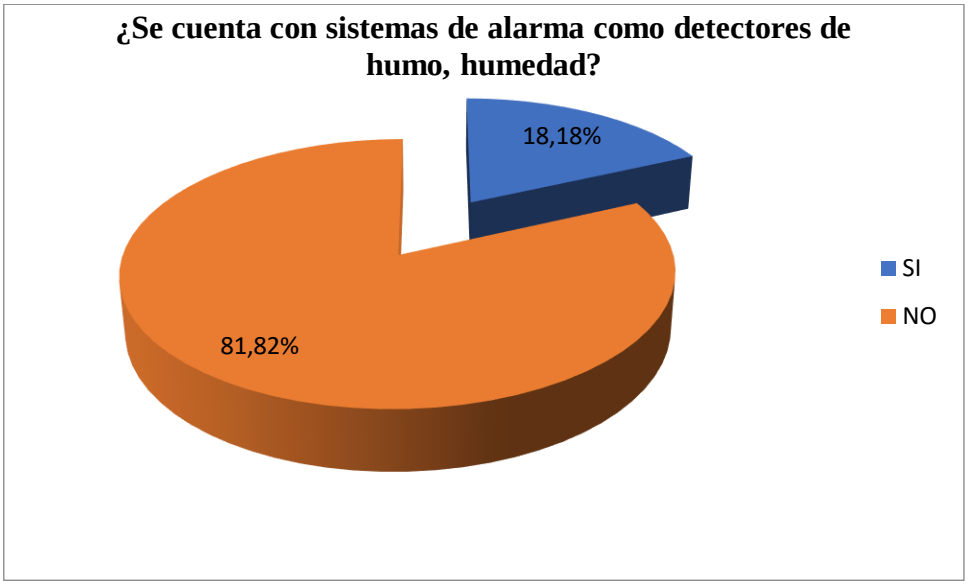



**Gráfico 30**: Pregunta 26
**Elaborado por:** Investigador

**Interpretación:** El 81,82% de encuestados aseguran que NO se cuenta con sistemas de alarma como detectores de humo, humedad en el lugar donde laboran; mientras que el 18,18% aseguran que, SI se cuenta con sistemas de alarma como detectores de humo, humedad.

**Análisis:** Se concluye que parcialmente se cuenta con sistemas de alarma como detectores de humo, humedad en las empresas.

**Pregunta 27:** ¿Existe vigilancia en la entrada del edificio?

**Tabla 27:** Resultados de la Pregunta 27

| | SI | NO | TOTAL |
|---|---|---|---|
| **Frecuencia** | 4 | 18 | 22 |
| **Porcentaje (%)** | 18,18 % | 81,82 % | 100 % |

**Elaborado por:** Investigador

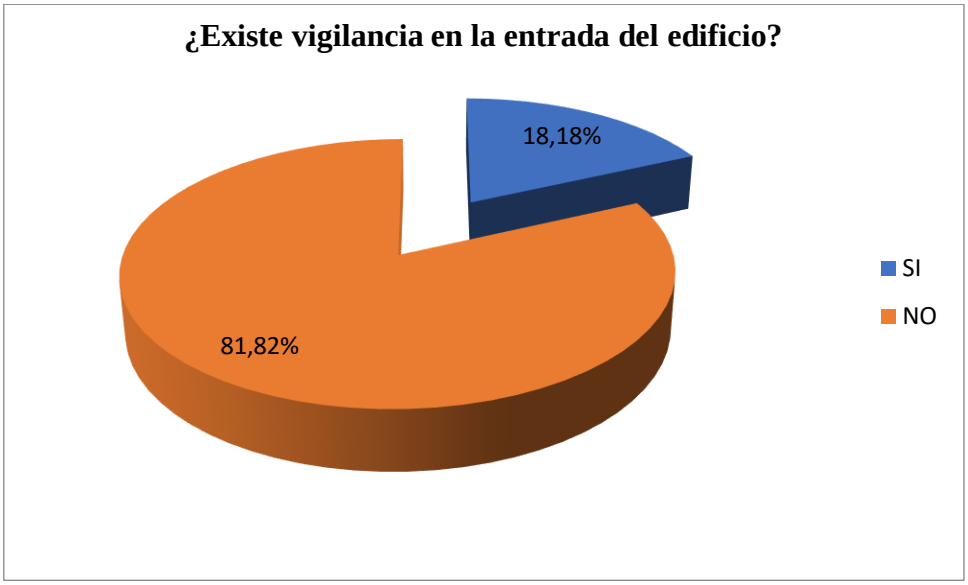



**Gráfico 31:** Pregunta 27
**Elaborado por:** Investigador

**Interpretación:** Se evidencia que el 81,82% de encuestados asegura que en el lugar donde laboran NO existe vigilancia en la entrada del edificio y el 18,18% aseguran que SI existe vigilancia en la entrada del edificio.

**Análisis:** Se concluye que mayoritariamente no existe vigilancia en la entrada del edificio donde funcionan las empresas.

**Resumen general de resultados obtenidos**

**Tabla 28:** Resumen general de resultados

| N.º Pregunta | SI | NO |
|---|---|---|
| 1 | 50% | 50% |
| 2 | 95,45% | 4,55% |
| 3 | 18,18% | 81,82% |
| 4 | 54,55% | 45,45% |
| 5 | 50% | 50% |
| 6 | 90,91% | 9,09% |
| 7 | 27,27% | 72,73% |
| 8 | 22,73% | 77,27% |
| 9 | 22,73% | 77,27% |
| 1 0 | 9,09% | 90,91% |
| 11 | 18,18% | 81,82% |
| 12 | 40,91% | 59,09% |
| 13 | 36,36% | 63,64% |
| 14 | 63,64% | 36,36% |
| 15 | 50% | 50% |
| 16 | 45,45% | 54,55% |
| 17 | 63,64% | 36,36% |
| 18 | 31,82% | 68,18% |
| 19 | 27,27% | 72,73% |
| 20 | 31,82% | 68,18% |
| 21 | 50% | 50% |
| 22 | 77,27% | 22,73% |
| 23 | 59,09% | 40, 91 % |
| 24 | 31,82% | 68,18% |
| 25 | 18,18% | 81,82% |
| 26 | 18,18% | 81,82% |
| 27 | 18,18% | 81,82% |
| **TOTAL** | **41%** | **59%** |

**Elaborado por:** Investigador


**Gráfico 32:** Resumen general de resultados – encuesta
**Elaborado por:** Investigador

**Análisis e interpretación general de resultados**

Con el 59% de información procesada, se evidencia que las empresas dedicadas al desarrollo de software no cumplen con controles básicos de seguridad de la información en todos los ámbitos de aplicación, mayoritariamente afirman que, es necesario que las empresas inviertan en la implementación de una normativa para la gestión de seguridad de la información, llevar a cabo capacitaciones y concienciar a los empleados acerca de buenas prácticas de protección de datos personales y de terceros, la confidencialidad, integridad y disponibilidad está comprometida a riesgos y vulnerabilidades por que la información no es totalmente exacta, no es completa, el almacenamiento y acceso oportuno no está garantizado, dificultad para determinar quien realiza alteraciones a los datos.

Con el 41% del total de información procesada, se afirma que parcialmente dichas empresas si poseen al menos controles de seguridad, hacen uso de software antivirus, poseen sistemas de enfriamiento de equipos, sistemas de seguridad física, controles básicos para el uso del internet, correo electrónico, cambio de contraseñas y respaldo de información.

## 4.2. Verificación de la hipótesis

### 4.2.1. Planteamiento de la hipótesis

**Hipótesis nula (H0):**

La seguridad de la información **NO** incide en la protección de los datos de los sistemas informáticos de las empresas de desarrollo de software.

**Hipótesis alterna (H1):**

La seguridad de la información **SI** incide en la protección de los datos de los sistemas informáticos de las empresas de desarrollo de software.

### 4.2.2. Nivel de significación

Una vez establecida la hipótesis nula y la hipótesis alternativa, se determina el nivel de significancia, y para este caso de estudio se utiliza un nivel de significancia del α=0,10.

### 4.2.3. Criterio

Como estadístico para la prueba de hipótesis se utiliza la técnica Chi-cuadrado, siendo la formula la siguiente expresión:

$$x^2 = \sum_i = \frac{(observada_i - esperada_i)^2}{esperada_i}$$

$$x^2 = \sum (\frac{(f_0 - f_e)^2}{f_e})$$

Simbología:

$$x^2 = Ji - Cuadrado$$

$$\sum = Sumatoria$$

$$f_0 = Frecuencia\ observada$$

$$f_e = Frecuencia\ esperada$$

**Frecuencia esperada:** el cálculo de la frecuencia esperada, se obtiene a través del producto de los totales marginales dividido por el número total de casos:

***Total, marginales:*** $(total\ del\ renglón).\ (\ total\ de\ la\ columna)$

***Número total de casos:*** $gran\ total$

$$f_e = \frac{(total\ del\ renglón).(total\ de\ la\ columna)}{gran\ total}$$

**Determinación de los grados de libertad:**

$$\boldsymbol{GL} = (f-1)(c-1)$$

Gl = Grado de libertad

f= Filas

c= Columnas.

Entonces,

$$\boldsymbol{Gl} = (\mathbf{2}-\mathbf{1})(\mathbf{3}-\mathbf{1})$$

$$\boldsymbol{Gl} = (\mathbf{1})(\mathbf{2})$$

$$\boldsymbol{Gl} = 2\ \ de\ libertad$$

De acuerdo a la tabla estadística de distribución de Chi – Cuadrado, con un nivel de significancia 0,1 a 2 grados de libertad, genera un valor de $X^2\ tabla = 4.605$.

**Tabla 29:** Estadística de distribución Chi - Cuadrado

| Grados de libertad | Posibilidad de casualidad en porcentaje | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **90%** | **80%** | **70%** | **50%** | **30%** | **20%** | **10%** | **5%** | **1%** |
| **1** | 0,016 | 0,064 | 0,148 | 0,455 | 1,074 | 1,642 | 2,706 | 3,841 | 6,635 |
| **2** | 0,211 | 0,446 | 0,713 | 1,386 | 2,408 | 3,219 | 4,605 | 5,991 | 9,210 |
| **3** | 0,584 | 1,005 | 1,424 | 2,366 | 2,665 | 4,642 | 6,251 | 7,815 | 11,341 |

**Fuente:** Estadística de Distribución Chi – Cuadrado.

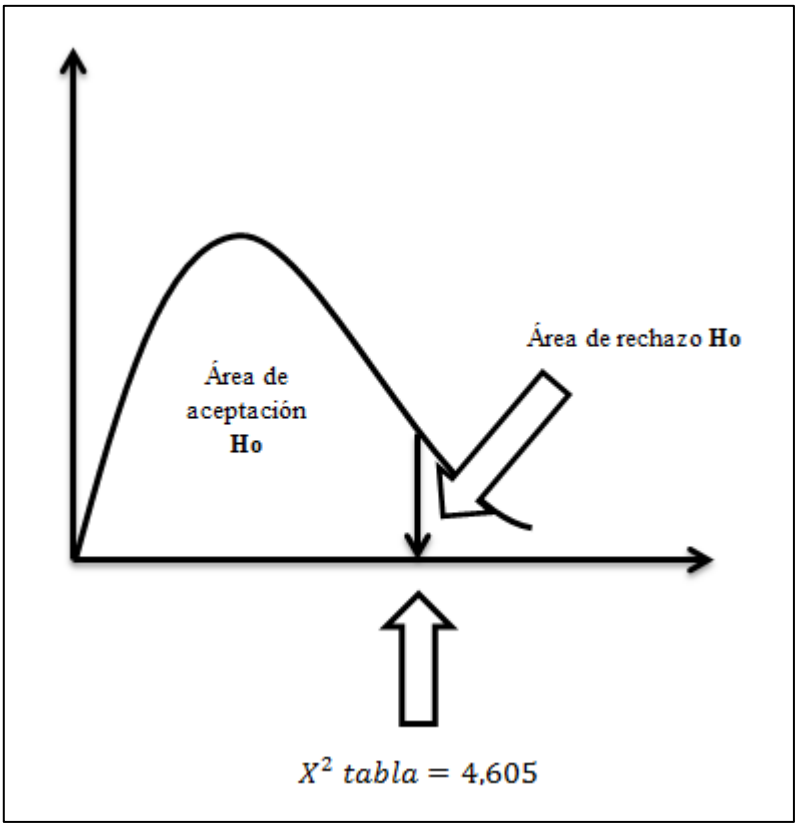



**Gráfico 33:** Área de aceptación y rechazo Chi - Cuadrado
**Elaborado por:** Investigador

**Regla de decisión:** No se rechaza $\boldsymbol{H_0}$ (hipótesis nula) si el valor que encuentra para de $\boldsymbol{X^2\ calculado}$ es menor que **4,605.** Si el valor que se encuentra es mayor o igual al valor crítico, se rechaza $\boldsymbol{H_0}$ y se acepta $\boldsymbol{H_1}$ (hipótesis alterna).

**Preguntas para la comprobación de la hipótesis:**

**Pregunta 5.** ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa?

**Pregunta 6.** ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información?

**Pregunta 7.** ¿La empresa capacita al personal en temas de seguridad de la información?

**Calculo de la frecuencia observada:**

**Tabla 30:** Frecuencia observada

| PARÁMETROS | ALTERNATIVAS | | TOTAL |
|---|---|---|---|
| | SI | NO | |
| ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa? | 11 | 11 | **22** |
| ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información? | 20 | 2 | **22** |
| ¿La empresa capacita al personal en temas de seguridad de la información? | 6 | 16 | **22** |
| **TOTAL** | **37** | **29** | **66** |

**Elaborado por:** Investigador

**Calculo de la frecuencia esperada:**

**Tabla 31:** Frecuencia esperada

| PARÁMETROS | ALTERNATIVAS | |
|---|---|---|
| | SI | NO |
| ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa? | 12,33 | 9,67 |
| ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información? | 12,33 | 9,67 |
| ¿La empresa capacita al personal en temas de seguridad de la información? | 12,33 | 9,67 |

**Elaborado por:** Investigador

### 4.2.4. Cálculos

**Tabla 32:** Cálculo Chi - Cuadrado

| PARÁMETRO/ALTERNATIVA | $f_0$ | $f_e$ | $f_0 - f_e$ | $(f_0 - f_e)^2$ | $(f_0 - f_e)^2/f_e$ |
|---|---|---|---|---|---|
| ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa? **SI** | 11 | 12,33 | -1,33 | 1,77 | 0,14 |
| ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa? **NO** | 11 | 9,67 | 1,33 | 1,77 | 0,18 |
| ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información? **SI** | 20 | 12,33 | 7,67 | 58,83 | 4,77 |
| ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información? **NO** | 2 | 9,67 | 7,67 | 58,83 | 5,99 |
| ¿La empresa capacita al personal en temas de seguridad de la información? **SI** | 6 | 12,33 | -6,33 | 40,01 | 6,67 |
| ¿La empresa capacita al personal en temas de seguridad de la información? **NO** | 16 | 9,67 | 6,33 | 40,01 | 4,13 |
| | | | | $X^2$ = | **21,88** |

**Elaborado por:** Investigador

### 4.2.5. Decisión

Si $X^2$ *calculado* = 21,88 y $X^2$ *tabla* = 4,605 Entonces:

$$X^2 \text{ calculado} > X^2 \text{ tabla}$$

Por lo tanto: $X^2$ *calculado* está en la zona de rechazo de la $H_0$ entonces se llega a la conclusión: se rechaza la hipótesis nula y se acepta la hipótesis $H_1$ (hipótesis alterna) que es: "La seguridad de la información **SI** incide en la protección de los datos de los sistemas informáticos de las empresas de desarrollo de software.

# CAPÍTULO V

# CONCLUSIONES Y RECOMENDACIONES

## 5.1. Conclusiones

- En las empresas de desarrollo de software, no se aplican eficientemente directrices en cuanto a la gestión de seguridad de la información, se evidencia que existe parcialmente políticas, controles, normativas o sistemas de gestión de seguridad de la información; por lo que, la disponibilidad, integridad y confidencialidad de la información en todos sus estados de presentación es vulnerable a riesgos y amenazas.
- Control del software operacional sobre todo restricciones sobre la instalación de software, educar y concientizar a los empleados en temas de seguridad, la navegación en internet es continua lo que compromete a tener un alto nivel de tráfico, la transferencia de la información está comprometida por que la mensajería electrónica carece de controles, además se determina que el acceso a las aplicaciones empresariales no está garantizada solo a los usuarios privilegiados, a nivel de base de datos la gestión de capacidad de almacenamiento está comprometido, además de los accesos permitidos, se identifica que la información disponible no es fácil comprobar.

## 5.2. Recomendaciones

- Se recomienda que, en las empresas de desarrollo de software se planteen soluciones a las amenazas, riegos y vulnerabilidades que está expuesta la información, siendo las más urgentes: restricciones en la instalación de software operacional, pruebas constantes del tráfico en la red, restricciones para la navegación en internet, control en la transferencia de información en la mensajería electrónica, controles de acceso a las aplicaciones por usuario, es decir, procedimientos de ingresos seguros a los recursos, a nivel de bases de datos es importante controlar la capacidad de almacenamiento de los recursos físicos.
- Se recomienda que, al poseer limitadas fortalezas en temas relacionados con la seguridad de la información las empresas deben establecer y documentar políticas de seguridad integrales que adopten criterios, directrices, procesos, estrategias y

hacer uso de normas y estándares internacionales que ajustando a sus necesidades organizativas, tecnológicas, administrativas les permita minimizar los riesgos a los niveles más bajos de aceptación.

# CAPÍTULO VI

# PROPUESTA

## 6.1. Tema

Implementación de una normativa de seguridad de la información para la protección de los datos en los sistemas informáticos de la empresa de desarrollo de software STD (STD: Soluciones Tecnológicas y Datos S. A.).

## 6.2. Datos informativos

**Organización:** Empresas de desarrollo de Software (STD).

**Favorecidos:** directores de proyectos tecnológicos, scrum masters, desarrolladores y DBAs.

## 6.3. Antecedentes de la propuesta

Por la información analizada e interpretada, de las empresas de desarrollo de software de la ciudad de Riobamba, se identificó que es una debilidad y amenaza no contar con procedimientos legales, organizativos, técnicos y tecnológicos aprobados que aseguren la información en todos sus niveles y estado.

## 6.4. Justificación

Garantizar la seguridad de la información es un principio y una política de la empresa de desarrollo de software STD, ya que el crecimiento de los datos que provienen de sus sistemas requiere cumplir con características de: disponibilidad, integridad y confidencialidad en todo momento.

## 6.5. Objetivos

- Determinar la situación actual de la seguridad de la información en la empresa de desarrollo de software STD.
- Diseñar una normativa de seguridad de seguridad de la información basada en la norma internacional ISO 27001:2013 que garantice el estado correcto de la información

- Obtener una proyección de posibles resultados por la aplicación de la normativa que faciliten la toma de decisiones en beneficio de los interese empresariales.

## 6.6. Análisis de factibilidad

### 6.6.1. Factibilidad técnica

El proyecto es técnicamente factible, ya que en la empresa existen recursos tecnológicos tales como: infraestructura tecnológica (hardware, software, sistemas de información), área de gestión de proyectos (calidad, testeo, metodología), área de base de datos, área de desarrollo web, área de desarrollo móvil, jefatura de proyectos, dirección de proyectos; administración general, control de activos, talento humano y proveedores que requieren contar con una normativa a seguir para asegurar el negocio y su presencia en el mercado tecnológico, respaldados de los criterios que plantea la NORMA ISO 27001: 2013 en materia de seguridad de la información.

### 6.6.2. Factibilidad operativa

Operativamente cuenta con el recurso humano adecuado y capacitado para gestionar la continuidad del proyecto.

### 6.6.3. Factibilidad organizativa

Organizacionalmente es factible el proyecto ya que los Directivos de la empresa muestran el interés por contar y disponer de medidas para la seguridad de la información, consientes que su aplicabilidad e implementación en a largo plazo.

### 6.6.4. Factibilidad económica

Económicamente es factible, para iniciar se requiere de una inversión económica en recursos de hardware y software de control de accesos para el personal, software para el control de vulnerabilidades, firewall; para lo que se estima realizar un análisis de costos con prioridad de los recursos que son necesarios, en base a dicho análisis obtener la aprobación de los directivos empresariales y posteriormente de la dirección financiera.

## 6.7. Fundamentación científica – técnica

La Normativa de seguridad permite sentar las bases de la fiabilidad con que los sistemas informáticos de la empresa prestaran sus servicios, como se custodiara la información de

acuerdo con sus especificaciones funcionales, sin interrupciones, sin modificaciones fuera de control, sin que la información pueda llegar a personas no autorizadas y sin accesos autorizados. La normativa busca establecer las medidas técnicas, administrativas, operativas, organizativas que estén encaminadas a conseguir el nivel de protección adecuado, garantizando el cumplimiento legal en términos tecnológicos, de la disponibilidad, confidencialidad e integridad que toda información debe poseer al estar disponible en sistemas de información y en la red.

## 6.8. Propuesta de normativa de seguridad

### 6.8.1. FASE 1: Situación actual

VER TABLA 33.

**Identificación de vulnerabilidades:**

**Tabla 33:** Vulnerabilidades en la empresa STD S.A.

| DOMINIOS | CRITERIO | DESCRIPCIÓN | RESPONSABLE | CUMPLE | NO CUMPLE |
|---|---|---|---|---|---|
| **A.5. Relativo a políticas de seguridad de la información** | | | | | |
| Directrices establecidas por la dirección para la seguridad de la información. | Políticas para la seguridad de la información. | No definidas | No definido | | **X** |
| | Revisión de políticas para la seguridad de la información. | No existe revisión | No definido | | **X** |
| **A.6. Relativo a organización de la seguridad de la información** | | | | | |
| Organización interna | Roles y responsabilidades para la seguridad de la información. | Variabilidad de roles y responsabilidades. | No definido | | **X** |
| | Separación de deberes. | No es específico la separación de deberes. | No definido | | **X** |
| | Contacto con las autoridades. | Frecuentemente. | **Coordinación de proyectos** | **X** | |
| | Contacto con grupos de interés especial. | Contacto limitado | No definido | | **X** |
| | Seguridad de la información en la gestión de proyectos. | No existe | No definido | | **X** |
| Dispositivos móviles y teletrabajo. | Políticas para dispositivos móviles | No existe | No definido | | **X** |
| | Teletrabajo | No existe | No definido | | **X** |
| **A.7. Relativo a seguridad de los recursos humanos** | | | | | |
| Antes de asumir el empleo.<br>Durante la ejecución del empleo. | Selección | Por perfil profesional, experiencia. | **Director del proyecto** | **X** | |
| | Términos y condiciones de empleo | Definidos en el contrato de trabajo | **Talento Humano** | **X** | |

| | | | | | |
|---|---|---|---|---|---|
| | Responsabilidades de la dirección. | Variabilidad absoluta | No definido | | **X** |
| | Toma de conciencia, educación y formación en la seguridad de la información. | No existe | No definido | | **X** |
| | Proceso disciplinario. | Parcialmente definido | No definido | | **X** |
| Terminación o cambio de empleo. | Terminación o cambio de responsabilidades de empleo. | La terminación es más a criterio personal.<br>Cambio de responsabilidad es a criterio ejecutivo. | No definido | | **X** |
| **A.8 Relativo a gestión de activos** | | | | | |
| Responsabilidad por los activos. | Inventario de activos | Si existe | **Control de Activos** | **X** | |
| | Propiedad de los activos | Si existe | **Control de Activos** | **X** | |
| | Uso aceptable de los activos | Parcialmente, varios responsables. | No definido | | **X** |
| | Devolución de los activos | Si existe | **Control de Activos** | **X** | |
| Clasificación de la información. | Clasificación de la información | No existe | No definido | | **X** |
| | Etiquetado de la información | No existe | No definido | | **X** |
| | Manipulado de la información | No existe | No definido | | **X** |
| | Gestión de medios removibles | No existe | No definido | | **X** |
| | Disposición de los medios | No existe | No definido | | **X** |
| | Transferencia de medios físicos | Si existe | **Control de Activos** | **X** | |

| | | | | | |
|---|---|---|---|---|---|
| **A.9. Relativo a control de accesos** | | | | | |
| Requisitos del negocio para el control de acceso. | Política de control de acceso. | No existe | No definido | | **X** |
| | Política sobre el uso de los servicios de red. | No existe | No definido | | **X** |
| Gestión de accesos de usuarios. | Registro y cancelación del registro de usuarios. | No existe | No definido | | **X** |
| | Suministro de acceso de usuarios. | No existe | No definido | | **X** |
| | Gestión de derechos de acceso de privilegiado. | No existe | No definido | | **X** |
| | Gestión de información de autenticación secreta de usuarios. | No existe | No definido | | **X** |
| | Revisión de los derechos de acceso de usuarios. | No existe | No definido | | **X** |
| | Retiro o ajuste de los derechos de acceso. | No existe | No definido | | **X** |
| Responsabilidad de los usuarios. | Uso de la información de autenticación secreta. | No existe | No definido | | **X** |
| Control de acceso a sistemas y aplicaciones. | Restricción de acceso a la información. | No existe | No definido | | **X** |
| | Procedimiento de ingreso seguro. | No existe | No definido | | **X** |
| | Sistemas de gestión de contraseñas. | No existe | No definido | | **X** |
| | Uso de programas utilitarios privilegiados. | No existe | No definido | | **X** |
| | Control de acceso a código fuente de programas. | No existe | No definido | | **X** |
| **A.10. Relativo a criptografía** | | | | | |
| Controles criptográficos | Política sobre el uso de controles criptográficos. | No existe | No definido | | **X** |

| | | | | | |
|---|---|---|---|---|---|
| | Gestión de llaves. | No existe | No definido | | **X** |
| **A.11. Relativo a Seguridad Física y Ambiental** | | | | | |
| Áreas seguras | Perímetro de seguridad física | No existe | No definido | | **X** |
| | Controles físicos de entrada | No existe | No definido | | **X** |
| | Seguridad de oficinas, recintos e instalaciones. | No existe | No definido | | **X** |
| | Protección contra amenazas externas y ambientales. | No existe | No definido | | **X** |
| | Trabajo en áreas seguras. | No existe | No definido | | **X** |
| | Áreas de despacho y carga. | No existe | No definido | | **X** |
| Equipos | Ubicación y protección de los equipos. | No existe | No definido | | **X** |
| | Servicios de suministro. | Existe mayoritariamente | Proveedores | **X** | |
| | Seguridad de cableado. | **Si existe** | Proveedores | **X** | |
| | Mantenimiento de equipos. | **Si existe** | **Soporte tecnológico** | **X** | |
| | Retiro de activos. | **Si existe** | **Control de Activos** | **X** | |
| | Seguridad de equipos y activos fuera de las instalaciones. | No existe | No definido | | **X** |
| | Disposición segura o reutilización de equipos. | **Si existe** | **Soporte tecnológico** | **X** | |
| | Equipos de usuarios desatendidos. | Si existe | No definido | | **X** |
| | Política de escritorio limpio y pantalla limpia. | No existe | No definido | | **X** |

| | | | | | |
|---|---|---|---|---|---|
| **A.12. Relativo a seguridad de las operaciones** | | | | | |
| Procedimientos operaciones y responsabilidades. | Procedimientos de operación documentados. | **Si existe** | **Metodología** | **X** | |
| | Gestión de cambios. | **Si existe** | **Metodología** | **X** | |
| | Gestión de capacidad. | No existe | No definido | | **X** |
| | Separación de los ambientes de desarrollo, pruebas y operación. | No existe | No definido | | **X** |
| Protección contra códigos maliciosos. | Controles contra códigos maliciosos. | **Si existe** | **Soporte tecnológico** | **X** | |
| Copias de respaldo. | Respaldos de información. | Existe parcialmente | No definido | | **X** |
| Registro y seguimiento. | Registro de eventos. | Existe parcialmente | No definido | | **X** |
| | Protección de la información de registro. | Existe parcialmente | No definido | | **X** |
| | Registros del administrador y del operador. | Existe parcialmente | No definido | | **X** |
| | Sincronización de relojes. | No existe | No definido | | **X** |
| Control de software operacional. | Instalación de software en sistemas operativos. | **Si existe** | **Soporte tecnológico** | **X** | |
| Gestión de la vulnerabilidad técnica. | Gestión de las vulnerabilidades técnicas. | Existe parcialmente | No definido | | **X** |
| | Restricciones sobre la instalación de software. | No existe | No definido | | **X** |
| Consideraciones sobre auditorias de sistemas de información. | Información controles de auditoria de sistemas. | No existe | No definido | | **X** |
| **A.13. Relativo a seguridad en las comunicaciones** | | | | | |
| | Controles de redes | Existe parcialmente | No definido | | **X** |

| | | | | | |
|---|---|---|---|---|---|
| Gestión de la seguridad de las redes. | Seguridad de los servicios de red. | Existe parcialmente | No definido | | **X** |
| | Separación en las redes. | **Si existe** | No definido | | **X** |
| Transferencia de información. | Políticas y procedimientos de transferencia de información. | No existe | No definido | | **X** |
| | Acuerdos sobre transferencia de información. | No existe | No definido | | **X** |
| | Mensajería electrónica. | **Si existe** | No definido | | **X** |
| | Acuerdos de confidencialidad o de no divulgación. | **Si existe** | **Talento Humano** | **X** | |
| **A.14. Relativo a adquisición, desarrollo y mantenimientos de sistemas** | | | | | |
| Requisitos de seguridad de los sistemas de información. | Análisis y especificación de requisitos de seguridad de la información. | No existe | No definido | | **X** |
| | Seguridad de servicios de las aplicaciones en redes públicas. | Si existe | No definido | | **X** |
| | Protección de transacciones de los servicios de las aplicaciones. | No existe | No definido | | **X** |
| Seguridad en los procesos de desarrollo y soporte. | Política de desarrollo seguro | No existe | No definido | | **X** |
| | Procedimientos de control de cambios en sistemas. | No existe | No definido | | **X** |
| | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. | Si existe | No definido | | **X** |
| | Restricciones en los cambios a los paquetes de software. | No existe | No definido | | **X** |
| | Principios de construcción de sistemas seguros. | No existe | No definido | | **X** |
| | Ambiente de desarrollo seguro. | **Si existe** | **Metodología** | **X** | |

| | | | | | |
|---|---|---|---|---|---|
| | Desarrollo contratado externamente. | No existe | No definido | | **X** |
| | Pruebas de seguridad de sistemas. | No existe | No definido | | **X** |
| | Pruebas de aceptación de sistemas. | Existe parcialmente | No definido | | **X** |
| Datos de prueba | Protección de datos de prueba. | No existe | No definido | | **X** |
| **A.15. Relativo a relación con proveedores** | | | | | |
| Seguridad de la información en las relaciones con los proveedores. | Política de seguridad de la información para las relaciones con los proveedores. | **Si existe** | No definido | | **X** |
| | Tratamiento de la seguridad dentro de los acuerdos con proveedores. | **Si existe** | No definido | | **X** |
| | Cadena de suministro de tecnología de información y comunicación. | No existe | No definido | | **X** |
| Gestión de la prestación de servicios con los proveedores. | Seguimiento y revisión de los servicios de los proveedores. | No existe | **Infraestructura tecnológica** | **X** | |
| | Gestión de cambios en los servicios de proveedores. | Si existe | **Infraestructura tecnológica** | **X** | |
| **A.16. Relativo a gestión de incidentes de seguridad de la información** | | | | | |
| Gestión de incidentes y mejoras en la seguridad de la información. | Responsabilidad y procedimientos. | No existe | No definido | | **X** |
| | Reporte de eventos de seguridad de la información. | No existe | No definido | | **X** |
| | Reporte de debilidades de seguridad de la información. | No existe | No definido | | **X** |
| | Evaluación de eventos de seguridad de la información y decisiones sobre ellos. | No existe | No definido | | **X** |
| | Respuesta a incidentes de seguridad de la información. | No existe | No definido | | **X** |
| | Aprendizaje obtenido de los incidentes de seguridad de la información. | **Si existe** | No definido | | **X** |

| | | | | | |
|---|---|---|---|---|---|
| | Recolección de evidencia. | No existe | No definido | | **X** |
| **A.17. Relativo a aspectos de seguridad de la información dentro de la continuidad del negocio** | | | | | |
| Continuidad de seguridad de la información. | Planificación de la continuidad de la seguridad de la información. | No existe | No definido | | **X** |
| | Implementación de la continuidad de la seguridad de la información. | No existe | No definido | | **X** |
| | Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | No existe | No definido | | **X** |
| Redundancias | Disponibilidad de instalaciones de procesamiento de información. | No existe | No definido | | **X** |
| **A.18. Relativo a Conformidad** | | | | | |
| Cumplimiento de requisitos legales y contractuales. | Identificación de la legislación aplicable y los requisitos contractuales. | **Si existe** | **Departamento legal** | **X** | |
| | Derechos de propiedad intelectual. | **Si existe** | **Departamento legal** | **X** | |
| | Protección de registros. | No existe | No definido | | **X** |
| | Privacidad y protección de datos personales. | No existe | No definido | | **X** |
| | Reglamentación de controles criptográficos. | No existe | No definido | | **X** |
| Revisión de seguridad de la información. | Revisión independiente de la seguridad de la información. | No existe | No definido | | **X** |
| | Cumplimiento con las políticas y normas de seguridad. | No existe | No definido | | **X** |
| | Revisión del cumplimiento técnico. | No existe | No definido | | **X** |

**Elaborado por:** Investigador

**Resumen general de vulnerabilidades**

**Tabla 34:** Resumen Vulnerabilidades

| DOMINIOS ISO 27001:2013 | TOTAL, CRITERIOS | CUMPLEN | NO CUMPLEN |
|---|---|---|---|
| **A.5. Relativo a Políticas de seguridad de la información** | 2 | 0 | 2 |
| **A.6. Relativo a Organización de la seguridad de la información** | 7 | 1 | 6 |
| **A.7. Relativo a Seguridad de los recursos humanos** | 6 | 2 | 4 |
| **A.8 Relativo a Gestión de Activos** | 10 | 4 | 6 |
| **A.9. Relativo a Control de Accesos** | 14 | 0 | 14 |
| **A.10. Relativo a Criptografía** | 2 | 0 | 2 |
| **A.11. Relativo a Seguridad Física y Ambiental** | 15 | 5 | 10 |
| **A.12. Relativo a Seguridad de las Operaciones** | 14 | 4 | 10 |
| **A.13. Relativo a Seguridad en las comunicaciones** | 7 | 1 | 6 |
| **A.14. Relativo a Adquisición, desarrollo y mantenimientos de sistemas** | 13 | 1 | 12 |
| **A.15. Relativo a Relación con proveedores** | 5 | 2 | 3 |
| **A.16. Relativo a Gestión de incidentes de seguridad de la información** | 7 | 0 | 7 |
| **A.17. Relativo a Aspectos de seguridad de la información dentro de la continuidad del negocio** | 4 | 0 | 4 |
| **A.18. Relativo a Conformidad** | 8 | 2 | 6 |
| **Total:** | **114** | **22** | **92** |
| **Porcentaje (%)** | **100%** | **19,30%** | **80,70%** |

**Elaborado por:** Investigador

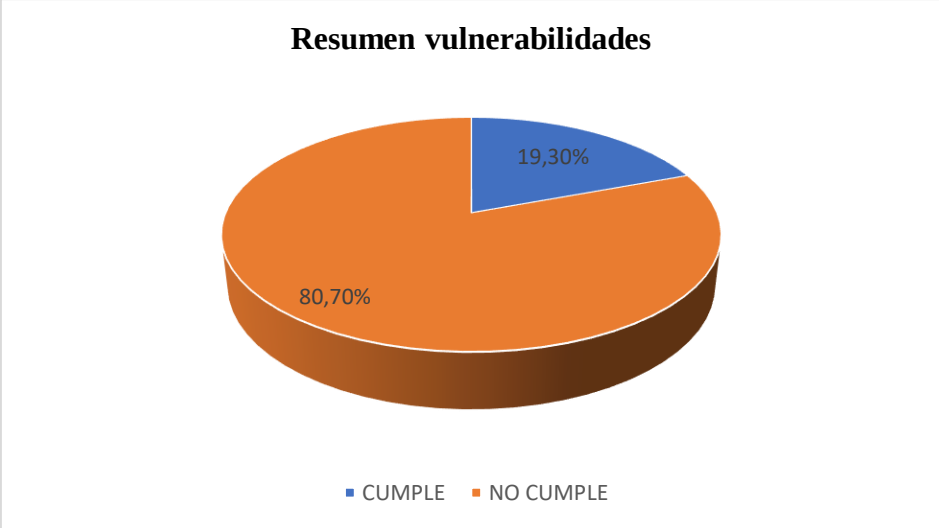



**Gráfico 34:** Resumen vulnerabilidades
**Elaborado por:** Investigador

**Resultados:** Se evidencia que en las empresas de desarrollo de software el cumplimiento con los criterios que establece la Norma ISO 27001:2013 en tema de Gestión de la seguridad de la información es tan solo el 19,30%, frente al 80,70% de criterios no cumplidos.

**Análisis:** Se concluye que las empresas de desarrollo de software minoritariamente cumplen con los dominios, criterios e indicadores de la NORMA ISO 27001:2013; para asegurar su permanencia y posicionamiento en el mercado de las TIC's (Tecnologías de la Información y Comunicación) es necesario cumplir con las exigencias de la Norma Internacional.

**Análisis de vulnerabilidades (tecnológicas)**

Para realizar el análisis de las vulnerabilidades, se toma en cuenta pruebas tecnológicas concretas como es el escaneo de puertos, vulnerabilidad de la URL empresarial, información del DNS, tráfico de la red y los complementos de navegadores; con el uso y aplicación de software libre especializado, por las razones expuestas a continuación:

**a) Escaneo de puertos**

Para el escaneo de puertos se utilizó la herramienta **PortScan & Stuff**, es un explorador de redes que permitió encontrar con rapidez los puertos abiertos de los equipos conectados a la red, identificar las versiones de los programas que se están ejecutando en los puertos detectados.

Es necesario aplicar el escaneo de puertos a la red tecnológica de STD S. A, para identificar que puertos están abiertos correctamente, su información básica; el escaneo ayudara a buscar posibles agujeros en cada uno de los servicios, ya que cada puerto abierto es una potencial entrada para los atacantes convirtiéndose en una vulnerabilidad tecnológica.

Se realizo el escaneo de puertos a la red de STD S. A., el resultado obtenido es que los puertos 135, 139 y 445 en el segmento 1 de análisis 192.168.3.0 – 192.168.3.16 están abiertos, lo que se convierte en una vulnerabilidad de puertos en la red empresarial, como se muestra a continuación:

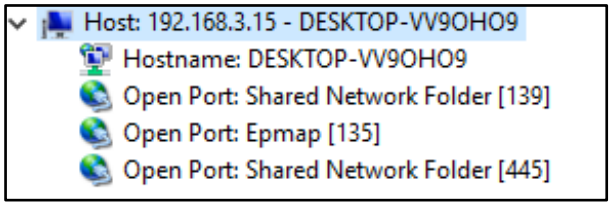



**Gráfico 35:** Escaneo de puertos – segmento 1
**Elaborado por:** Investigador

Para el segmento 2 de red 192.168.0.1 / 192.168.0.254 están abiertos los puertos: 135, 443, 445, 1433, 3306, 3389.

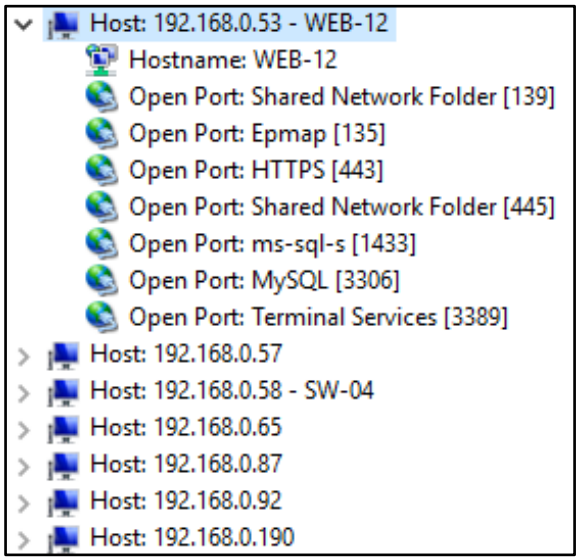



**Gráfico 36:** Escaneo de puertos – segmento 2
**Elaborado por:** Investigador

Para el segmento 3 de red 192.168.3.1 / 192.168.3.254 están abiertos los puertos: 22, 53.

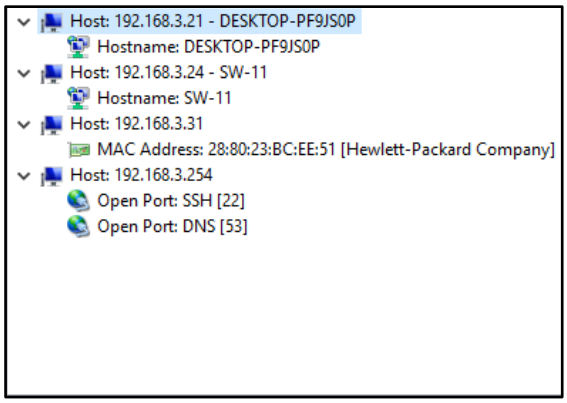



**Gráfico 37:** Escaneo de puertos – segmento 3
**Elaborado por:** Investigador

## b) Vulnerabilidad de la URL

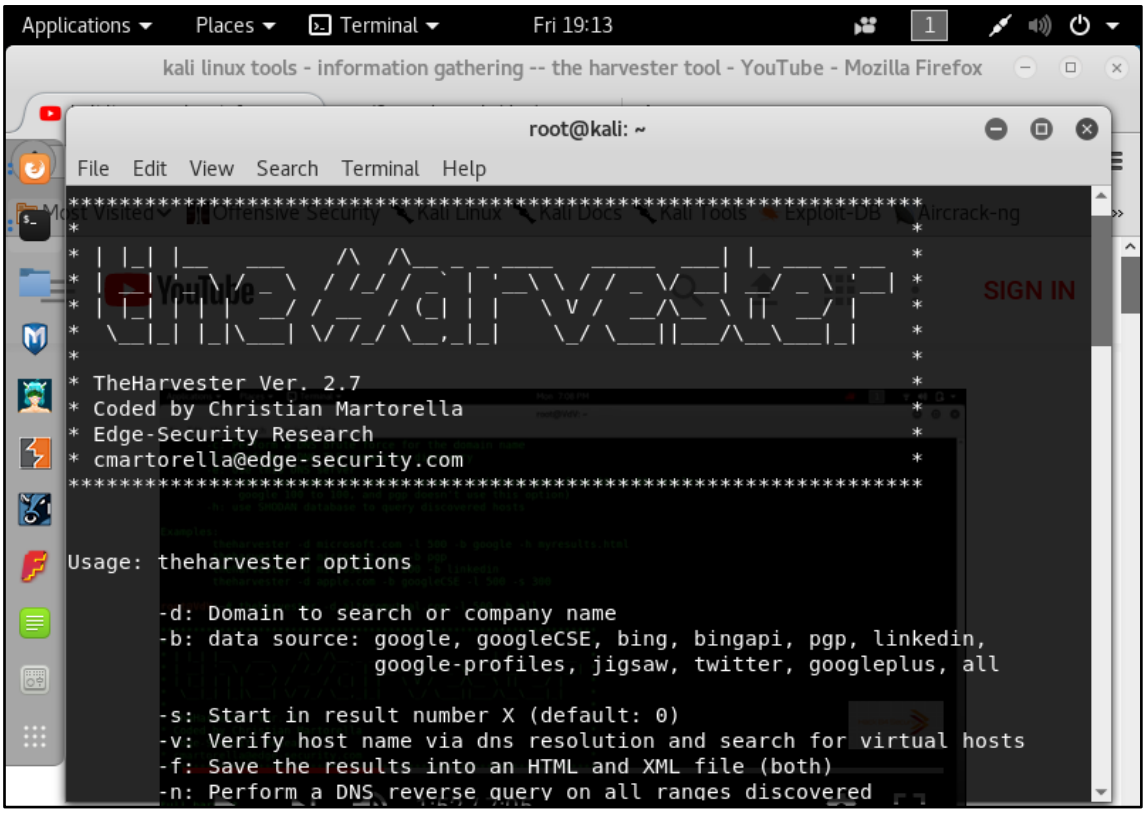



**Gráfico 38:** Vulnerabilidad URL 1
**Elaborado por:** Investigador

El acceso a las diferentes rutas de las aplicaciones disponibles puede ser por la (s) URL (URL: Localizador de recursos uniforme) obteniendo información relevante de los emails corporativos, subdominios, host, nombres de personal de trabajo. Realizar pruebas de penetración para conocer las huellas de los posibles clientes en internet, además es muy útil para identificar que puede un atacante ver de la empresa.

El análisis de Vulnerabilidades a la URL empresarial, se realizan con la herramienta The Harvester, de manera efectiva obteniendo los siguientes resultados: Datos de los motores de búsqueda, URL del host de STD, cuentas de correo electrónicas.

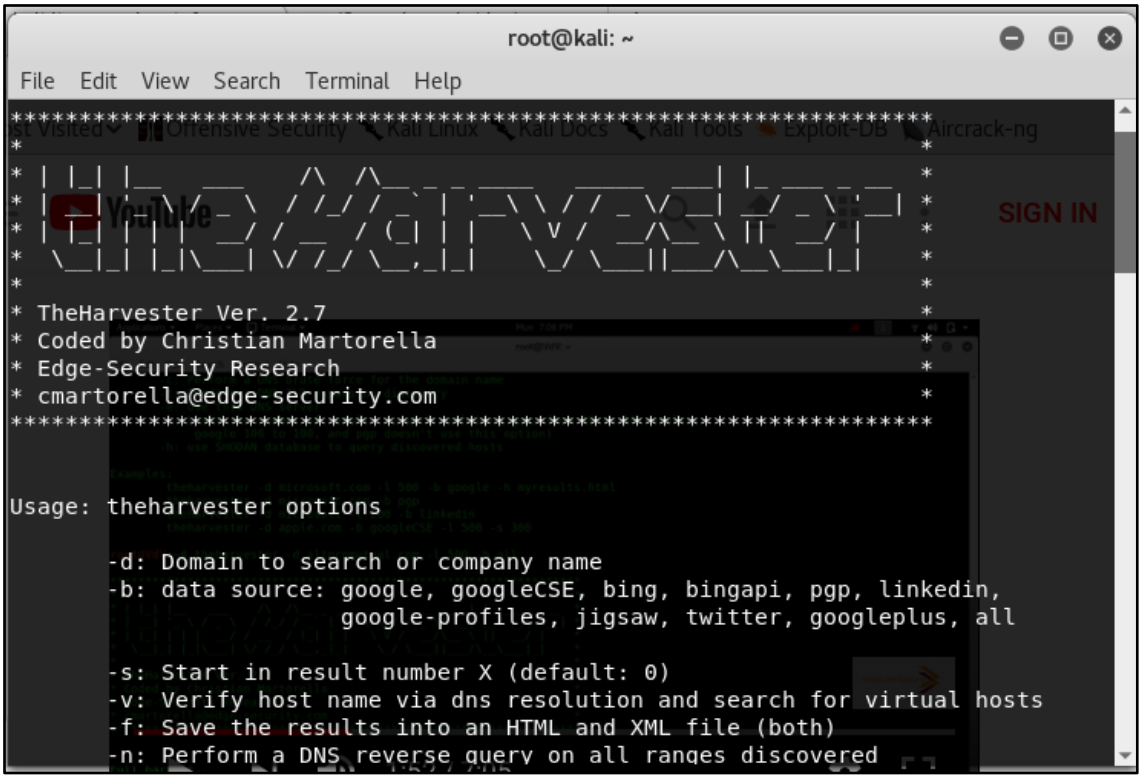



**Gráfico 39:** Vulnerabilidad URL 2
**Elaborado por:** Investigador

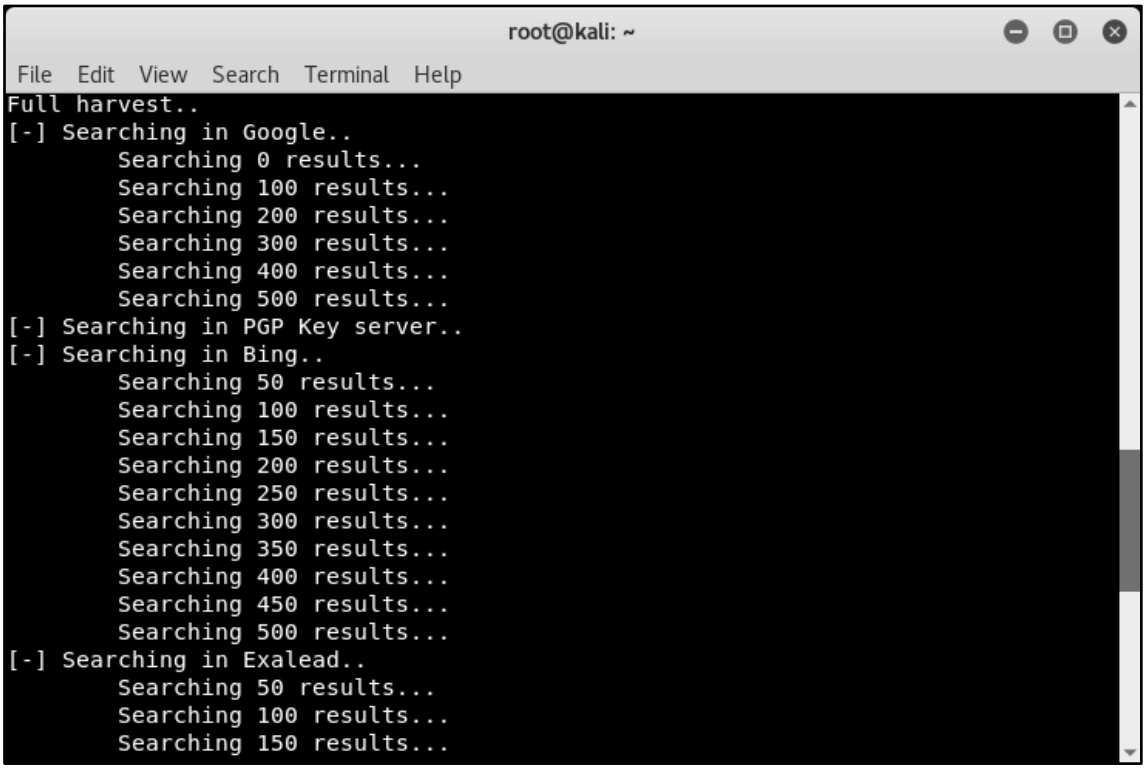



**Gráfico 40:** Vulnerabilidad URL 3
**Elaborado por:** Investigador

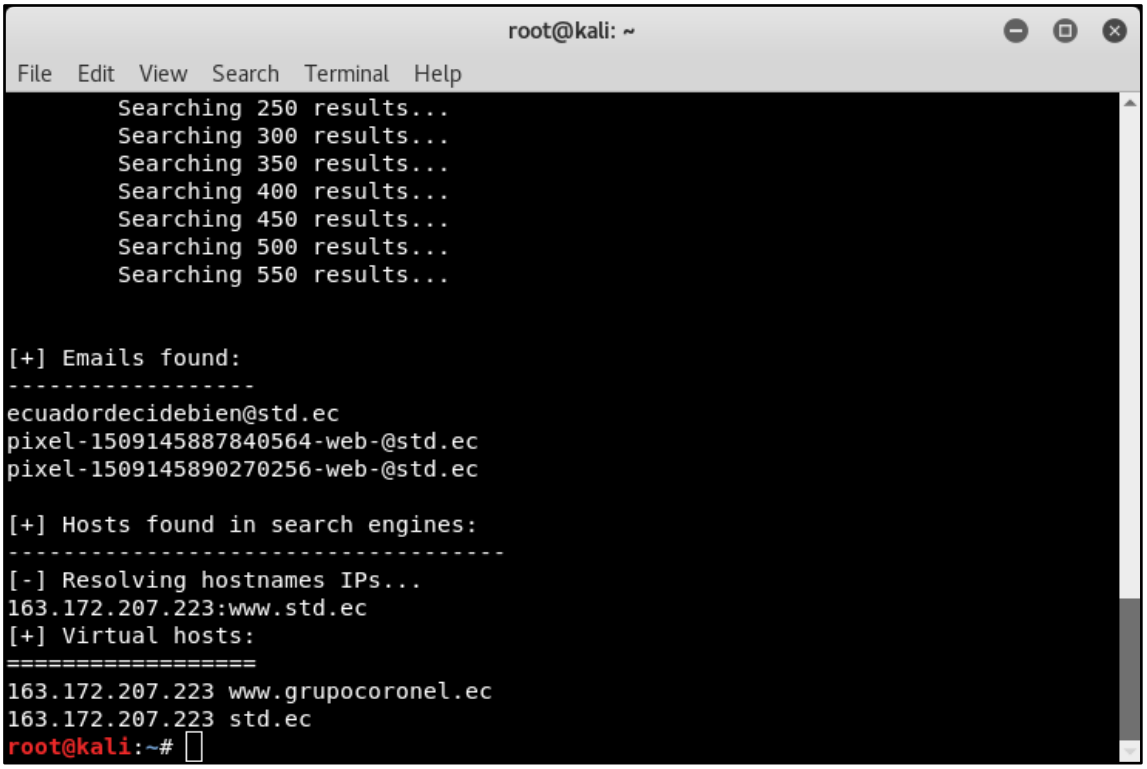



**Gráfico 41:** Vulnerabilidad URL 4
**Elaborado por:** Investigador

### c) Información del DNS

Para este caso de pruebas se obtuvo el nombre del host, los servidores que maneja, direcciones IP y el puerto que usa: VER GRÁFICO N° 42, 43, 44.

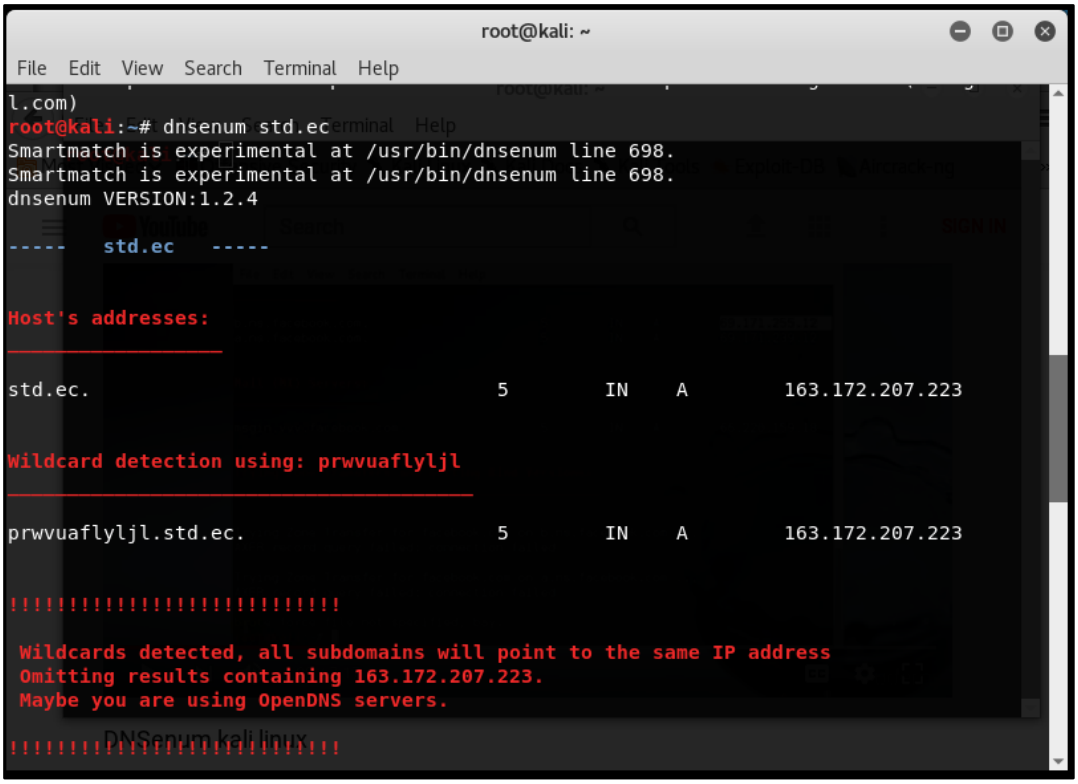



**Gráfico 42:** Información del DNS
**Elaborado por:** Investigador

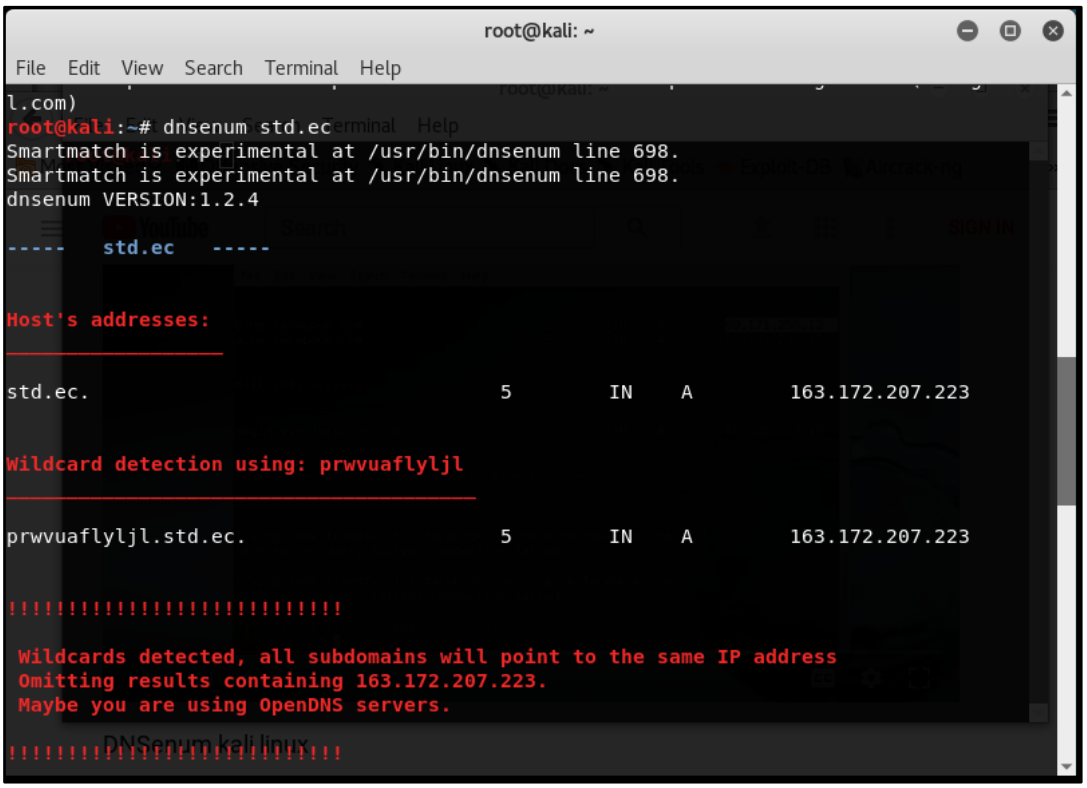



**Gráfico 43:** Información del DNS
**Elaborado por:** Investigador

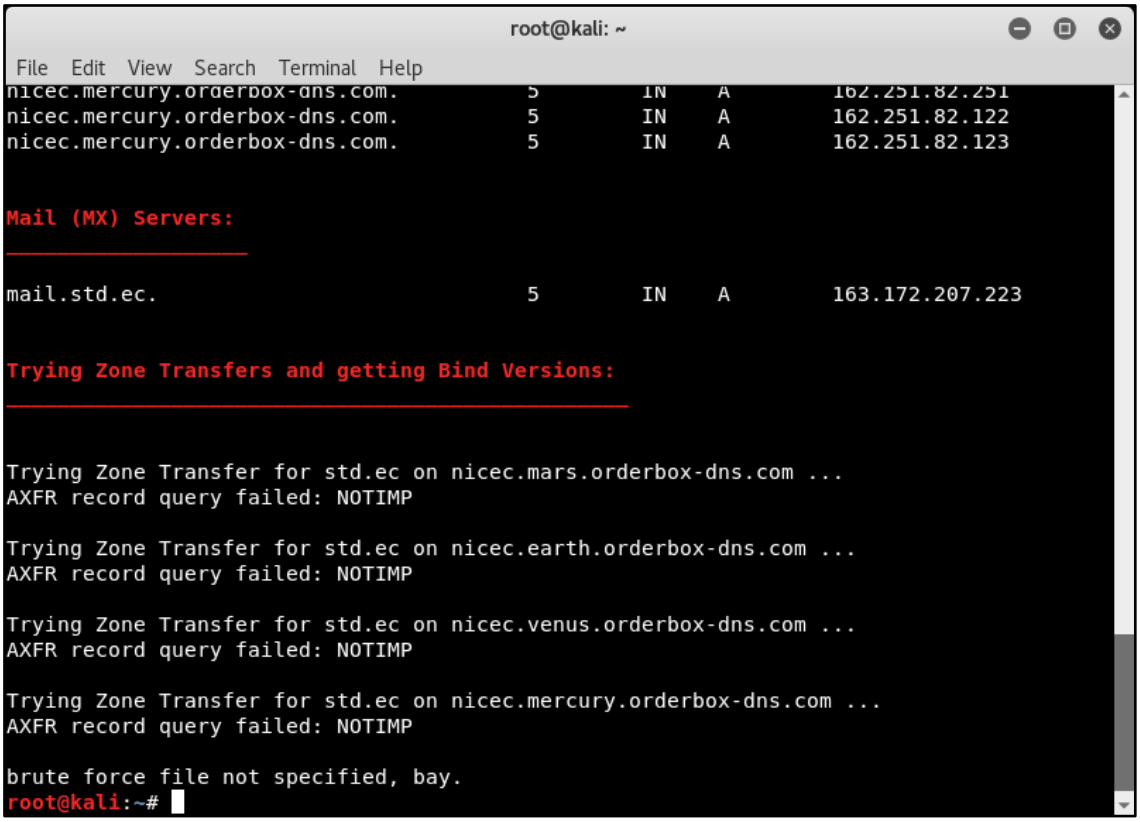



**Gráfico 44:** Información del DNS
**Elaborado por:** Investigador

El propósito es capturar la información que sea posible del dominio web empresarial, dicha información es muy útil cuando se dispone hacer pruebas de seguridad al dominio. Mediante la herramienta DNSenum se llega a obtener los siguientes parámetros: servidores DNS, servidores de nombres que proporcionan información del proveedor de alojamiento que se utiliza, registro MX en el que se puede ver el servidor de correo del host destino.

**d) Tráfico de la red**

Analizar el tráfico en la red, es una prueba para detectar él envió de información, escuchar el tráfico que se produce en la red de comunicaciones, controlar que ningún virus o el mal funcionamiento de una tarjeta de red estuviera provocando una inundación de tráfico que puede disminuir el rendimiento de la red. Con el uso de la herramienta Wireshark, multiplataforma, se captura los paquetes que sale o entra en la red y desde la red (ethernet y wifi), mostrando resultados de la lista de paquetes que van llegando, información de los

paquetes y la información binaria de los paquetes, con opciones para filtrar solo la información de interés luego de la captura de un paquete.

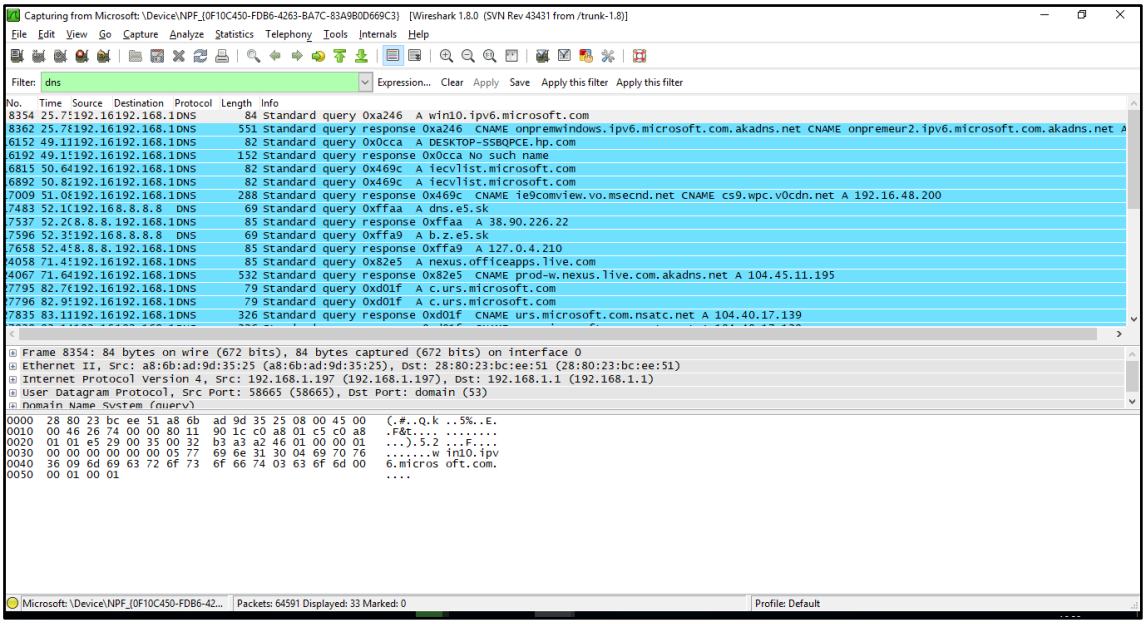



**Gráfico 45:** Tráfico de la red
**Elaborado por:** Investigador

Se identifico que existe navegación en páginas como Microsoft.com, officeapps.live.com, facebook, youtube; en el caso de redes sociales su uso es una debilidad que posee la empresa, el uso de páginas exclusivas para videos consume muchos recursos de ancho de banda y más aún cuando el número de conectados supera a los 40 diarios.

### e) Complementos de navegadores

Consultar la configuración de los complementos del navegador Mozilla Firefox, se identifica que, si existe software desactualizado, lo que provoca que los equipos/ordenadores sean vulnerable a los ataques. Firefox ofrece complementos clasificados como herramientas de evaluación de la accesibilidad web, que ayudan a personalizar el navegador, mejorar el rendimiento y su funcionalidad.

### Parámetros de seguridad de la información

Para diseñar la normativa de seguridad de la información se definen los parámetros, identificados a partir del análisis de la información recolectada en las empresas de desarrollo de software en la ciudad de Riobamba, el nivel de cumplimiento y no cumplimiento de los criterios de seguridad que establece la Norma ISO 27001 por parte

de la empresa STD S. A., por lo que dichos parámetros se establecen por prioridad, siendo su estructura la siguiente: VER GRÁFICO 46.

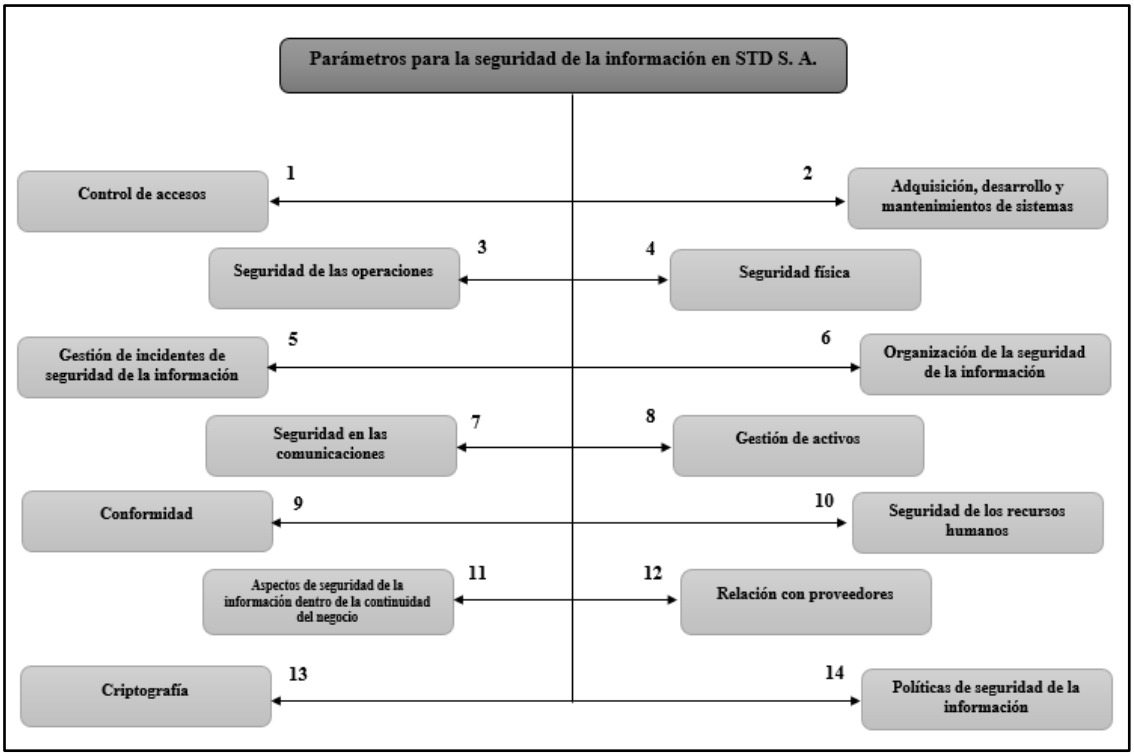



**Gráfico 46:** Parámetros para la seguridad de la información en S.T.D S.A.
**Elaborado por:** Investigador

### 6.8.2. FASE 2: Diseño de la normativa de seguridad

a) Control de accesos

**Tabla 35:** Control de accesos

| **Objetivo:** | Limitar el acceso a los recursos de tratamiento de información y a la información. |
|---|---|
| **Criterios de seguridad** | |
| Política de control de acceso. | Se debe considerar las siguientes directrices:<br>Lógicos y físicos.<br>Se deberá tener en cuenta lo siguiente:<br>• Los requisitos de seguridad de las aplicaciones del negocio.<br>• Consistencia entre los derechos de acceso y las políticas de clasificación de la información de sistemas y redes.<br>• La legislación aplicable y cualquier obligación contractual relativa a la limitación de acceso a datos o servicios.<br>• La gestión de los derechos de acceso en un entorno distribuido e interconectado que reconozca todo tipo de conexiones disponibles.<br>• La segregación de las funciones en el control de acceso de diversos roles.<br>• Los requisitos para la autorización formal de las peticiones de accesos. |

| | |
|---|---|
| | • Los requisitos para la revisión periódica de los derechos de acceso.<br>• Los roles con derechos de accesos privilegiados.<br>(AENOR, 2015) |
| Política sobre el uso de los servicios de red. | Se debe considerar las siguientes directrices:<br>Se formula una política para el uso de redes y los servicios de red, en dicha política de especifica lo siguiente:<br>• Las redes y los servicios de red a los que está permitido el acceso.<br>• Los procedimientos de autorización que determinen quien tiene permitido el acceso a qué redes y a que servicios de red.<br>• Los controles para la gestión y los procedimientos para proteger el acceso a las conexiones de red y a los servicios de red.<br>• Los medios usados para acceder a las redes o a los servicios de red.<br>• Los requisitos de autenticación de usuarios para el acceso a los servicios de red.<br>(AENOR, 2015) |
| Registro y cancelación del registro de usuarios. | Se debe considerar las siguientes directrices:<br>El proceso para la gestión de los identificadores de usuarios debería incluir:<br>• Uso de identificadores (ID) de usuario que le identifiquen y le hagan responsable de sus acciones (aprobados y documentados).<br>• La inhabilitación o eliminación inmediata de los identificadores (ID) de usuarios que dejan la empresa.<br>• La identificación periódica y eliminación o inhabilitación de identificadores de usuarios redundantes,<br>• La identificación es única por usuario.<br>(AENOR, 2015) |
| Suministro de acceso de usuarios. | Se debe considerar las siguientes directrices:<br>El proceso para la asignación o revocación de los derechos de accesos concedidos a los identificadores (ID) del usuario deben incluir:<br>• Obtener la autorización del propietario del sistema de información o del servicio para el uso de éste.<br>• Verificar que el nivel de acceso concedido es apropiado de acuerdo a las políticas de acceso, coherente con otros requisitos, tales como la segregación de funciones.<br>• Asegurar que los derechos de acceso no se activan hasta concluir con los procedimientos de autorización.<br>• Mantener un registro centralizado de los derechos de acceso a sistemas de información y servicios concedidos a un identificador de usuario.<br>• Adaptar los derechos de acceso de usuario que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han abandonado la empresa.<br>• Revisar periódicamente los derechos de acceso concedidos con los propietarios de los sistemas de información o de los servicios.<br>(AENOR, 2015) |
| Gestión de derechos de acceso de privilegiado. | Se debe considerar las siguientes directrices:<br>• Debe identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso junto con los usuarios a los que hay que asignarlos. |

| | |
|---|---|
| | • Los derechos de acceso privilegiados deben asignarse en base a la necesidad de uso, caso a caso de acuerdo con la política de control de acceso.<br>• Debe mantenerse un proceso de autorización y registro de todos los privilegios asignados.<br>• Definirse los requisitos para el vencimiento de los derechos de acceso privilegiados.<br>• Los derechos de acceso privilegiados deben asignarse a un identificador de usuario diferente al usado en las actividades normales del negocio.<br>• Debe revisarse regularmente las competencias de los usuarios con derechos de acceso privilegiados verificando que correspondan con sus tareas.<br>(AENOR, 2015) |
| Gestión de información de autenticación secreta de usuarios. | Se debe considerar las siguientes directrices:<br>• De los usuarios la firma de un compromiso de mantener la confidencialidad de la información secreta para la autenticación personal y mantener la información de autenticación secreta del grupo entre todos los miembros, dicho compromiso firmado se debe incluir en los términos y condiciones de empleo.<br>• Si se requiere de los usuarios mantener su autenticación secreta, al inicio proporcionarles información de autenticación temporal y que sea cambiada en su primer uso.<br>• Establecerse procedimientos para verificar la identidad de un usuario antes de proporcionarle la información de autenticación secreta ya sea nueva, de sustitución o provisional.<br>• La información de autenticación secreta será proporcionada a los usuarios de manera segura, evitando el uso de terceras partes o de correos electrónicos no protegidos.<br>• La información de autenticación secreta temporal es única para el individuo y no se debe poder adivinar.<br>• Los usuarios deberían confirmar la recepción de la información de autenticación secreta.<br>(AENOR, 2015) |
| Revisión de los derechos de acceso de usuarios. | Se debe considerar las siguientes directrices:<br>• Los derechos de acceso de usuario deben revisarse a intervalos regulares y tras cualquier cambio.<br>• Los derechos de acceso de usuario deben revisarse y reasignarse cuando este cambie de rol dentro de la misma empresa.<br>• Las autorizaciones de derechos de accesos privilegiados deberían revisarse a intervalos frecuentes.<br>• La asignación de privilegios debe verificarse a intervalos regulares para asegurar que no se han obtenido privilegios no autorizados.<br>• Los cambios en cuentas privilegiadas deben registrarse para su revisión periódica.<br>(AENOR, 2015) |
| Retiro o ajuste de los derechos de acceso. | Se debe considerar las siguientes directrices:<br>• Si la finalización o el cambio de puesto de trabajo la inicia el empleado, el usuario de la tercera parte o la Dirección, así como la razón para la finalización.<br>• Las responsabilidades actuales del empleado, del usuario de la tercera parte o cualquier otro usuario. |

| | |
|---|---|
| | • El valor de los activos accesibles en ese momento.<br>(AENOR, 2015) |
| Uso de la información de autenticación secreta. | Se debe considerar las siguientes directrices, los usuarios deben ser advertidos de:<br>• Mantener confidencial la información de autenticación, asegurando que no se divulgue a cualquier otra parte.<br>• Evitar guardar la información secreta de autenticación en un fichero software, en papel, o un dispositivo portátil; a no ser que ésta pueda ser almacenada de forma segura y que el método de almacenamiento haya sido probado.<br>• Cambiar la información secreta de autenticación, seleccionar contraseñas de calidad, con una longitud mínima suficiente que sean: fáciles de recordar, que no estén basadas en algo que alguien más pueda adivinar con facilidad u obtener usando información asociada a la persona, que no sea vulnerable a ataques de diccionario, libres de caracteres consecutivos ya sean alfabéticos o numéricos, si es temporal que sea cambiada en el primer inicio se sesión.<br>• No compartir la información secreta de autenticación individual del usuario.<br>(AENOR, 2015) |
| Restricción de acceso a la información. | Para apoyar los requisitos de restricción de acceso se considera las siguientes directrices:<br>• Proporcionar menús para el control de acceso a las funciones del sistema de aplicaciones.<br>• Controlar que datos pueden ser accedidos por un usuario determinado.<br>• Controlar los derechos de acceso de los usuarios.<br>• Controlar los derechos de acceso de otras aplicaciones.<br>• Limitar la información contenida en las salidas del sistema.<br>• Proporcionar controles de acceso físico y lógico para aislar las aplicaciones sensibles, los datos de aplicación o los sistemas.<br>(AENOR, 2015) |
| Procedimiento de ingreso seguro. | Se debe considerar las siguientes directrices:<br>• Mostrar un aviso general de que únicamente deben acceder al ordenador los usuarios autorizados.<br>• No proporcionar mensajes de ayuda durante el proceso de entrada que pudieran ayudar a un usuario no autorizado.<br>• Validar la información de un inicio de sesión, solo cuando se hayan completado todos los datos.<br>• Proteger contra intentos de fuerza bruta de inicio de sesión.<br>• Registrar los intentos con y sin éxitos ocurridos.<br>• Mostrar la siguiente información tras completar con éxito el inicio de sesión (fecha y hora del anterior inicio de sesión con éxito, los detalles de cualquier intento de inicio de sesión sin éxito).<br>• No mostrar contraseñas que se han introducido.<br>• No transmitir por red contraseñas sin cifrar.<br>• Terminar las sesiones inactivas tras un periodo definido de inactividad.<br>(AENOR, 2015) |
| Sistemas de gestión de contraseñas. | Se debe considerar las siguientes directrices:<br>• Usar identificadores de usuario y contraseñas individuales para mantener la responsabilidad. |

| | |
|---|---|
| | • Permitir a los usuarios escoger y cambiar sus propias contraseñas.<br>• Imponer la selección de contraseñas de calidad.<br>• Forzar a los usuarios cambiar sus contraseñas tras el primer inicio de sesión.<br>• Forzar cambios regulares de contraseñas y bajo petición.<br>• Mantener un registro de contraseñas usadas anteriormente y evitar su reutilización.<br>• No mostrar las contraseñas en la pantalla cuando se estén introduciendo.<br>• Almacenar los ficheros de contraseñas de manera separada de los datos del sistema de aplicación.<br>• Almacenar y transmitir las contraseñas de manera protegida.<br>(AENOR, 2015) |
| Uso de programas utilitarios privilegiados. | Se debe considerar las siguientes directrices:<br>• Uso de procedimientos de identificación, autenticación y autorización para los programas de utilidades.<br>• Segregación de los programas de utilidades del software de aplicaciones.<br>• Limitar el uso de programas de utilidades al mínimo número viable de usuarios autorizados y de confianza.<br>• Limitar la disponibilidad de los programas de utilidades.<br>• Registrar todo uso de programas de utilidades.<br>• Definir y documentar los niveles de autorización para los programas de utilidades.<br>• Eliminar o inhabilitar todos los programas de utilidades que no sean necesarios.<br>(AENOR, 2015) |
| Control de acceso a código fuente de programas. | Se debe considerar las siguientes directrices:<br>El acceso al código fuente de programas y elementos relacionados debe estar controlado estrictamente para prevenir la introducción de funcionalidades no autorizadas y para evitar cambios no intencionados, así como para mantener la confidencialidad de la propiedad intelectual de valor. Para el código fuente de programas, esto puede considerarse controlando el almacenamiento centralizado del mismo, preferiblemente en librerías de programas fuente. Se debe considerar las directrices siguientes para controlar el acceso a dichas librerías de programas fuentes:<br>• Las librerías de programas fuente no deberían guardarse en los sistemas en producción o en explotación.<br>• El código fuente de programas y las librerías de programas deben gestionarse de acuerdo con los procedimientos establecidos.<br>• El personal de soporte no debería tener acceso sin restricciones a las librerías de programas fuentes.<br>• La actualización de las librerías de programas fuentes y elementos relacionados y su envío a los programadores debe ejecutarse solo con la autorización adecuada.<br>• Debe mantenerse un registro de auditoria de todos los accesos a las librerías de programas fuente.<br>• El mantenimiento y copia de las librerías de programas fuente debería estar sujeto a procedimientos estrictos de control de cambio.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

b) Adquisición, desarrollo y mantenimiento de sistemas

**Tabla 36:** Adquisición, desarrollo y mantenimiento de sistemas

| **Objetivo:** | Garantizar que la seguridad de la información a través de todo ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas. |
|---|---|
| **Criterios de seguridad** | |
| Análisis y especificación de requisitos de seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Identificar requisitos de seguridad de la información, aplicando métodos derivados del cumplimiento de políticas y normativas, evaluación de incidentes.<br>• Documentar los requisitos identificados.<br>• Requisitos de autenticación de usuarios.<br>• Procesos de aprobación y autorización de accesos para todos los usuarios.<br>• Protección para los activos involucrados (disponibilidad, confidencialidad y la integridad).<br>• Requisitos, derivados de los procesos del negocio.<br>• Requisitos por otros controles de seguridad.<br>(AENOR, 2015) |
| Seguridad de servicios de las aplicaciones en redes públicas. | Se debe considerar las siguientes directrices:<br>• Procesos de autorización asociados con quien puede aprobar, emitir o firmar documentos transaccionales claves.<br>• Garantías de que las partes en comunicación están plenamente informadas de sus autorizaciones para la prestación o uso del servicio.<br>• Acuerdos sobre los requisitos de confidencialidad, integridad, prueba de envío y recepción de documentos clave y el no repudio de los contratos.<br>• Nivel de confianza requerido para la integridad de los documentos claves.<br>• Requisitos de protección de la información confidencial.<br>• Nivel de protección requerido para mantener la confidencialidad e integridad de la información de los pedidos.<br>• Evitar la pérdida o duplicación de información de la transacción.<br>• Responsabilidad asociada con cualquier transacción fraudulenta.<br>(AENOR, 2015) |
| Protección de transacciones de los servicios de las aplicaciones. | Se debe considerar las siguientes directrices:<br>• Utilización de firmas electrónicas para cada una de las partes involucradas en las transacciones.<br>• Considerar aspectos de las transacciones (información secreta de autenticación de los usuarios, transacciones que permanezcan de manera confidencial, privacidad de todas las partes involucradas).<br>• Protocolos seguros utilizados para la comunicación de todas las partes involucradas.<br>• Garantizar que el almacenamiento de los detalles de la transacción se encuentra fuera de cualquier entorno de acceso público.<br>(AENOR, 2015) |
| Política de desarrollo seguro | Se debe considerar las siguientes directrices:<br>• La seguridad del entorno de desarrollo. |

| | |
|---|---|
| | • Directrices sobre la seguridad en el ciclo de vida de desarrollo de software.<br>• Requisitos de seguridad en la fase de diseño.<br>• Puntos de verificación de seguridad incorporados a los hitos del proyecto.<br>• Repositorios seguros.<br>• Seguridad en el control de versiones.<br>• Conocimientos necesarios sobre la seguridad de aplicaciones.<br>• Capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades.<br>(AENOR, 2015) |
| Procedimientos de control de cambios en sistemas. | Se debe considerar las siguientes directrices:<br>• Mantenimiento de un registro de los niveles de autorización aprobados.<br>• Asegurar que los cambios son enviaos a los usuarios autorizados.<br>• Revisión de controles y procedimientos de integridad para asegurar que no se verán comprometidos por los cambios.<br>• Identificación de todo el software, información, entidades de base de datos y el hardware que requieren cambios.<br>• Identificación y comprobación de la seguridad del código crítico para minimizar la probabilidad de fallos se seguridad conocidos.<br>• Aprobación formal de propuestas detalladas.<br>• Aceptación de los cambios por los usuarios autorizados,<br>• Actualización del conjunto de documentación del sistema a la finalización de cada cambio.<br>• Mantenimiento de un control de versiones para todas las actualizaciones de software.<br>• Implantación de los cambios en el momento adecuado en el momento adecuado.<br>(AENOR, 2015) |
| Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. | Se debe considerar las siguientes directrices:<br>• Revisión de procedimientos de control y de integridad de las aplicaciones.<br>• Garantía de que los cambios en los sistemas operativos están previstos en un plazo que permita realizar pruebas y revisiones antes de la implantación.<br>• Realización de los cambios necesarios en los planes de continuidad del negocio.<br>(AENOR, 2015) |
| Restricciones en los cambios a los paquetes de software. | Se debe considerar las siguientes directrices:<br>• Riesgo de que los controles y los procesos de integridad incorporados se vean comprometidos.<br>• Necesidad de obtener el consentimiento del proveedor.<br>• Posibilidad de obtener los cambios necesarios del proveedor como actualizaciones del programa estándar.<br>• Impacto producido si la empresa se convierte en el responsable del mantenimiento futuro del software como resultado de los cambios.<br>• Compatibilidad con otro software en uso.<br>(AENOR, 2015) |
| Principios de construcción de sistemas seguros. | Se debe considerar las siguientes directrices:<br>• Establecer y documentar procedimientos de ingeniería de sistemas de información seguros, basados en principios de |

| | |
|---|---|
| | ingeniería de seguridad y aplicarse a las actividades de ingeniería de sistemas de información.<br>• La seguridad se debe diseñar en todas capas de la arquitectura.<br>• Analizar los riesgos de seguridad de las nuevas tecnologías.<br>• Revisar el diseño contra los patrones de ataques conocidos.<br>• Revisión periódica/Actualizaciones periódicas.<br>• La empresa debe confirmar que el rigor de los principios de ingeniería de seguridad de los proveedores en comparable con el propio.<br>(AENOR, 2015) |
| Ambiente de desarrollo seguro. | Se debe considerar las siguientes directrices:<br>• Sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema.<br>• Requisitos internos y externos aplicables.<br>• Honradez del personal que trabaja en el entorno empresarial.<br>• Controles de seguridad ya implementados por la empresa que apoyen el desarrollo de los sistemas.<br>• Grado de contratación externa asociada con el desarrollo de sistemas.<br>• Control de acceso al entorno de desarrollo.<br>• Monitorización de los cambios en el entorno y el código almacenado en el mismo.<br>• Control del movimiento de datos desde y hacia el entorno.<br>(AENOR, 2015) |
| Desarrollo contratado externamente. | Se debe considerar las siguientes directrices:<br>• Acuerdos de licencias, la propiedad del código y los derechos de la propiedad intelectual, relacionados con los contenidos subcontratados.<br>• Requisitos contractuales para las prácticas de diseño seguro, codificación y pruebas.<br>• Entrega del modelo de amenazas aprobado al desarrollador externo.<br>• Pruebas de aceptación de calidad y adecuación de las entregas.<br>• Presentación de pruebas de seguridad, se utilizan para establecer los niveles mínimos aceptables de seguridad y calidad de la privacidad (vulnerabilidades, código malicioso).<br>• Acuerdos de garantías, cuando el código fuente no esté disponible.<br>• Derechos contractuales para auditar procesos y controles del desarrollo contratado.<br>• Documentación real del entorno de compilación utilizado para crear los entregables.<br>• La empresa sigue siendo responsable de cumplir leyes aplicables y la verificación de la eficacia de control.<br>(AENOR, 2015) |
| Pruebas de seguridad de sistemas. | Se debe considerar las siguientes directrices:<br>• Sistemas nuevos y actualizados.<br>• Aplicación de pruebas.<br>• Verificaciones en los procesos de desarrollo.<br>• Preparación de un plan de pruebas, actividades y datos de prueba junto con los resultados esperados y bajo condiciones establecidas. |

| | |
|---|---|
| | (AENOR, 2015) |
| Pruebas de aceptación de sistemas. | Se debe considerar las siguientes directrices:<br>• Pruebas de los requisitos de seguridad de la información.<br>• Pruebas de que se han aplicado prácticas de desarrollo seguro del sistema.<br>• Pruebas sobre componentes.<br>• Pruebas sobre sistemas integrados.<br>• Usos de herramientas para el análisis de código, escáneres de vulnerabilidad.<br>• Verificación de la solución de los defectos relacionados con la seguridad.<br>(AENOR, 2015) |
| Protección de datos de prueba. | Se debe considerar las siguientes directrices:<br>• Procedimientos de control de acceso que se aplican a los sistemas operacionales.<br>• Procedimientos de control de acceso que se aplican a los sistemas de pruebas.<br>• La información operacional se debería borrar del entorno de pruebas, inmediatamente después que las pruebas se hayan completado.<br>• La copia y utilización de información operacional deberían ser registradas para proporcionar evidencias de auditoria.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

c) Seguridad de las operaciones

**Tabla 37:** Seguridad de las operaciones

| **Objetivo:** | Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. |
|---|---|
| **Criterios de seguridad** | |
| Procedimientos de operación documentados. | Deben especificar las instrucciones para la ejecución detallada de cada tarea, considerar las siguientes directrices:<br>• La instalación y configuración de sistemas.<br>• Tratamiento y manipulación de la información tanto automatizada como manual.<br>• Copias de respaldos.<br>• Requisitos de planificación, incluyendo las interdependencias con otros sistemas.<br>• Instrucciones para manejar errores u otras condiciones excepcionales que pueden ocurrir durante la ejecución del trabajo, incluyendo restricciones en el uso de las utilidades del sistema.<br>• Los contactos de soporte para el caso de dificultades operacionales o técnicas inesperadas.<br>• Las instrucciones para el manejo de resultados especiales y soporte.<br>• El reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema.<br>• La gestión de pistas de auditoria y de la información de registros de sistemas.<br>(AENOR, 2015) |
| Gestión de cambios. | Se debe considerar las siguientes directrices:<br>• Identificación y registro de los cambios significativos.<br>• Planificación de pruebas de los cambios. |

| | |
|---|---|
| | • Evaluación de los impactos potenciales, en la seguridad de la información.<br>• Procedimientos de aprobación formal de los cambios propuestos.<br>• Verificar que los requisitos de seguridad se cumplan.<br>• Comunicación de los detalles de los cambios a todas las personas correspondientes.<br>• Procedimientos de vuelta atrás, con los responsables y los procedimientos para abortar y recuperar los cambios infructuosos y los eventos improvistos.<br>• Disposición de un proceso de cambio de emergencia que habilite la implantación rápida y controlada de los cambios necesarios para resolver un incidente.<br>(AENOR, 2015) |
| Gestión de capacidad. | Se debe considerar las siguientes directrices:<br>• Borrar de datos obsoletos.<br>• Desmantelar aplicaciones, sistemas, bases de datos.<br>• Optimizar el tratamiento por lotes y la planificación.<br>• Optimizar la lógica de la aplicación o las consultas de base de datos.<br>• Denegar y restringir el ancho de banda para los consumidores de muchos recursos.<br>(AENOR, 2015) |
| Separación de los ambientes de desarrollo, pruebas y operación. | Se debe considerar las siguientes directrices:<br>• Definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hasta el estado de operación.<br>• El software de desarrollo y explotación debe ejecutarse en diferentes sistemas o procesadores de ordenador en diferentes dominios o directorios.<br>• Los cambios en las aplicaciones y sistemas de operación deben probarse en un entorno de pruebas de modo previo a ser aplicados en sistemas de operación.<br>• Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema deben ser accesibles desde los sistemas de operación cuando sean necesarios.<br>• Los usuarios deberían utilizar diferentes perfiles para los sistemas de operación y de prueba.<br>• Los datos sensibles no deben ser copiados en el entorno del sistema de pruebas, a menos que se proporcionen controles equivalentes en dicho entorno.<br>(AENOR, 2015) |
| Controles contra códigos maliciosos. | Se debe considerar las siguientes directrices:<br>• Definir una política formal e implantar controles para prohibir el uso de software no autorizado.<br>• Implantar controles para prevenir o detectar el uso de sitios web de los que se sospecha su carácter malicioso.<br>• Reducción de vulnerabilidades que podrían ser explotadas por código malicioso.<br>• Llevar a cabo revisiones regulares del software y datos contenidos en los sistemas.<br>• Instalación y actualización continua de software de detección y reparación de código malicioso para escanear ordenadores y los dispositivos.<br>• Realizar un informe de los ataques de código malicioso y de los procesos de recuperación aplicados. |

| | |
|---|---|
| | • Preparar planes adecuados de continuidad de negocio para la reparación de los ataques de código malicioso, incluyendo todos los datos y software de respaldo.<br>(AENOR, 2015) |
| Respaldos de información. | Se debe considerar las siguientes directrices:<br>• Deben producirse registros precisos y completos de las copias de respaldos, así como de los procedimientos de recuperación documentados.<br>• Las copias de respaldos deben ser almacenadas en un emplazamiento alejado, para salvarse de cualquier daño proveniente de la nube.<br>• La información de las copias de respaldo debe tener un nivel adecuado de protección física como ambiental.<br>• Los soportes de las copias de respaldo deben ser comprobados periódicamente para asegurarse de que pueden responder en caso de emergencia.<br>• En las situaciones donde es importante la confidencialidad, las copias de respaldos deben ser protegidas mediante cifrado.<br>(AENOR, 2015) |
| Registro de eventos. | Se debe considerar las siguientes directrices:<br>• Identificadores de usuario.<br>• Actividades del sistema.<br>• Fechas, tiempos y detalle de eventos claves.<br>• Identidad y localización del dispositivo.<br>• Registro de intentos de acceso al sistema exitosos y fallidos.<br>• Registro de intentos de acceso a los recursos y a los datos exitosos y fallidos.<br>• Cambios en la configuración del sistema.<br>• Uso de privilegios.<br>• Uso de utilidades y aplicaciones del sistema.<br>• Activación y desactivación de los sistemas de protección.<br>(AENOR, 2015) |
| Protección de la información de registro. | Se debe considerar las siguientes directrices:<br>• Alteraciones en los tipos de mensajes que son registrados.<br>• Edición y borrado de los ficheros de registro.<br>• Superación de la capacidad de almacenamiento de los soportes de ficheros de registro.<br>(AENOR, 2015) |
| Registros del administrador y del operador. | Se debe considerar las siguientes directrices:<br>• Los titulares de cuentas de usuario con privilegios pueden ser capaces de manipular los registros en las instalaciones de tratamiento de información bajo su control directo, por lo que es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios con privilegios.<br>(AENOR, 2015) |
| Sincronización de relojes. | Se debe considerar las siguientes directrices:<br>• Se debe documentar los requisitos externos e internos para las representación, sincronización y precisión del tiempo.<br>• Debe establecerse un tiempo de referencia normalizado.<br>(AENOR, 2015) |
| Instalación de software en sistemas operativos. | Se debe considerar las siguientes directrices:<br>• La actualización del software operacional, de las aplicaciones y de las bibliotecas de programas solo deben ser llevadas a cabo por administradores formados con la adecuada autorización de la dirección. |

| | |
|---|---|
| | • Los sistemas operativos solo deben manejar códigos ejecutables aprobados.<br>• Debe emplearse un sistema de control de la configuración para supervisar todo el software implantado, así como la documentación de sistemas.<br>• Debe existir una estrategia de vuelta atrás antes de implantar los cambios.<br>• Debe mantenerse un registro de auditoria de todas las actualizaciones de las bibliotecas de los programas de explotación.<br>• Debe conservarse versiones anteriores del software de las aplicaciones como medida de contingencia.<br>• Deben archivarse las versiones más antiguas del software, junto con toda la información requerida, parámetros, procedimientos, detalles de configuración y software de apoyo durante todo el tiempo en que la información se conserve en el archivo.<br>(AENOR, 2015) |
| Gestión de las vulnerabilidades técnicas. | Se debe considerar las siguientes directrices:<br>• Definir funciones y responsabilidades asociadas con la gestión de vulnerabilidades técnicas: identificar vulnerabilidades, supervisar las vulnerabilidades identificadas, evaluar los riegos, mantener alertas sobre las vulnerabilidades, seguimiento de activos comprometidos y demás medidas que deben adoptarse.<br>• Definirse una escala temporal para reaccionar a las notificaciones de vulnerabilidades técnicas que pueden resultar relevantes.<br>• Dependiendo de la urgencia con que deba tratarse la vulnerabilidad, la medida debería ser llevada a cabo de acuerdo con los controles relativos a la gestión de cambios.<br>• Debe mantenerse un registro de auditoria de todos los procedimientos adoptados.<br>• El proceso de gestión de vulnerabilidades técnicas debe supervisarse y evaluarse periódicamente para garantizar su efectividad y eficacia.<br>• Los sistemas con elevado riesgo son los primeros que deben tratarse.<br>• El proceso de gestión de vulnerabilidades técnicas debe estar alineado con las actividades de gestión de incidentes, para comunicar datos sobre las vulnerabilidades relativas a la función de respuesta a incidentes y proporcionar procedimientos técnicos a desarrollar cuando ocurra un incidente.<br>(AENOR, 2015) |
| Restricciones sobre la instalación de software. | Se debe considerar las siguientes directrices:<br>• Conceder ciertos privilegios para que los empleados puedan tener la capacidad de instalar software, se debe identificar qué tipos de instalaciones de software están permitidas y cuales están prohibidas, estos privilegios deben asignarse en atención a las funciones de los empleados.<br>(AENOR, 2015) |
| Información controles de auditoria de sistemas. | Se debe considerar las siguientes directrices:<br>• Los requisitos de acceso de auditoria a sistemas y datos deben acordarse con la Dirección de la empresa.<br>• Debe controlarse y acordarse el alcance de las comprobaciones técnicas de auditoria. |

| | |
|---|---|
| | • Las comprobaciones deben limitarse accesos de sólo lectura al software y a los datos.<br>• El acceso de solo lectura debe permitirse únicamente a copias aisladas de los archivos del sistema, que deberían borrarse cuando finalice la auditoría.<br>• Las pruebas de auditoria que puedan afectar a la disponibilidad de los sistemas deben ejecutarse fuera del horario laboral.<br>• Todos los accesos deben ser supervisados y registrados para obtener pistas de referencia.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

d) Seguridad física

**Tabla 38:** Seguridad física y ambiental

| **Objetivo:** | Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información. |
|---|---|
| **Criterios de seguridad** | |
| Perímetro de seguridad física | Se debe considerar los siguientes parámetros de seguridad física:<br>• Perímetros bien definidos: sólidos, muros y tejados de construcción sólidos, puertas adecuadamente protegidas contra accesos no autorizados a través de mecanismos de control (barras, alarmas, cerraduras).<br>• Puertas y ventanas bloqueadas, cuando no se atienda.<br>• Debe situarse un área de recepción, controles de acceso físico a las instalaciones o al edificio, y solo el personal autorizado debe tener accesos permitidos.<br>• Las puertas deben estar dotadas de un sistema de seguridad, monitorizadas y probadas con las paredes, para establecer el nivel requerido de resistencia de acuerdo a las normas nacionales.<br>• Se debe operar de acuerdo a los códigos locales de protección contra incendios en modo de fallos seguro.<br>• Contar con un sistema de detección de intrusos conforme a las normas nacionales y ser probado periódicamente para dar cobertura a todas las puertas externas y ventanas accesibles.<br>• Los recursos de tratamiento de la información gestionado por terceras partes deben estar físicamente separados.<br>(AENOR, 2015) |
| Controles físicos de entrada | Se consideran las siguientes directrices:<br>• Registrar la fecha y la hora de la entrada y la salida de los visitantes, que debe ser supervisados.<br>• Los accesos son solo para propósitos específicos y autorizados.<br>• La identidad de los visitantes debe autenticarse mediante medios adecuados.<br>• El acceso a las áreas donde se almacena y procesa la información sensible debe ser controlados y restringido únicamente al personal autorizado.<br>• Controles de autenticación para autorizar y validar todos los accesos. |

| | |
|---|---|
| | • Mantenerse y monitorizarse de manera segura un libro físico de registro o una pista de auditoria electrónica de todos los accesos.<br>• Proporcionar un documento de identificación a los empleados y terceros, en caso que no se lleve dicho documento de identificación se debe informar al personal de seguridad de que existen personas que no portan dicha identificación.<br>• Para el personal de apoyo de terceros el acceso a las áreas seguras de tratamiento de la información tiene que ser restringido, autorizados y controlados.<br>(AENOR, 2015) |
| Seguridad de oficinas, recintos e instalaciones. | Se consideran las siguientes directrices:<br>• Situar las instalaciones de manera que se evite el acceso público general.<br>• Las instalaciones deben configurarse para prevenir que la información confidencial sea visible o audibles desde el exterior.<br>• Los directorios telefónicos internos que involucren información sensible no deben ser de fácil acceso por personas no autorizadas.<br>(AENOR, 2015) |
| Protección contra amenazas externas y ambientales. | Se debe optar por un asesoramiento especializado en temas de:<br>• Evitar daños causados por fuego.<br>• Inundación.<br>• Terremoto.<br>• Explosión.<br>• Revueltas sociales.<br>• Otras formas de desastre causadas por el hombre.<br>(AENOR, 2015) |
| Trabajo en áreas seguras. | Se consideran las siguientes directrices.<br>• El personal debe conocer la existencia de áreas seguras.<br>• Evitar el trabajo no supervisado, por motivos de seguridad y por actividades maliciosas.<br>• Las áreas seguras vacías deben estar físicamente cerradas.<br>• No se permitirá equipos de fotografía, video, audio y otros equipos de grabación, salvo autorización especial.<br>(AENOR, 2015) |
| Áreas de despacho y carga. | Se consideran las siguientes directrices:<br>• Restringir acceso a las áreas de carga y descarga a personas no autorizadas.<br>• El material debe ser inspeccionado para evitar amenazas potenciales.<br>• El material entrante debe registrarse de acuerdo a los procedimientos de gestión de activos.<br>• El material debe ser inspeccionado para identificar si hubo manipulación durante su traslado, en caso de que si existiera se debe informar al personal de seguridad.<br>(AENOR, 2015) |
| Ubicación y protección de los equipos. | Se consideran las siguientes directrices:<br>• Los equipos de tratamiento de información que manejen datos sensibles, se deben instalar donde se reduzca el riesgo de que la información sea visible durante su uso por personas no autorizadas.<br>• Las instalaciones de almacenamiento deben asegurarse para evitar accesos no autorizados. |

| | |
|---|---|
| | • Establecer directrices para comer, beber y fumar en las proximidades a las instalaciones de tratamiento de información.<br>• Controlar condiciones ambientales: temperatura y humedad, que puedan afectar al funcionamiento de los equipos de tratamiento de información.<br>• Considerar el uso de métodos de protección especial para los equipos, en especial para los que procesan información sensible para minimizar el riesgo de fugas de información.<br>(AENOR, 2015) |
| Servicios de suministro. | Los suministros de apoyo: electricidad, telecomunicaciones, agua, gas, residuales, calefacción/ventilación y aire acondicionado deben considerar las siguientes directrices:<br>• Ser conformes a las especificaciones del fabricante de los equipos y a los requisitos legales locales.<br>• Ser evaluadas regularmente respecto a su capacidad para satisfacer el desarrollo del negocio y con respecto a la interacción con otros servicios de apoyo.<br>• Ser inspeccionados regularmente, mediante pruebas para asegurar su correcto funcionamiento.<br>• Disponer de alarmas para detectar fallos en su funcionamiento.<br>• Disponer de múltiples fuentes con canales físicos y alimentación independiente.<br>(AENOR, 2015) |
| Seguridad de cableado. | Se debe considerar las siguientes directrices:<br>• Las líneas de energía y telecomunicaciones en las áreas de tratamiento de la información, deben ser soterradas, cuando sea posible, y cuando sea posible se adoptará medidas alternativas de protección.<br>• Se deben separar los cables de energía de los de comunicación para evitar interferencias.<br>• Instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación.<br>• Implantación de barreras técnicas e inspecciones físicas para detectar la conexión del cableado de dispositivos no autorizados.<br>• Accesos controlados a los paneles de parcheo y a las salas de cableado.<br>(AENOR, 2015) |
| Mantenimiento de equipos. | Se debe considerar las siguientes directrices:<br>• Debe mantenerse de acuerdo a las recomendaciones de intervalos de servicio y especificaciones del proveedor.<br>• Solo el personal de mantenimiento debidamente autorizado debería realizar la reparación y el servicio de los equipos.<br>• Llevar un registro de todos los fallos, reales y sospechados, así como de todo el mantenimiento preventivo y correctivo.<br>• Adoptar controles adecuados para cuando se programe el mantenimiento de los equipos, teniendo en cuenta si el mantenimiento se lleva a cabo por el personal de la empresa o por algún lugar externo.<br>• Antes de poner un quipo en funcionamiento después del mantenimiento, debe ser inspeccionado para asegurar que el equipo no ha sido manipulado y que no funciona incorrectamente.<br>(AENOR, 2015) |

| | |
|---|---|
| Retiro de activos. | Se debe considerar las siguientes directrices:<br>• Los empleados y usuarios de terceras partes con permisos para sacar los activos fuera de las instalaciones, debe estar claramente identificados.<br>• Se debe establecer limitaciones al tiempo que el equipo puede estar fuera de las instalaciones y verificar a su retorno que ha cumplido con dichas limitaciones.<br>• Donde sea necesario y adecuado, se debe registrar la salida de equipos de la empresa y también el retorno.<br>• La identidad, las funciones y la afiliación de cualquier persona que maneja o usa los activos debe documentarse y dicha documentación estar junta al equipo, información o software.<br>(AENOR, 2015) |
| Seguridad de equipos y activos fuera de las instalaciones. | Se debe considerar las siguientes directrices:<br>• Cuando el equipo fuera de las instalaciones se transfiere entre distintos individuos o entidades externas, se debe mantener un registro que defina la cadena de custodia de los equipos incluyendo, al menos, los nombres y las empresas de los responsables de dichos equipos.<br>• Los equipos y soportes sacados de las instalaciones no se deben dejar desatendidos en lugares públicos.<br>(AENOR, 2015) |
| Disposición segura o reutilización de equipos. | Se debe considerar las siguientes directrices:<br>• Los soportes que contengan información sensible o con derechos de autor deben ser destruidos físicamente, o la información debe ser borrada o sobrescrita mediante técnicas que hagan imposible la recuperación de la información original, en lugar de utilizar un borrador o un formateado normal.<br>(AENOR, 2015) |
| Equipos de usuarios desatendidos. | Se debe considerar las siguientes directrices:<br>• Terminar las sesiones activas cuando se acaben, a menos que estén aseguradas a través de un mecanismo de bloqueo adecuado.<br>• Salir de las aplicaciones o servicios de red cuando ya no las necesiten.<br>• Asegurara los ordenadores personales frente accesos n autorizados a través de un bloqueo con clave.<br>(AENOR, 2015) |
| Política de escritorio limpio y pantalla limpia. | Se debe considerar las siguientes directrices:<br>• La información del negocio sensible o crítica (papel, soporte de almacenamiento electrónico) debe estar guardada, cuando no se necesite y las oficinas estén abiertas. (caja fuerte, armario u otro mueble de seguridad)<br>• Los ordenadores deben quedar apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña.<br>• Debe prevenirse el uso por usuarios no autorizados de fotocopias y otros dispositivos de reproducción.<br>• Los soportes que contengan información sensible o clasificada deben retirarse de forma inmediata de las impresoras.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

e) Gestión de incidentes de seguridad de la información

**Tabla 39:** Gestión de incidentes de seguridad de la información

| **Objetivo:** | Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades. |
|---|---|
| **Criterios de seguridad** | |
| Responsabilidad y procedimientos. | Se debe considerar las siguientes directrices:<br>• Establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos se desarrollen y se comuniquen adecuadamente en la empresa.<br>• Establecer procedimientos que aseguren: el manejo eficiente de incidentes de seguridad de la información, detección y comunicación de incidentes de seguridad.<br>• Contacto apropiado con las autoridades que tratan asuntos relacionados con incidentes de seguridad de la información.<br>• Los procedimientos deben incluir: formularios de comunicación de los eventos de seguridad de la información, comportamiento adecuado que debería tomarse en caso de un evento de seguridad de la información, referencia de un proceso disciplinario formal establecido para tratar al personal, contratistas, terceros que haya incumplido en la seguridad, procesos de retroalimentación adecuados para garantizar que las personas que comuniquen eventos de seguridad de la información sean informadas de los resultados después que se haya tratado y cerrado el problema.<br>(AENOR, 2015) |
| Reporte de eventos de seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Control ineficaz de la seguridad.<br>• Quebrantamiento de las expectativas de integridad, confidencialidad y disponibilidad de la información.<br>• Errores humanos.<br>• Incumplimientos de políticas y directrices.<br>• Quebrantamientos de las directrices de seguridad física.<br>• Cambios incontrolados del sistema.<br>• Disfunciones del software y hardware.<br>• Violaciones de acceso.<br>(AENOR, 2015) |
| Reporte de debilidades de seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Todo el personal y contratistas deben comunicar los incidentes lo antes posible para evitar incidentes en la seguridad de la información.<br>(AENOR, 2015) |
| Evaluación de eventos de seguridad de la información y decisiones sobre ellos. | Se debe considerar las siguientes directrices:<br>• Evaluar cada evento de seguridad de la información recurriendo a una escala de clasificación de eventos e incidentes de seguridad establecida.<br>• Decidir si un evento debe clasificarse como un incidente de seguridad.<br>• Priorizar incidentes, identificar el impacto del incidente.<br>(AENOR, 2015) |
| Respuesta a incidentes de seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Recogida de videncias tan pronto sea posible, tras la ocurrencia de un incidente.<br>• Escalado del incidente. |

| | |
|---|---|
| | • Asegurarse de que todos los implicados en las actividades de respuesta a incidentes son adecuadamente incorporados para realizar el correspondiente análisis posterior.<br>• Comunicación de la existencia del incidente se seguridad de la información a las personas internas, externas, terceras entidades que requieran y deban conocer.<br>• Tratamiento de las debilidades encontradas que puedan contribuir en otro accidente.<br>• Tratamiento del incidente.<br>• Cierre del incidente, registro del cierre.<br>(AENOR, 2015) |
| Aprendizaje obtenido de los incidentes de seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Mecanismos para cuantificar y supervisar los tipos, volúmenes y costos de los incidentes de seguridad de la información. A cuantificar y monitorizar.<br>• La información obtenida a partir de la evaluación de los incidentes de seguridad de la información debe utilizarse para identificar incidentes recurrentes.<br>(AENOR, 2015) |
| Recolección de evidencia. | Se debe considerar las siguientes directrices:<br>• Cadena de custodia.<br>• Integridad de la evidencia.<br>• Protección de las personas.<br>• Funciones y responsabilidades del personal implicado.<br>• Documentación.<br>• Resumen.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

f) Organización de la seguridad de la información

**Tabla 40:** Organización de la seguridad de la información

| **Objetivo:** | Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la empresa. |
|---|---|
| **Criterios de seguridad** | |
| Roles y responsabilidades para la seguridad de la información. | Se debe considerar las siguientes directrices:<br>• De acuerdo con las políticas de seguridad de la información.<br>• Identificarse y definirse los activos y los procesos de seguridad de la información.<br>• Asignarse un área responsable para cada activo y proceso de seguridad de la información y documentarse los detalles de dicha responsabilidad.<br>• Definirse y documentarse los niveles de autorización.<br>• Los responsables deben mostrar capacidad en el área.<br>• Identificarse y documentarse los aspectos de coordinación y supervisión de seguridad de la información relativa a las relaciones con los proveedores.<br>(AENOR, 2015) |
| Separación de deberes. | Se debe considerar las siguientes directrices:<br>• El acceso, modificación o utilización de activos bajo autorización previa.<br>• Monitorización de actividades.<br>• Pistas de auditorías.<br>• Supervisión por la dirección empresarial. |

| | |
|---|---|
| | (AENOR, 2015) |
| Contacto con las autoridades. | Se debe considerar las siguientes directrices:<br>• Procedimientos que especifiquen cuando y con qué autoridades se debe contactar.<br>• Contactos con otras autoridades (públicos, privados)<br>(AENOR, 2015) |
| Contacto con grupos de interés especial. | Se debe considerar las siguientes directrices:<br>• Mejorar los conocimientos sobre las mejores prácticas y mantenerse actualizado en temas de seguridad.<br>• Recibir asesoramiento, alertas y parches correspondientes a ataques y vulnerabilidades.<br>• Obtener asesoramiento especializado en seguridad de la información.<br>• Compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas y vulnerabilidades.<br>(AENOR, 2015) |
| Seguridad de la información en la gestión de proyectos. | Se debe considerar las siguientes directrices:<br>• Integrar en la metodología de gestión de proyectos.<br>• Definir en los objetivos del proyecto.<br>• Definir para todas las fases de la metodología aplicada en el proyecto.<br>(AENOR, 2015) |
| Políticas para dispositivos móviles | Se debe considerar las siguientes directrices:<br>• No comprometer la información del negocio.<br>• Registro de dispositivos móviles.<br>• Requisitos para protección física.<br>• Restricciones de instalación de software.<br>• Restricciones de conexión a servicios de información.<br>• Controles de acceso.<br>• Técnicas criptográficas.<br>• Protección ante software malicioso.<br>• Copias de respaldo.<br>(AENOR, 2015) |
| Teletrabajo | Se debe considerar las siguientes directrices:<br>• Seguridad física<br>• Seguridad del entorno.<br>• Requisitos de seguridad de las comunicaciones.<br>• Facilitar el acceso a escritorios virtuales<br>• Control a amenazas de intentos de accesos no autorizados a la información.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

g) Seguridad en las comunicaciones

**Tabla 41:** Seguridad en las comunicaciones

| **Objetivo:** | Asegurar la protección de la información en las redes y los recursos de tratamiento de la información. |
|---|---|
| **Criterios de seguridad** | |
| Controles de redes | Se debe considerar las siguientes directrices:<br>• Debe establecerse las responsabilidades y los procedimientos para la gestión de los equipos de red.<br>• La responsabilidad operacional de las redes debe estar separada de las operaciones de los sistemas informáticos donde sea apropiado. |

| | |
|---|---|
| | • Debe establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas o redes inalámbricas y proteger los sistemas conectados a sus aplicaciones.<br>• Debe establecerse controles especiales para mantener la disponibilidad de los servicios de red y los ordenadores conectados.<br>• Debe realizarse un adecuado registro de eventos y monitorización para permitir el registro y detección de acciones que podrían afectar, o ser relevantes, para la seguridad de la información.<br>• Deben estar coordinadas las actividades de gestión, tanto para optimizar el servicio de la empresa, como para asegurar que los controles sean aplicados consistentemente en toda la infraestructura de tratamiento de la información.<br>• Los sistemas de la red deben ser autenticados.<br>• La conexión a los sistemas de red debe ser restringido.<br>(AENOR, 2015) |
| Seguridad de los servicios de red. | Se debe considerar las siguientes directrices:<br>• Se debe determinar y supervisar la capacidad del proveedor del servicio de red para gestionar los servicios acordados de una manera segura.<br>• Se debe acordar el derecho de ser auditado.<br>• Se debe identificar las disposiciones de seguridad necesarias para los servicios particulares: características de seguridad, niveles de servicios y requisitos de gestión.<br>(AENOR, 2015) |
| Separación en las redes. | Se debe considerar las siguientes directrices:<br>• Se debe optar por un método para gestionar la seguridad de redes, separarlas en dominios.<br>• Los dominios deben establecerse por nivel de confianza.<br>• El perímetro de cada dominio debe estar bien definido.<br>• El acceso entre dominios debe estar permitidos.<br>• Para redes inalámbricas de entornos sensibles se debe hacer oportunas consideraciones para tratar todos los accesos inalámbricos.<br>• La autenticación, cifrado y las tecnologías de control de acceso a la red debe tomar en cuenta normas, estándares así se garantiza la conexión a las redes.<br>(AENOR, 2015) |
| Políticas y procedimientos de transferencia de información. | Se debe considerar las siguientes directrices:<br>• El diseño de procedimientos para proteger la información transferida de interceptación, copia, modificación, errores de enrutamiento y destrucción.<br>• Procedimientos para la detección y la protección contra el malware que puede ser transmitido a través del uso de comunicaciones electrónicas.<br>• Procedimientos para proteger información electrónica sensible que tiene la forma de adjuntos.<br>• Usos de técnicas criptográficas.<br>• Controles y restricciones asociadas con el uso de los recursos de comunicación.<br>• Asesorar al personal para que tome las precauciones necesarias de no revelar información confidencial.<br>(AENOR, 2015) |

| | |
|---|---|
| Acuerdos sobre transferencia de información. | Se debe considerar las siguientes directrices:<br>• Responsabilidades de la Dirección sobre el control y la notificación de la transmisión, el envío y la recepción.<br>• Procedimientos para garantizar la trazabilidad y el no repudio.<br>• Las normas técnicas mínimas para la compresión.<br>• Las responsabilidades y obligaciones en caso de incidentes se seguridad de la información.<br>• Las normas técnicas para la grabación y la lectura de la información y el software.<br>• Niveles aceptables de control de acceso.<br>(AENOR, 2015) |
| Mensajería electrónica. | Se debe considerar las siguientes directrices:<br>• Protección de mensajes frente a accesos no autorizados, modificación o denegación de servicio acorde con el esquema de clasificación adoptados por la empresa.<br>• Asegurar el correcto direccionamiento y transporte del mensaje.<br>• Fiabilidad y disponibilidad del servicio.<br>• Consideraciones legales.<br>• Aprobación para el uso de mensajería instantánea, redes sociales.<br>(AENOR, 2015) |
| Acuerdos de confidencialidad o de no divulgación. | Se debe considerar las siguientes directrices:<br>• Duración prevista del acuerdo, incluyendo los casos en los que la confidencialidad necesitase mantenerse indefinidamente.<br>• Acciones necesarias para cuando se termine el acuerdo.<br>• Las responsabilidades y a las acciones de los que firman para evitar la revelación no autorizada de la información.<br>• Propiedad de la información, propiedad intelectual y como se relaciona con la protección de la información confidencial.<br>• Uso permitido de información confidencial y los derechos de los firmantes para utilizar la información.<br>• Derechos de auditar y supervisar las actividades que involucren a la información confidencial.<br>• Los procesos para la notificación y aviso de la revelación no autorizada o fugas de información confidencial.<br>• Los términos en los que la información debe ser devuelta o destruida en el cese de un acuerdo.<br>• Las acciones que se espera sean tomadas en caso de incumplimiento del acuerdo.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

h) Gestión de activos

**Tabla 42:** Gestión de activos

| **Objetivo:** | Identificar los activos de la organización y definir las responsabilidades de protección adecuadas. |
|---|---|
| **Criterios de seguridad** | |
| Inventario de activos de TI | Se debe considerar las siguientes directrices:<br>• Activos, recursos asociados a la información deben estar claramente identificados y mantenerse en inventario.<br>• Identificar activos relevantes y documentar su importancia. |

| | |
|---|---|
| | • La documentación permanecer en inventarios, según sea adecuado.<br>• El inventario de los activos debe ser preciso, estar actualizado, ser consistente y estar en consonancia con otros inventarios.<br>• Cada uno de los activos identificados debe estar asignado a un responsable e identificada su clasificación.<br>(AENOR, 2015) |
| Propiedad de los activos | Se debe considerar las siguientes directrices:<br>• Todos los activos que figuran en el inventario deben tener un responsable.<br>• Implementar un proceso para asegurar la puntual asignación de responsabilidad sobre los activos.<br>• El responsable del activo debe proporcionar la adecuada gestión del activo durante todo su ciclo de vida.<br>El responsable debe:<br>• Asegurar que los activos son inventariados.<br>• Asegurar que los activos se clasifiquen y protejan debidamente.<br>• Definir y revisar periódicamente restricciones de acceso y la clasificación de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso.<br>• Asegurar el manejo adecuado para el borrado o destrucción del activo.<br>Responsable: individuo o área autorizada.<br>Tareas: cuidado diario.<br>(AENOR, 2015) |
| Uso aceptable de los activos | Se debe considerar las siguientes directrices:<br>• Identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con el tratamiento de la información.<br>• Concienciar a los usuarios en el uso y acceso a los activos tomando en cuenta los requisitos de seguridad de la información.<br>• Deben ser responsables del uso de los recursos de tratamiento de la información.<br>(AENOR, 2015) |
| Devolución de los activos | Se debe considerar las siguientes directrices:<br>• Todos los empleados y terceras partes deben devolver todos los activos, que estén en su poder al finalizar su empleo, contrato.<br>• Debe estar formalizado un proceso de desvinculación que incluya la devolución de todo activo físico y electrónico que sean de propiedad de la organización o estén bajo su custodia.<br>• Verificar que la información sea devuelta a la empresa.<br>• Si el empleado o tercero tiene conocimiento sobre asuntos importantes para las operaciones en curso, debe documentarse dichos conocimientos y ser transferidos a la empresa.<br>• La empresa debe controlar la copia no autorizada de la información relevante durante el periodo entre la notificación de desvinculación de empleados y terceros y la materialización efectiva de la misma.<br>(AENOR, 2015) |

| | |
|---|---|
| Clasificación de la información | Se debe considerar las siguientes directrices:<br>• La información debe ser clasificada en términos de importancia y su relevancia frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizada.<br>• Controles de protección en base a las necesidades del negocio.<br>• Clasificación de la información que se almacena, procesa por los activos.<br>• Los responsables de los activos de información son los responsables de su clasificación en base a la normativa.<br>Esquema de clasificación:<br>• Normas<br>• Criterios de revisión en el tiempo.<br>• Nivel de protección (confidencialidad, integridad y disponibilidad)<br>• Alineado con las políticas de control de acceso.<br>Debe ser un proceso formal de la empresa, consistente y coherente.<br>• Los resultados de la clasificación deben indicar el valor de los activos en función de su sensibilidad y criticidad.<br>• Los resultados de la clasificación deben actualizarse cuando cambie su valor, sensibilidad y criticidad.<br>(AENOR, 2015) |
| Etiquetado de la información | Se debe considerar las siguientes directrices:<br>Desarrollar e implantar un procedimiento formal para etiquetar la información de acuerdo con el esquema de clasificación de la empresa.<br>Debe contemplar:<br>• Información de activos de soporte físico.<br>• Información de activos de soporte electrónico.<br>• Etiquetas fácilmente reconocibles.<br>• Procedimiento con directrices de donde y como se vinculan las etiquetas.<br>• Procedimientos de etiquetado tanto para empleados y terceros.<br>Marcar con una etiqueta adecuada los resultados producidos por sistemas que contengan información clasificada como sensible.<br>(AENOR, 2015) |
| Manipulado de la información | Se debe considerar las siguientes directrices:<br>• Restringir el acceso por empleado, terceros y de acuerdo a cada nivel de clasificación de la información.<br>• Proteger las copias de la información original ya sea temporal o permanente.<br>• Marcado claro en todas las copias de soporte para la debida atención del receptor autorizado.<br>(AENOR, 2015) |
| Gestión de medios removibles | Se debe considerar las siguientes directrices:<br>• En caso de ya no ser necesario, se debe borrar definitivamente los contenidos de cualquier soporte reutilizable que vaya a ser retirado.<br>• Cuando sea necesario y práctico, solicitar autorización para extraer soportes de la empresa y debe mantenerse un registro de las retiradas para tener trazabilidad a efectos de auditoria.<br>• Todos los soportes deben almacenarse en un entorno seguro y protegido, conforme a especificaciones de sus fabricantes. |

| | |
|---|---|
| | • Deben usarse técnicas criptográficas para proteger datos en soportes extraíbles en caso de que apliquen requisitos importantes de confidencialidad e integridad.<br>• Deben almacenarse copias múltiples de datos valiosos en soportes separados para aun reducir más el riesgo de daño o perdida simultanea de los datos.<br>• El inventariado de soportes extraíbles debe considerarse para limitar las posibilidades de pérdida de datos.<br>• Solo debe permitirse reproductores de soportes extraíbles cuando haya una razón de negocio para ello.<br>• La transferencia de información a medios extraíbles debe ser monitorizada, cuando haya necesidad de usar dichos soportes.<br>(AENOR, 2015) |
| Disposición de los medios | Se debe considerar las siguientes directrices:<br>Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarias, mediante procedimientos formales.<br>Elementos a considerar:<br>• Usar procesos de trituración, incineración, borrado de datos.<br>• Identificar elementos que requieren una eliminación segura.<br>• Tomar precaución si se elige a terceros para la recolección y eliminación de soportes, que tengan experiencia y controles.<br>• La eliminación de elementos debe quedar registrado a fin de mantener trazabilidad para su auditoria.<br>(AENOR, 2015) |
| Transferencia de medios físicos | Se debe considerar las siguientes directrices:<br>• Emplear un servicio fiable de transporte o mensajería.<br>• Acordar con la dirección de la empresa una lista de mensajeros autorizados.<br>• Desarrollar procedimientos para verificar la identidad de los mensajeros.<br>• Proteger el contenido de todo daño físico que pueda ocurrir durante la transferencia.<br>• Mantener registros, identificando el contenido de los soportes, la protección aplicada, así como los momentos de transferencia a los custodios y la recepción en el destino.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

i) Conformidad

**Tabla 43:** Conformidad

| **Objetivo:** | Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad. |
|---|---|
| **Criterios de seguridad** | |
| Identificación de la legislación aplicable y los requisitos contractuales. | Se debe considerar las siguientes directrices:<br>• Definir y documentar los controles específicos y las responsabilidades individuales para cumplir con los requisitos.<br>• Los directivos deben identificar la legislación aplicable a la empresa para cumplir con los requisitos de su tipo de negocio.<br>(AENOR, 2015) |

| | |
|---|---|
| Derechos de propiedad intelectual. | Se debe considerar las siguientes directrices:<br>• Publicar una política para el cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos de software y de los de la información.<br>• Adquirir software únicamente desde fuentes conocidas para garantizar que no se infringen los derechos de autor.<br>• Mantener el conocimiento de las políticas de protección de los derechos de propiedad intelectual y notificar la intención de aplicar medidas disciplinarias a cualquier miembro del personal que quebrante dichas políticas.<br>• Mantener pruebas y evidencias de la propiedad de licencias, manuales, etc.<br>• Implementar controles para garantizar que no se excede el número máximo de usuarios permitidos por licencia.<br>• Llevar a cabo comprobaciones de que solo se instala software autorizado y productos licenciados.<br>• Disponer de política para mantener las condiciones de licencias en forma adecuada.<br>(AENOR, 2015) |
| Protección de registros. | Se debe considerar las siguientes directrices:<br>• Publicar directrices sobre la retención, almacenamiento, manipulación y eliminación de registros e información.<br>• Preparar un calendario de retención que identifique los registros y el periodo de tiempo que deberían conservarse.<br>• Mantener un inventario de fuentes de información clave.<br>(AENOR, 2015) |
| Privacidad y protección de datos personales. | Se debe considerar las siguientes directrices:<br>• Desarrollar e implementar una política de privacidad y protección de la información de carácter personal.<br>• Comunicar la política a todas las personas involucradas en el tratamiento de la información de carácter personal.<br>• Nombrar un responsable de la protección de datos que deba orientar a los directivos, usuarios y proveedores sobre sus responsabilidades individuales y los procedimientos específicos a seguir.<br>(AENOR, 2015) |
| Reglamentación de controles criptográficos. | Se debe considerar las siguientes directrices:<br>• Restricciones en la importación/exportación de hardware y software que realicen funciones criptográficas.<br>• Restricciones en la importación y exportación de hardware y software diseñado para tener funciones criptográficas añadidas.<br>• Restricciones en el uso de cifrado.<br>(AENOR, 2015) |
| Revisión independiente de la seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Responsabilidad de la Dirección de la empresa.<br>• Es necesaria para saber la efectividad de la empresa en la gestión de la seguridad de la información.<br>• Realizada por personas independientes al área revisada.<br>• Los resultados deben quedar debidamente registrados y ser presentados a la Dirección.<br>• Dichos registros deben ser mantenidos en el tiempo.<br>(AENOR, 2015) |

| | |
|---|---|
| Cumplimiento con las políticas y normas de seguridad. | Se debe considerar las siguientes directrices:<br>• Los directivos deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.<br>• En caso de incumplimiento se debe: identificar causas, evaluar acciones necesarias para asegurar la implementación de acciones correctivas necesarias, las que deben ser revisadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.<br>(AENOR, 2015) |
| Revisión del cumplimiento técnico. | Se debe considerar las siguientes directrices:<br>• Toda revisión de cumplimiento técnico debe ser realizado por personal competente y autorizado.<br>• Tomar las medidas necesarias para no comprometer la seguridad del sistema cuando se realizar pruebas de intrusión o evaluación de vulnerabilidades.<br>• Apoyarse de herramientas automáticas para verificar el cumplimiento técnico, que generen informes y los resultados sean interpretados por un especialista técnico.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

j) Seguridad de los recursos humanos

**Tabla 44:** Seguridad de los recursos humanos

| **Objetivo:** | Asegurar que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran. |
|---|---|
| **Criterios de seguridad** | |
| Selección | Se debe considerar las siguientes directrices:<br>• Disponibilidad de referencias.<br>• Comprobación del curriculum vitae del candidato.<br>• Confirmación de cualificaciones académicas y profesionales.<br>• Comprobación de la identificación.<br>• Competencias necesarias para desarrollar su rol en ámbito de seguridad.<br>(AENOR, 2015) |
| Términos y condiciones de empleo | Se debe considerar las siguientes directrices:<br>• Firmar compromisos de confidencialidad.<br>• Responsabilidades y derechos legales de los empleados y contratistas.<br>• Responsabilidades de: clasificación, gestión, organización, recursos, servicios asociados con la información manejados por los empleados y contratistas.<br>• Responsabilidades del empleado o contratista en lo referente al manejo de información.<br>• Acciones a tomar en caso de hacer caso omiso de los requisitos de seguridad por parte del empleado o contratista.<br>(AENOR, 2015) |
| Responsabilidades de la dirección. | Se debe considerar las siguientes directrices:<br>• Informar sobre los roles y responsabilidades relativas a la seguridad de la información previamente a serles concedidos accesos a la información sensible y/o a los sistemas. |

| | |
|---|---|
| | • Proporcionar las directrices en cuanto a seguridad de la información en lo relativo a su función dentro de la empresa.<br>• Motivar para cumplir las políticas de seguridad de la información en la empresa.<br>• Asegurar que se acepten términos y condiciones de las contrataciones.<br>• Demostrar apoyo a las políticas o procedimientos de seguridad de la información.<br>(AENOR, 2015) |
| Toma de conciencia, educación. | Se debe considerar las siguientes directrices:<br>• Comprometer a la dirección con la seguridad de la información empresarial.<br>• Conocer y cumplir con las normas y obligaciones aplicables en seguridad de la información, según se definan en acuerdos, políticas, normas, leyes, reglamentos, contratos y acuerdos.<br>• Responsabilidad personal por las propias acciones, omisiones y responsabilidades generales relativas a asegurar y proteger la información que pertenece a la empresa.<br>• Determinar procedimientos básicos en materia de seguridad de la información.<br>• Llevar a cabo programas de capacitación y formación eficaces.<br>• Evaluar el grado de comprensión alcanzado por los empleados al final de cada actividad de concienciación, capacitación y formación para determinar el nivel de asimilación de conocimientos.<br>(AENOR, 2015) |
| Proceso disciplinario. | Se debe considerar las siguientes directrices:<br>• Formal<br>• Informar a los empleados.<br>• Iniciar con la verificación de que se ha producido una violación de seguridad.<br>• Tratamiento correcto e imparcial para los empleados de los que se sospeche hayan cometido alguna violación de la seguridad.<br>• Proporcionar respuestas graduales que tenga en cuenta la naturaleza y la gravedad de la violación de la seguridad y su impacto en el negocio.<br>• Convertir en una motivación si se definen recompensas para un comportamiento notable con respecto a la seguridad de la información.<br>(AENOR, 2015) |
| Terminación o cambio de responsabilidades de empleo. | Se debe considerar las siguientes directrices:<br>• La responsabilidad y obligaciones en términos de seguridad de la información siguen vigentes después del cambio del empleo, se debe definir, comunicar al empleado o contratista y se debe cumplir.<br>• Las responsabilidades deben incluir requisitos de seguridad.<br>• Responsabilidades legales (acuerdos de confidencialidad).<br>• Los cambios de responsabilidad, deben ser gestionados al igual que la finalización de responsabilidades y estar en coordinación con el inicio de la nueva responsabilidad o puesto de trabajo.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

k) Aspectos de seguridad de la información dentro de la continuidad del negocio

**Tabla 45:** Aspectos de seguridad de la información dentro de la continuidad del negocio

| **Objetivo:** | La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de continuidad de negocio de la empresa. |
|---|---|
| **Criterios de seguridad** | |
| Planificación de la continuidad de la seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Definir si es esta dentro del proceso de continuidad del negocio o dentro del proceso de recuperación de desastre.<br>• Los requisitos de seguridad de la información deben determinarse al planificar la continuidad del negocio y la recuperación de desastres.<br>(AENOR, 2015) |
| Implementación de la continuidad de la seguridad de la información. | Se debe considerar las siguientes directrices:<br>De acuerdo a los requisitos de continuidad de la seguridad de la información se debe establecer, documentar, implantar y mantener:<br>• Controles de seguridad de la información en: procesos, procedimientos, sistemas, herramientas de soporte de continuidad del negocio o recuperación de desastres.<br>• Procesos, procedimientos e implantación de cambios para mantener los controles existentes de seguridad de la información durante situaciones adversas.<br>• Controles compensatorios para aquellos controles de seguridad de la información que no puedan mantenerse durante una situación adversa.<br>(AENOR, 2015) |
| Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | Se debe considerar las siguientes directrices:<br>La empresa debe verificar su gestión de la continuidad de la seguridad de la información:<br>• Ejecutar, probar la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información.<br>• Ejecutar, probar el conocimiento y la rutina para operar los procesos, procedimientos y controles de la continuidad de la seguridad de la información.<br>• Revisar la validez y efectividad de las medidas para la continuidad de la seguridad de la información cuando cambien los sistemas de información, los procesos de seguridad de la información, procedimientos y controles o los procesos y soluciones de gestión de negocio y recuperación de desastres.<br>(AENOR, 2015) |
| Disponibilidad de instalaciones de procesamiento de información. | Se debe considerar las siguientes directrices:<br>• La empresa debe identificar los requisitos de disponibilidad para los sistemas de información.<br>• Si no se pueden garantizar la disponibilidad de los sistemas, con la arquitectura actual, optar por componentes o arquitecturas redundantes.<br>• Si se aplica arquitecturas redundantes se debe probar para asegurar la continuidad y el funcionamiento esperado.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

l) Relación con los proveedores

**Tabla 46:** Relación con los proveedores

| **Objetivo:** | Asegurar la protección de los activos de la organización que sean accesibles para los proveedores. |
|---|---|
| **Criterios de seguridad** | |
| Política de seguridad de la información para las relaciones con los proveedores. | Se debe considerar las siguientes directrices:<br>• Identificación y documentación de los tipos de proveedores.<br>• Definir tipos de acceso a la información que se les permitirá a los proveedores.<br>• Requisitos de seguridad de la información: por datos, tipos de acceso, para los proveedores de acuerdo a las necesidades del negocio, empresa.<br>• Procesos y procedimientos para supervisar el cumplimiento de los requisitos de seguridad establecidos para cada proveedor.<br>• Controles de exactitud y completitud para los datos.<br>• Obligaciones aplicables a los proveedores.<br>• Gestión de incidencias y contingencias asociadas al acceso de los proveedores.<br>• Concienciación al personal de la empresa que realiza compras con respecto a las políticas, procesos y procedimientos aplicables.<br>• Condiciones bajo las que los requisitos y controles de seguridad de la información se documentan, firmado por las 2 partes.<br>(AENOR, 2015) |
| Tratamiento de la seguridad dentro de los acuerdos con proveedores. | Se debe considerar las siguientes directrices:<br>• Descripción de la información facilitada o accedida.<br>• Métodos para facilitar o acceder a la información.<br>• Clasificación de la información de acuerdo con el esquema de clasificación de la empresa.<br>• Requisitos legales, incluyendo protección de datos personales, derechos de propiedad intelectual, derechos de autor.<br>• Normas de uso aceptable de la información.<br>• Lista explicita del personal autorizado para acceder o recibir la información de la empresa, procedimientos y condiciones de la autorización, baja de la autorización.<br>• Requisitos y procedimientos de gestión de incidentes.<br>• Derecho de auditar procesos de los proveedores.<br>• Procesos de resolución de contrato por defecto y por conflictos.<br>• Obligaciones de los proveedores para cumplir con los requisitos de seguridad de la empresa.<br>(AENOR, 2015) |
| Cadena de suministro de tecnología de información y comunicación. | Se debe considerar las siguientes directrices:<br>• Requisitos de seguridad en la compra de productos y servicios de TICs.<br>• Requisitos de seguridad de la información general de relaciones con los proveedores.<br>• Requisitos de seguridad de la información a nivel de servicios.<br>• Requisitos de seguridad de la información a nivel de productos TIC, prácticas de seguridad en toda la cadena se suministró. |

| | |
|---|---|
| | • Procesos de supervisión y métodos para validar productos y servicios.<br>• Procesos para la gestión de información, ciclo de vida, disponibilidad y los riesgos asociados a los componentes TIC.<br>(AENOR, 2015) |
| Seguimiento y revisión de los servicios de los proveedores. | Se debe considerar las siguientes directrices:<br>• Supervisar los niveles de rendimiento del servicio para verificar el cumplimiento de los acuerdos.<br>• Revisar los informes del servicio producidos por el proveedor.<br>• Llevar a cabo auditorias de los proveedores.<br>• Documentar los incidentes de seguridad de la información<br>• Revisar pistas de auditorías de los proveedores, registro s de eventos de seguridad de la información, problemas operativos, fallos, registro de errores, interrupciones del servicio prestado.<br>• Resolver los problemas detectados.<br>(AENOR, 2015) |
| Gestión de cambios en los servicios de proveedores. | Se debe considerar las siguientes directrices:<br>• Cambios en los acuerdos con los proveedores.<br>• Cambios realizados por la empresa para implementar.<br>• Cambios en los servicios de los proveedores para implementar.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

m)Criptografía

**Tabla 47:** Criptografía

| **Objetivo:** | Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información. |
|---|---|
| **Criterios de seguridad** | |
| Política sobre el uso de controles criptográficos. | Las políticas de criptografía deben tomar en cuenta:<br>• Identificar el nivel de protección necesario, tomando en cuenta el tipo, fortaleza y la calidad del algoritmo de cifrado requerido.<br>• Uso de cifrado para proteger la información sensible transportada a través de dispositivos móviles o extraíbles.<br>• Uso de métodos para la protección de claves criptográficas y la recuperación de la información cifrada en caso de perdida, vulneración o daño.<br>Los controles criptográficos deben utilizarse para alcanzar los objetivos de seguridad:<br>• Confidencialidad: uso de cifrado para proteger información sensible o critica, cuando se almacena o transporta.<br>• Integridad/autenticidad: uso de códigos de autenticación de mensajes para verificar la autenticidad, la integridad de la información sensible o critica, si se almacena o se transmite.<br>• No repudio: uso de técnicas criptográficas para obtener pruebas de la existencia o inexistencia de un evento o acción.<br>• Autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso, |

| | |
|---|---|
| | transacciones con usuarios, entidades y recursos de los sistemas.<br>(AENOR, 2015) |
| Gestión de llaves. | La gestión de llaves se basa en un conjunto de normas, procedimiento y métodos seguros:<br>• Generar claves para las diferentes aplicaciones.<br>• Generar y obtener certificados de claves públicas.<br>• Distribuir las claves a los usuarios, la forma en que los usuarios autorizados deben acceder a las mismas.<br>• Almacenar claves, incluyendo la forma en que los usuarios autorizados deben acceder a las mismas.<br>• Cambiar o actualizar claves, incluyendo las normas relativas a cuándo y cómo deberían cambiarse.<br>• Medidas para actual ante claves comprometidas.<br>• Retirar o desactivar claves, incluyendo el procedimiento que debe aplicarse.<br>• Recuperar claves pérdidas o corruptas.<br>• Realizar copias de respaldos o archivar claves.<br>• Destruir claves.<br>• Registrar y auditar las actividades que tiene que ver con la gestión de claves.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

n) Políticas de seguridad de la información

**Tabla 48:** Políticas de seguridad de la información

| **Objetivo:** | Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas vigentes. |
|---|---|
| **Criterios de seguridad** | |
| Políticas para la seguridad de la información. | Se debe considerar las siguientes directrices:<br>• Control de accesos<br>• Clasificación de la información<br>• Seguridad física y ambiental<br>• Temas orientados al usuario final<br>• Copias de respaldos<br>• Transferencia de información<br>• Protección ante software malicioso<br>• Gestión de vulnerabilidades técnicas<br>• Controles criptográficos<br>• Seguridad de las comunicaciones<br>• Privacidad y protección de la información identificativa de personas.<br>• Relaciones con proveedores.<br>(AENOR, 2015) |
| Revisión de políticas para la seguridad de la información. | Se debe considerar las siguientes directrices:<br>• En intervalos planificados.<br>• Cuando se produzcan cambios significativos.<br>• Responsable de desarrollo, revisión y evaluación.<br>• Aprobación de la Dirección empresarial a la política revisada.<br>(AENOR, 2015) |

**Elaborado por:** Investigador

Los criterios de seguridad que requieren definir la normativa de control, son: política de desarrollo seguro, principios de construcción de sistemas seguros y ambiente de desarrollo seguro, que engloban un conjunto de directrices, que se detallan en las TABLAS 49, 50, 51.

**Normativa para el criterio:** Política de desarrollo seguro

**Tabla 49:** Política de desarrollo seguro

| N° | Directriz | Recurso | Política | |
|---|---|---|---|---|
| **1** | Seguridad del entorno de desarrollo. | Personas<br>Tecnología | Debe existir expertos en el uso y manejo de las herramientas configuradas en el entorno de desarrollo para responder a todas las interrogantes que se presente. | Herramientas para el desarrollo web, móvil.<br>Expertos en herramientas: Framework Netbens 8.2, PostgreSQL 9.3, Mongo DB Ireport – Designer.<br>Entorno de ejecución para NODE JS (8.9.3), IONIC 2 |
| | | | Uso de herramienta de gestión de proyectos y procesos de software. | Genji 4.0.2 para metodologías de desarrollo ágil, como es SCRUM. |
| | | | Uso de compiladores y generadores de código apropiados para el producto a construir. | |
| **2** | Seguridad en el ciclo de vida de desarrollo de software. | Análisis | Identificación de requerimientos que tendrán impacto en aspectos de seguridad. | Iniciar de sesión, cerrar sesión, cambio de contraseña, actualización de los datos de las cuentas de usuario, registro de datos (datos sensibles). |
| | | | Requerimientos de registro de auditorías, que es lo que debe registrar la aplicación en los logs. | Identificador del Cliente<br>Identificador de la organización<br>Identificador del usuario que registra los datos.<br>Identificador del usuario que actualiza los datos.<br>Fecha de creación del registro.<br>Fecha de modificación del registro.<br>Estado del registro. |
| | | | Evaluación de riesgos. | Identificar riesgos basados en:<br>Requerimientos incompletos.<br>Deficiencia en el involucramiento del usuario.<br>Deficiencia de recursos. |

| | | | | |
|---|---|---|---|---|
| | | | | Cambios en los requerimientos y especificaciones.<br>Deficiencia en la planeación.<br>Desconocimiento en tecnología.<br>Deficiencia en la administración de TI (TI: tecnologías de la información). |
| | | | | Analizar los riesgos:<br>Estimar los riesgos, priorizarlos de mayor a menor exposición. |
| | | | | Planear los riesgos:<br>Prevenir, minimizar y establecer planes de contingencia. |
| | | | | Supervisión de riesgos:<br>Alertar sobre los riesgos del proyecto y evitar que los administradores y desarrolladores los ignoren en la planificación.<br>Supervisar la efectividad de los planes de reducción de riesgos.<br>Realizar el análisis costo – beneficio para la prevención. |
| | | Diseño | Diseño de autorización: roles, permisos y privilegios. | Roles de usuarios: nivel alto (administrador), nivel medio (operador), nivel bajo (cliente). |
| | | | Mecanismos de protección de datos.<br>Diseño seguro de mensajes de autenticación.<br>Diseño seguro de mensajes de advertencia.<br>Diseño seguro de mensajes de confirmación.<br>Diseño seguro de mensajes de error. | Los mensajes se personalizan de acuerdo al perfil de usuario, módulo, vista y operación.<br>Para los errores internos de los aplicativos, se utilizarán 6 campos dentro del mensaje<br>**Nombre:** nombre corto del error.<br>**Número:** identificador del diccionario de errores.<br>**Descripción:** es la causa dl error.<br>**Solución:** se enviará una posible solución al error.<br>**Detalle:** se enviará toda la captura del error. |

| | | | | |
|---|---|---|---|---|
| | | | | **Id:** número entero de identificación del sistema. |
| | | | Diseño de autenticación (Modo en que los usuarios se van a autenticar). | Nombre de usuario, o correo electrónico, o número de celular y la contraseña. |
| | | Codificación | Validar siempre los datos de entrada antes de procesarlos.<br>Realizar validación de datos en todas las capas.<br>Controlar tamaño y tipo de datos.<br>Eliminar caracteres especiales.<br>Transformar los datos de entrada a una codificación establecida.<br>Utilizar sentencias SQL dinámicas en vez de procedimientos almacenados.<br>No mezclar datos con código.<br>Capturar errores de capas inferiores y no mostrarlos al usuario. | Aplicación de las buenas prácticas que recomiendan el CERT, OWASP, SAFECODE. |
| | | Pruebas | Diseño del plan de pruebas.<br>Diseño de casos de pruebas.<br>Encontrar errores funcionales.<br>Uso de herramientas de prueba. | Pruebas de integración.<br>Pruebas de funcionalidad.<br>Pruebas de rendimiento.<br>Pruebas de carga.<br>Pruebas de desempeño.<br>Pruebas de volumen.<br>Pruebas de integridad de los datos y de la base de datos.<br>Pruebas de configuraciones.<br>Pruebas de interfaces. |
| | | Despligue | Cambios de usuarios y contraseñas iniciales por defecto.<br>Borrado de datos de prueba.<br>Cambios de permisos de accesos.<br>Revisión de las configuraciones y su nivel de seguridad (servidor, red). | Si se utiliza un servidor en la nube, configurar los patrones de conexión, para que no pueda acceder cualquier persona que tenga acceso a la red. |
| **3** | Seguridad en el control de versiones. | | Evaluación de las seguridades al momento que se efectúen cambios o actualizaciones de versiones en el software. | Pruebas del software para determinar el nivel de cumplimiento de las directrices de seguridad. |

| | | | | |
|---|---|---|---|---|
| **4** | Capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades. | Evitar | Conocimiento y puesta en aplicación de buenas prácticas de codificación segura.<br>Conocimiento del modelado de seguridad que les permita describir y planificar como evitar vulnerabilidades, determinando el nivel correcto de seguridad.<br>Uso de herramientas de modelado de seguridad en las primeras fases de diseño. | Aplicación de las buenas prácticas que recomiendan el CERT, OWASP, SAFECODE. |
| | | Encontrar | Mediante el uso de inyección SQL<br>Secuencia de comandos cruzados.<br>Falsificación de sitios cruzados. | Informar las vulnerabilidades encontradas. |
| | | Reparar | Plan de remediación específico para las vulnerabilidades encontradas.<br>Reparar las vulnerabilidades a corto, mediano y largo plazo.<br>Implantar el control respectivo (costo, capacidad y facilidad de implementación).<br>Informar. | |

**Elaborado por:** Investigador

**Normativa para el criterio:** Principios de construcción de sistemas seguros.

**Tabla 50:** Política para la construcción de sistemas seguros

| N° | Directriz | Recurso | Política |
|---|---|---|---|
| **1** | Seguridad diseñada en todas capas de la arquitectura del software. | Datos | Inserción y extracción segura de los datos desde y hacia la base de datos.<br>El repositorio se debe comunicar solo con la lógica de negocio.<br>Resguardo y recuperación.<br>Clasificación.<br>Planificar la gestión de los datos: listar los datos gestionados por cada proyecto, descripción del formato y sus requisitos de privacidad y seguridad, establecer los permisos para controlar datos confidenciales. |
| | | Negocio | Uso del estándar para la construcción de servicios web seguros.<br>Creación y control de servicios web genéricos y seguros para las aplicaciones web y móviles.<br>Método GET para consultas.<br>Método POST para inserciones.<br>Método PUT para actualizaciones.<br>Método DELETE para eliminaciones.<br>En las bases de datos el CORE filtrara automáticamente solo la información a la cual tiene acceso el usuario. |
| | | Presentación | Alto grado de seguridad en las interfaces para los clientes web y móviles de los aplicativos. |

| | | | |
|---|---|---|---|
| **2** | Analisis de los riesgos de seguridad de las nuevas tecnologías a utilizar. | | Análisis de la calidad de herramientas.<br>Prueba de las nuevas tecnologías.<br>Análisis de la interacción de una nueva tecnología con las ya existentes. |

**Elaborado por:** Investigador

**Normativa para el criterio:** Ambiente de desarrollo seguro.

**Tabla 51:** Política para ambiente de desarrollo seguro

| N° | Directriz | Política |
|---|---|---|
| **1** | Sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema. | Los datos productivos de la empresa son procesados por aplicaciones desarrolladas para ese fin.<br>Los datos altamente sensibles, requieren ser cifrados a través de un algoritmo de cifrado simétrico para ser almacenados o transmitidos. |
| **2** | Honradez del personal que trabaja en el entorno empresarial. | Hacer cumplir las políticas de seguridad de la información.<br>Realizar prácticas de concienciación del personal, publicar boletines, recomendaciones para captar su compromiso de trabajo. |
| **3** | Controles de seguridad ya implementados por la empresa que apoyen el desarrollo de los sistemas. | En el diseño de las bases de datos del Core se definen campos de control para auditorias: en cada entidad deben existir los siguientes campos, ejemplo:<br>ad_nombretabla_id (clave_primaria),<br>ad_nombretabla_id (clave foránea, en caso que exista),<br>creado_por (nombre de la persona que creo),<br>modificado_por (nombre de la persona que modifico),<br>fecha_creacion (fecha de creación),<br>fecha_actualizacion (fecha de actualización),<br>activo (Valores que toma: true, false),<br>ad_cliente_id (identificador del cliente al que le pertenece la información),<br>ad_organizacion_id(identificador de la organización a la que pertenece).<br><br>Módulo de seguridades (Configuraciones) |
| **4** | Control de acceso al entorno de desarrollo. | Responder por las claves de ingreso a los sistemas, no deben compartir las calves con otros empleados, ya que estas serán privadas.<br>Cambiar regularmente la clave, siguiendo estándares de claves seguras.<br>Cada empleado es responsable de los procedimientos ejecutados con sus credenciales de acceso. |
| **5** | Control del movimiento de datos desde y hacia el entorno. | Comprobar la realización de copias de seguridad. |

**Elaborado por:** Investigador

### 6.8.3. FASE 3: Proyección de resultados por aplicación de la normativa

(VER TABLA 52)

**Tabla 52:** Proyección de resultados por aplicación de la normativa

| DOMINIOS ISO 27001:2013 | PLAZO DE EJECUCIÓN | PROYECCIÓN DE RESULTADOS |
|---|---|---|
| Políticas de seguridad de la información | Si las directrices son puestas en marcha, a mediano y largo plazo. | Políticas analizadas, definidas, revisadas y documentadas. |
| Organización de la seguridad de la información | Si las directrices son puestas en marcha, a mediano y largo plazo. | Roles y responsabilidades definidas.<br>Separación de deberes definidas.<br>Contacto con las autoridades y grupos de interés definidas de acuerdo a las necesidades.<br>Cumplimiento de políticas de seguridad para dispositivos móviles y teletrabajo. |
| Seguridad de los recursos humanos | Si las directrices son puestas en marcha, a mediano y largo plazo. | Personal capacitado, educado y concientizado.<br>Conocimiento y cumplimiento de los términos y condiciones para trabajar y cuando se cambie de funciones o finalice el trabajo.<br>Conocimiento y cumplimiento de las responsabilidades que tiene la dirección empresarial.<br>Socialización de los procesos disciplinarios al personal de trabajo. |
| Gestión de Activos | Si las directrices son puestas en marcha, a mediano y largo plazo. | Inventariado todos los recursos de TI.<br>Responsables de los activos definido.<br>Constancia del uso aceptable de activos.<br>Constancia de la devolución de activos.<br>Información empresarial etiquetada.<br>La manipulación de la información bajo autorización y por procesos aprobados.<br>Gestión de medios removibles completada.<br>Disposición de medios completada.<br>Transferencia de medios físicos seguros, bajo autorización y con el registro correspondiente. |
| Control de Accesos | Si las directrices son puestas en marcha, mediano y largo plazo. | Políticas de control de acceso definidas y cumplidas.<br>Política sobre el uso de los servicios de red definidas y cumplidas.<br>Registro y cancelación del registro de usuarios definidas y cumplidas.<br>Suministro de acceso de usuarios autorizados garantizado.<br>Gestión de información de autenticación secreta de usuarios controlado.<br>Retiro o ajuste de los derechos de acceso bajo políticas establecidas formalmente.<br>Uso de la información de autenticación secreta bajo autorización y procesos establecidos.<br>Restricciones de acceso a la información definidas y en cumplimiento.<br>Procedimiento de ingreso seguro definido y en cumplimiento.<br>Sistemas de gestión de contraseñas definido y en ejecución. |

| | | |
|---|---|---|
| | | Uso de programas utilitarios privilegiados bajo autorización y con las restricciones aplicadas.<br>El control de acceso a código fuente de los programas esta/estará controlado. |
| Criptografía | Si las directrices son puestas en marcha, a mediano y largo plazo. | Política sobre el uso de controles criptográficos definidos y aplicados.<br>Gestión de llaves definido y aplicados. |
| Seguridad Física y Ambiental | Si las directrices son puestas en marcha, a mediano y largo plazo. | Seguridad de oficinas, recintos e instalaciones garantizado.<br>Protección contra amenazas externas y ambientales garantizado.<br>Trabajo en áreas seguras garantizado.<br>Áreas de despacho y carga garantizado.<br>Ubicación y protección de los equipos en espacios adecuados y seguros.<br>Servicios de suministro debidamente controlados.<br>Seguridad del cableado garantizado.<br>Mantenimiento de equipos continuo.<br>Retiro de activos bajo procesos definidos.<br>Seguridad de equipos y activos fuera de las instalaciones garantizado.<br>Disposición segura o reutilización de equipos garantizado.<br>Equipos de usuarios desatendidos controlado.<br>Política de escritorio limpio y pantalla limpia definida y aplicado. |
| Seguridad de las Operaciones | Si las directrices son puestas en marcha, a mediano y largo plazo. | Procedimientos de operación documentados y en ejecución.<br>Gestión de cambios definidos y aplicados.<br>La separación de los ambientes de desarrollo, pruebas y operación garantizado.<br>Controles contra códigos maliciosos, en ejecución y aplicados.<br>Respaldos de información programados de manera continua.<br>Registro de eventos documentados.<br>Protección de la información de registro garantizado.<br>Registros del administrador y del operador.<br>Sincronización de relojes según acuerdos generales.<br>Instalación de software en sistemas operativos, bajo autorización.<br>Gestión de las vulnerabilidades técnicas, atendidas y documentadas.<br>Restricciones sobre la instalación de software, socializadas.<br>La información de los controles de auditoria de sistemas, documentada, registrada y disponible. |

| | | |
|---|---|---|
| Seguridad en las comunicaciones | Si las directrices son puestas en marcha, a mediano y largo plazo. | Controles de redes aplicados.<br>Seguridad de los servicios de red garantizado.<br>Separación en las redes de acuerdo a prioridades.<br>Políticas y procedimientos de transferencia de información documentadas y en ejecución.<br>Acuerdos sobre transferencia de información cumplidos.<br>Mensajería electrónica controlada.<br>Acuerdos de confidencialidad o de no divulgación definidos y en cumplimiento. |
| Adquisición, desarrollo y mantenimientos de sistemas | Si las directrices son puestas en marcha, a mediano y largo plazo. | Análisis y especificación de requisitos de seguridad de la información cumplido y completo.<br>Seguridad de servicios de las aplicaciones en redes públicas garantizado.<br>Protección de transacciones de los servicios de las aplicaciones garantizado.<br>Política de desarrollo seguro documentada y en cumplimiento.<br>Procedimientos de control de cambios en sistemas cumplidos.<br>Revisión técnica de las aplicaciones después de cambios en la plataforma de operación garantizado.<br>Restricciones en los cambios a los paquetes de software aplicados.<br>Aplicados los principios de construcción de sistemas seguros.<br>Ambiente de desarrollo seguro garantizado.<br>Desarrollo contratado externamente bajo políticas y acuerdos establecidos.<br>Pruebas de seguridad de sistemas finalizadas.<br>Pruebas de aceptación de sistemas finalizadas.<br>Protección de datos de prueba finalizadas. |
| Relación con proveedores | Si las directrices son puestas en marcha, a mediano y largo plazo. | Política de seguridad de la información para las relaciones con los proveedores documentadas y aplicadas.<br>Tratamiento de la seguridad dentro de los acuerdos con proveedores garantizado.<br>Seguimiento y revisión de los servicios de los proveedores en ejecución.<br>Gestión controlada de los cambios en los servicios de proveedores. |
| Gestión de incidentes de seguridad de la información | Si las directrices son puestas en marcha, a mediano y largo plazo. | Responsabilidades y procedimientos definidos, documentados y en ejecución.<br>Reporte de eventos de seguridad de la información, acorde en el tiempo y de acuerdo a la necesidad o urgencia.<br>Reporte de debilidades de seguridad de la información acorde en el tiempo y de acuerdo a la necesidad o urgencia. |

| | | |
|---|---|---|
| | | Evaluación de eventos de seguridad de la información y decisiones sobre ellos, en ejecución, informes generados.<br>Respuesta a incidentes de seguridad de la información, documentados técnicamente.<br>Aprendizaje obtenido de los incidentes de seguridad de la información socializados.<br>Recolección de evidencia, debe tener un sustento aceptable. . |
| Aspectos de seguridad de la información dentro de la continuidad del negocio | Si las directrices son puestas en marcha, a mediano y largo plazo. | La planificación de la continuidad de la seguridad de la información será continuamente, documentada y estará en constante ejecución.<br>Implementación de la continuidad de la seguridad de la información.<br>Verificación, revisión y evaluación de la continuidad de la seguridad de la información, será un proceso formal y se realizará continuamente.<br>Disponibilidad de instalaciones de procesamiento de información garantizado. |
| Conformidad | Si las directrices son puestas en marcha, a mediano y largo plazo. | Identificación de la legislación aplicable y los requisitos contractuales en ejecución.<br>Derechos de propiedad intelectual.<br>Protección de registros.<br>Privacidad y protección de datos personales garantizado.<br>Reglamentación de controles criptográficos documentados, aplicados.<br>Revisión independiente de la seguridad de la información será un proceso continuo que generará informes técnicos de los resultados obtenidos.<br>Cumplimiento de políticas y normas de seguridad.<br>Revisión de cumplimiento técnico. |

**Elaborado por:** Investigador

## 6.9. Conclusiones

- Los parámetros de protección que son parte de la normativa de seguridad de la información se definen en base a los requisitos que exige la Norma Internacional ISO 27001:2013, estos son complementarios entre sí y contemplan los siguientes dominios: políticas y seguridad de la información; seguridad de los recursos humanos, física y ambiental, de las operaciones, de las comunicaciones; gestión de activos, incidentes de seguridad; controles de accesos, criptografía, adquisición, desarrollo y mantenimientos de sistemas, proveedores, continuidad del negocio y conformidad; todos tienen el mismo nivel de importancia en la aplicabilidad a los procesos del negocio empresarial.

- La normativa de seguridad de la información a aplicar a los recursos que intervienen en la protección de datos de los sistemas informáticos en la empresa de desarrollo de software STD S.A., contemplan un conjunto aceptado de directrices de control a implantar, supervisar, revisar y mejorar lo que tiende a garantizar la seguridad de la información en todo el ciclo de vida.
- Los criterios de seguridad (13) establecidos en el dominio **adquisición, desarrollo y mantenimiento de sistemas** determinan que es necesario tomar en cuenta el análisis y especificación de requisitos de seguridad, seguridad de servicios de las aplicaciones en redes públicas, protección de transacciones, políticas de desarrollo seguro, pruebas de seguridad y aceptación, y la protección de datos de prueba para disponer de sistemas informáticos seguros.
- Las directrices aplicables en la implementación de los sistemas informáticos en STD son la política de desarrollo seguro, política para la construcción de sistemas seguros y política para ambiente de desarrollo seguro, se definen los recursos tecnológicos, profesionales, metodológicos y las acciones que favorezcan a la seguridad de la información, siendo la seguridad diseñada en todas capas de la arquitectura del software, la seguridad en el ciclo de vida de desarrollo de software y la seguridad del entorno de desarrollo las directrices que apoyen a responder por seguridad de la información

## 6.10. Recomendaciones

- Se recomienda a las empresas que se dedican al desarrollo de software enfatizar la atención en todos los dominios que la norma ISO 27001:2013 establece ser implantados en materia de seguridad de la información.
- Se recomienda que, la implementación de la normativa de seguridad de la información en la empresa de desarrollo de software STD, cumpla con todos los dominios que establece la Norma ISO 27001; el mayor nivel de aceptación y cumplimiento de dichos dominios dependerá de las propuestas de solución que se planteen a medida que se maneje y gestione las vulnerabilidades, amenazas y riesgos identificados.
- Se recomienda que los criterios de seguridad establecidos en el dominio **adquisición, desarrollo y mantenimiento de sistemas** sean planificados,

ejecutados, revisados y documentados continuamente tomado en cuenta todas las directrices planteadas, ya que de esta manera se garantiza la creación de sistemas informáticos seguros y confiables, minimizando los posibles riesgos de la información.

- Se recomienda que en la política **Seguridad diseñada en todas capas de la arquitectura del software**, desde el recurso **capa de negocio**, se vigile la seguridad de los datos mediante la definición y uso de servicios web genéricos para las consultas, inserciones, actualizaciones y eliminaciones en las bases de datos.

## BIBLIOGRAFÍA


AENOR. (2015). UNE-ISO/IEC 27002. En C. T. AEN/CTN, *Código e prácticas para controles de seguridad de la información* (pág. 99). Madrid: AENOR.

Agencia de Control y Regulación de Electricidad. (19 de Septiembre de 2013). Esquema Gubernamental de Seguridad de la Información (EGSI). Quito, Provincia, Ecuador.

Asociación Española de Normalización y Certificación. (Julio de 2015). Tecnologías de la Información, Técnicas de seguridad, Código de prácticas para controles de la información. Madrid, España: Aenor.

Guaman, J. A. (04 de 2015). *http://bibdigital.epn.edu.ec.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Guindel, E. (11 de 2009). *Calidad y seguridad de la información y auditoria informática.* Obtenido de http://e-archivo.uc3m.es: http://e-

archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence=1

Investigador. (15 de 05 de 2017). Protección de los datos de los sistemas informáticos de las empresas de desarrollo de software. Riobamba, Chimborazo, Ecuador.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN. (30 de 06 de 2011). *MINISTERIO DE TELECOMUNICACIONES PARTICIPÓ EN EL XIII CONGRESO INTERAMERICANO DE SEGURIDAD DE LA*, pág. 3.

Ribagorda , A. (2008). LA PROTECCIÓN DE DATOS PERSONALES. *REVISTA JURÍDICA DE CASTILLA Y LEÓN. N.º 16.*, 28.

Rosero, P. (Abril de 2015). *http://bibdigital.epn.edu.ec.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/10488/1/CD-6208.pdf

Secretaría Nacional de la Administración Pública. (01 de 2014). *http://www.administracionpublica.gob.ec.* Obtenido de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2015/04/PROYECTO-IMPLEMENTACION-CONTROL-Y-SEGUIMIENTO.pdf

Techtarget. (08 de 2015). *techtarget.com.* Obtenido de http://searchdatacenter.techtarget.com/es/cronica/La-Seguridad-de-la-Informacion-crece-entre-las-empresas-individuos-y-el-gobierno-brasileno

**ANEXOS**

## ENCUESTA

**UNIVERSIDAD TÉCNICA DE AMBATO**
**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL**

Encuesta dirigida a gerentes, directores, scrum masters y desarrolladores de software.

**Objetivo:** Conocer el criterio de los Gerentes, directores, scrum masters y desarrolladores de software sobre la seguridad de información en sus ambientes de trabajo.

**Instrucciones:**

- Al ser anónima la encuesta, responda con toda libertad y sinceridad.
- Antes de contestar las preguntas, lea detenidamente.
- Marque con una X dentro de la caja de texto la respuesta que usted considere.

### Cuestionario

**1. ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?**

SI (__)

NO (__)

**2. ¿El computador asignado para el desarrollo de sus funciones posee un antivirus?**

SI (__)

NO (__)

**3. ¿La empresa posee software legal en su totalidad?**

SI (__)

NO (__)

4. **¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado?**

SI (__)

NO (__)

5. **¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa?**

SI (__)

NO (__)

6. **¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información?**

SI (__)

NO (__)

7. **¿La empresa capacita al personal en temas de seguridad de la información?**

SI (__)

NO (__)

8. **¿Existe algún control para navegar en internet?**

SI (__)

NO (__)

9. **¿Existe control sobre el uso del correo electrónico?**

SI (__)

NO (__)

10. **¿Existe alguna política para el cambio regular de las contraseñas?**

SI (__)

NO (__)

**11. ¿Antes y después de la contratación del personal se hace entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información?**

SI (__)

NO (__)

**12. ¿La información disponible en los repositorios de datos se mantiene exacta?**

SI (__)

NO (__)

**13. ¿La información disponible en los repositorios de datos es completa?**

SI (__)

NO (__)

**14. ¿La información solo está disponible para accesos autorizados?**

SI (__)

NO (__)

**15. ¿Se garantiza el almacenamiento de la información?**

SI (__)

NO (__)

**16. ¿Se garantiza el acceso oportuno hacia la información?**

SI (__)

NO (__)

**17. ¿La información está disponible para actualizaciones constantes?**

SI (__)

NO (__)

**18. ¿Se identifica quién realiza cambios en la información?**

SI (__)

NO (__)

**19. ¿Se conoce en qué momento se cambió la información?**

SI (__)

NO (__)

**20. ¿El contenido de la información que está disponible es comprobable?**

SI (__)

NO (__)

**21. ¿La información disponible es verdadera?**

SI (__)

NO (__)

**22. ¿Se realiza respaldos de los datos?**

SI (__)

NO (__)

**23. ¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?**

SI (__)

NO (__)

**24. ¿Existen zonas restringidas de acceso de personal?**

SI (__)

NO (__)

**25. ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?**

SI (__)

NO (__)

**26. ¿Se cuenta con sistemas de alarma como detectores de humo, humedad?**

SI (__)

NO (__)

**27. ¿Existe vigilancia en la entrada del edificio?**

SI (__)

NO (__)

**GRACIAS POR SU ATENCIÓN**

## GUIA DE OBSERVACIÓN

**Objetivo:** Determinar a través de la observación los criterios de la seguridad de la información que se aplican en las empresas de desarrollo de software, basado en la Norma Internacional ISO/IEC 27001:2013.

| DOMINIOS | CRITERIO | DESCRIPCIÓN | RESPONSABLE | CUMPLE | NO CUMPLE |
|---|---|---|---|---|---|
| **A.5. Relativo a políticas de seguridad de la información** | | | | | |
| Directrices establecidas por la dirección para la seguridad de la información. | Políticas para la seguridad de la información. | | | | |
| | Revisión de políticas para la seguridad de la información. | | | | |
| **A.6. Relativo a Organización de la seguridad de la información** | | | | | |
| Organización interna | Roles y responsabilidades para la seguridad de la información. | | | | |
| | Separación de deberes. | | | | |
| | Contacto con las autoridades. | | | | |
| | Contacto con grupos de interés especial. | | | | |
| | Seguridad de la información en la gestión de proyectos. | | | | |
| | Políticas para dispositivos móviles | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Dispositivos móviles y teletrabajo. | Teletrabajo | | | | |
| **A.7. Relativo a seguridad de los recursos humanos** | | | | | |
| Antes de asumir el empleo. Durante la ejecución del empleo. | Selección | | | | |
| | Términos y condiciones de empleo | | | | |
| | Responsabilidades de la dirección. | | | | |
| | Toma de conciencia, educación y formación en la seguridad de la información. | | | | |
| | Proceso disciplinario. | | | | |
| Terminación o cambio de empleo. | Terminación o cambio de responsabilidades de empleo. | | | | |
| **A.8 Relativo a gestión de activos** | | | | | |
| Responsabilidad por los activos. | Inventario de activos | | | | |
| | Propiedad de los activos | | | | |
| | Uso aceptable de los activos | | | | |
| | Devolución de los activos | | | | |
| Clasificación de la información. | Clasificación de la información | | | | |
| | Etiquetado de la información | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Manipulación de la información | | | | |
| | Gestión de medios removibles | | | | |
| | Disposición de los medios | | | | |
| | Transferencia de medios físicos | | | | |
| **A.9. Relativo a control de accesos** | | | | | |
| Requisitos del negocio para el control de acceso. | Política de control de acceso. | | | | |
| | Política sobre el uso de los servicios de red. | | | | |
| Gestión de accesos de usuarios. | Registro y cancelación del registro de usuarios. | | | | |
| | Suministro de acceso de usuarios. | | | | |
| | Gestión de derechos de acceso de privilegiado. | | | | |
| | Gestión de información de autenticación secreta de usuarios. | | | | |
| | Revisión de los derechos de acceso de usuarios. | | | | |
| | Retiro o ajuste de los derechos de acceso. | | | | |
| Responsabilidad de los usuarios. | Uso de la información de autenticación secreta. | | | | |
| Control de acceso a sistemas y aplicaciones. | Restricción de acceso a la información. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Procedimiento de ingreso seguro. | | | | |
| | Sistemas de gestión de contraseñas. | | | | |
| | Uso de programas utilitarios privilegiados. | | | | |
| | Control de acceso a código fuente de programas. | | | | |
| **A.10. Relativo a criptografía** | | | | | |
| Controles criptográficos | Política sobre el uso de controles criptográficos. | | | | |
| | Gestión de llaves. | | | | |
| **A.11. Relativo a seguridad física y ambiental** | | | | | |
| Áreas seguras | Perímetro de seguridad física | | | | |
| | Controles físicos de entrada | | | | |
| | Seguridad de oficinas, recintos e instalaciones. | | | | |
| | Protección contra amenazas externas y ambientales. | | | | |
| | Trabajo en áreas seguras. | | | | |
| | Áreas de despacho y carga. | | | | |
| Equipos | Ubicación y protección de los equipos. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Servicios de suministro. | | | | |
| | Seguridad de cableado. | | | | |
| | Mantenimiento de equipos. | | | | |
| | Retiro de activos. | | | | |
| | Seguridad de equipos y activos fuera de las instalaciones. | | | | |
| | Disposición segura o reutilización de equipos. | | | | |
| | Equipos de usuarios desatendidos. | | | | |
| | Política de escritorio limpio y pantalla limpia. | | | | |
| **A.12. Relativo a seguridad de las operaciones** | | | | | |
| Procedimientos operaciones y responsabilidades. | Procedimientos de operación documentados. | | | | |
| | Gestión de cambios. | | | | |
| | Gestión de capacidad. | | | | |
| | Separación de los ambientes de desarrollo, pruebas y operación. | | | | |
| Protección contra códigos maliciosos. | Controles contra códigos maliciosos. | | | | |
| Copias de respaldo. | Respaldos de información. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Registro y seguimiento. | Registro de eventos. | | | | |
| | Protección de la información de registro. | | | | |
| | Registros del administrador y del operador. | | | | |
| | Sincronización de relojes. | | | | |
| Control de software operacional. | Instalación de software en sistemas operativos. | | | | |
| Gestión de la vulnerabilidad técnica. | Gestión de las vulnerabilidades técnicas. | | | | |
| | Restricciones sobre la instalación de software. | | | | |
| Consideraciones sobre auditorias de sistemas de información. | Información controles de auditoria de sistemas. | | | | |
| **A.13. Relativo a seguridad en las comunicaciones** | | | | | |
| Gestión de la seguridad de las redes. | Controles de redes | | | | |
| | Seguridad de los servicios de red. | | | | |
| | Separación en las redes. | | | | |
| Transferencia de información. | Políticas y procedimientos de transferencia de información. | | | | |
| | Acuerdos sobre transferencia de información. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Mensajería electrónica. | | | | |
| | Acuerdos de confidencialidad o de no divulgación. | | | | |
| **A.14. Relativo a adquisición, desarrollo y mantenimientos de sistemas** | | | | | |
| Requisitos de seguridad de los sistemas de información. | Análisis y especificación de requisitos de seguridad de la información. | | | | |
| | Seguridad de servicios de las aplicaciones en redes públicas. | | | | |
| | Protección de transacciones de los servicios de las aplicaciones. | | | | |
| Seguridad en los procesos de desarrollo y soporte. | Política de desarrollo seguro | | | | |
| | Procedimientos de control de cambios en sistemas. | | | | |
| | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. | | | | |
| | Restricciones en los cambios a los paquetes de software. | | | | |
| | Principios de construcción de sistemas seguros. | | | | |
| | Ambiente de desarrollo seguro. | | | | |
| | Desarrollo contratado externamente. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Pruebas de seguridad de sistemas. | | | | |
| | Pruebas de aceptación de sistemas. | | | | |
| Datos de prueba | Protección de datos de prueba. | | | | |
| **A.15. Relativo a relación con proveedores** | | | | | |
| Seguridad de la información en las relaciones con los proveedores. | Política de seguridad de la información para las relaciones con los proveedores. | | | | |
| | Tratamiento de la seguridad dentro de los acuerdos con proveedores. | | | | |
| | Cadena de suministro de tecnología de información y comunicación. | | | | |
| Gestión de la prestación de servicios con los proveedores. | Seguimiento y revisión de los servicios de los proveedores. | | | | |
| | Gestión de cambios en los servicios de proveedores. | | | | |
| **A.16. Relativo a gestión de incidentes de seguridad de la información** | | | | | |
| Gestión de incidentes y mejoras en la seguridad de la información. | Responsabilidad y procedimientos. | | | | |
| | Reporte de eventos de seguridad de la información. | | | | |
| | Reporte de debilidades de seguridad de la información. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Evaluación de eventos de seguridad de la información y decisiones sobre ellos. | | | | |
| | Respuesta a incidentes de seguridad de la información. | | | | |
| | Aprendizaje obtenido de los incidentes de seguridad de la información. | | | | |
| | Recolección de evidencia. | | | | |
| **A.17. Relativo a aspectos de seguridad de la información dentro de la continuidad del negocio** | | | | | |
| Continuidad de seguridad de la información. | Planificación de la continuidad de la seguridad de la información. | | | | |
| | Implementación de la continuidad de la seguridad de la información. | | | | |
| | Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | | | | |
| Redundancias | Disponibilidad de instalaciones de procesamiento de información. | | | | |
| **A.18. Relativo a conformidad** | | | | | |
| Cumplimiento de requisitos legales y contractuales. | Identificación de la legislación aplicable y los requisitos contractuales. | | | | |
| | Derechos de propiedad intelectual. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Protección de registros. | | | | |
| | Privacidad y protección de datos personales. | | | | |
| | Reglamentación de controles criptográficos. | | | | |
| Revisión de seguridad de la información. | Revisión independiente de la seguridad de la información. | | | | |
| | Cumplimiento con las políticas y normas de seguridad. | | | | |
| | Revisión del cumplimiento técnico. | | | | |

**Elaborado por:** Investigador

## PROCESAMIENTO DE LA INFORMACIÓN DE LAS ENCUESTAS POR EMPRESA

**Pregunta 1.** ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| Frecuencia | 5 | 7 | **12** | 1 | 4 | **5** | 5 | 0 | **5** |
| Porcentaje (%) | 41,67 | 58,83 | **100%** | 20 | 80 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 2:** ¿El computador asignado para el desarrollo de sus funciones posee un antivirus?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 11 | 1 | **12** | 5 | 0 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 91,67 | 8,33 | **100%** | 100 | 0 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 3:** ¿La empresa posee software legal en su totalidad?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 0 | 5 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 0 | 100 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 4:** ¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 5 | 7 | **12** | 3 | 2 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 41,67 | 58,33 | **100%** | 60 | 40 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 5:** ¿Existe al menos políticas, normativas o Sistema de Gestión de Seguridad de la Información en la empresa?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 0 | 12 | **12** | 4 | 1 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 0 | 100 | **100%** | 80 | 20 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 6:** ¿Considera necesario que la empresa invierta en la implantación de una normativa de Gestión de Seguridad de la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 10 | 2 | **12** | 5 | 0 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 83,33 | 16,67 | **100%** | 100 | 0 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 7:** ¿La empresa capacita al personal en temas de seguridad de la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 2 | 3 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 40 | 60 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 8:** ¿Existe algún control para navegar en internet?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 0 | 12 | **12** | 1 | 4 | **5** | 2 | 3 | **5** |
| **Porcentaje (%)** | 0 | 100 | **100%** | 20 | 80 | **100%** | 40 | 60 | **100%** |

**Elaborado por:** Investigador

**Pregunta 9:** ¿Existe control sobre el uso del correo electrónico?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 0 | 12 | **12** | 2 | 3 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 0 | 100 | **100%** | 40 | 60 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 10:** ¿Existe alguna política para el cambio regular de las contraseñas?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 0 | 12 | **12** | 0 | 5 | **5** | 1 | 4 | **5** |
| **Porcentaje (%)** | 0 | 100 | **100%** | 0 | 100 | **100%** | 20 | 80 | **100%** |

**Elaborado por:** Investigador

**Pregunta 11:** ¿Antes y después de la contratación del personal se hace entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 0 | 5 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 0 | 100 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 12:** ¿La información disponible en los repositorios de datos se mantiene exacta?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 3 | 2 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 60 | 40 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 13:** ¿La información disponible en los repositorios de datos es completa?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 2 | 3 | **5** | 4 | 1 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 40 | 60 | **100%** | 80 | 20 | **100%** |

**Elaborado por:** Investigador

**Pregunta 14:** ¿La información solo está disponible para accesos autorizados?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 7 | 5 | **12** | 3 | 2 | **5** | 4 | 1 | **5** |
| **Porcentaje (%)** | 58,33 | 41,67 | **100%** | 60 | 40 | **100%** | 80 | 20 | **100%** |

**Elaborado por:** Investigador

**Pregunta 15:** ¿Se garantiza el almacenamiento de la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 4 | 8 | **12** | 1 | 4 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 33,33 | 66,67 | **100%** | 20 | 80 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 16:** ¿Se garantiza el acceso oportuno hacia la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 4 | 8 | **12** | 2 | 3 | **5** | 4 | 1 | **5** |
| **Porcentaje (%)** | 33,33 | 66,67 | **100%** | 40 | 60 | **100%** | 80 | 20 | **100%** |

**Elaborado por:** Investigador

**Pregunta 17:** ¿La información está disponible para actualizaciones constantes?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 5 | 7 | **12** | 4 | 1 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 41,67 | 58,33 | **100%** | 80 | 20 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 18:** ¿Se identifica quién realiza cambios en la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 2 | 3 | **5** | 4 | 1 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 40 | 60 | **100%** | 80 | 20 | **100%** |

**Elaborado por:** Investigador

**Pregunta 19:** ¿Se conoce en qué momento se cambió la información?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 0 | 12 | **12** | 3 | 2 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 0 | 100 | **100%** | 60 | 40 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 20:** ¿El contenido de la información que está disponible es comprobable?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 0 | 12 | **12** | 3 | 2 | **5** | 3 | 2 | **5** |
| **Porcentaje (%)** | 0 | 100 | **100%** | 60 | 40 | **100%** | 60 | 40 | **100%** |

**Elaborado por:** Investigador

**Pregunta 21:** ¿La información disponible es verdadera?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 4 | 8 | **12** | 3 | 2 | **5** | 4 | 1 | **5** |
| **Porcentaje (%)** | 33,33 | 66,67 | **100%** | 60 | 40 | **100%** | 80 | 20 | **100%** |

**Elaborado por:** Investigador

**Pregunta 22:** ¿Se realiza respaldos de los datos?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 8 | 4 | **12** | 4 | 1 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 66,67 | 33,33 | **100%** | 80 | 20 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 23:** ¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 6 | 6 | **12** | 2 | 3 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 50 | 50 | **100%** | 40 | 60 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 24:** ¿Existen zonas restringidas de acceso de personal?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 2 | 3 | **5** | 4 | 1 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 40 | 60 | **100%** | 80 | 20 | **100%** |

**Elaborado por:** Investigador

**Pregunta 25:** ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 1 | 11 | **12** | 2 | 3 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 8,33 | 91,67 | **100%** | 40 | 60 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 26:** ¿Se cuenta con sistemas de alarma como detectores de humo, humedad?

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 6 | 6 | **12** | 3 | 2 | **5** | 5 | 0 | **5** |
| **Porcentaje (%)** | 50 | 50 | **100%** | 60 | 40 | **100%** | 100 | 0 | **100%** |

**Elaborado por:** Investigador

**Pregunta 27:** ¿Existe vigilancia en la entrada del edificio?

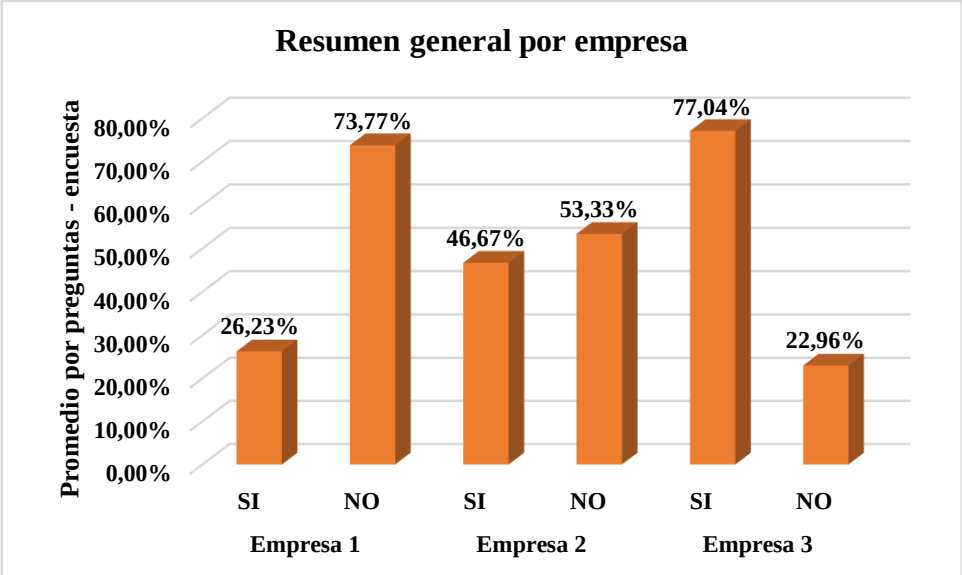
| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Frecuencia** | 2 | 10 | **12** | 1 | 4 | **5** | 1 | 4 | **5** |
| **Porcentaje (%)** | 16,67 | 83,33 | **100%** | 20 | 80 | **100%** | 20 | 80 | **100%** |

**Elaborado por:** Investigador

**Resumen general de la encuesta por empresas**

| | Empresa 1 | | | Empresa 2 | | | Empresa 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** | **SI** | **NO** | **Total** |
| **Pregunta 1** | 41,67% | 58,83% | **100%** | 20% | 80% | **100%** | 100% | 0% | **100%** |
| **Pregunta 2** | 91,67% | 8,33% | **100%** | 100% | 0% | **100%** | 100% | 0% | **100%** |
| **Pregunta 3** | 8,33% | 91,67% | **100%** | 0% | 100% | **100%** | 60% | 40% | **100%** |
| **Pregunta 4** | 41,67% | 58,33% | **100%** | 60% | 40% | **100%** | 60% | 40% | **100%** |
| **Pregunta 5** | 0% | 100% | **100%** | 80% | 20% | **100%** | 100% | 0% | **100%** |
| **Pregunta 6** | 83,33% | 16,67% | **100%** | 100% | 0% | **100%** | 100% | 0% | **100%** |
| **Pregunta 7** | 8,33% | 91,67% | **100%** | 40% | 60% | **100%** | 60% | 40% | **100%** |
| **Pregunta 8** | 0% | 100% | **100%** | 20% | 80% | **100%** | 40% | 60% | **100%** |
| **Pregunta 9** | 0% | 100% | **100%** | 40% | 60% | **100%** | 60% | 40% | **100%** |
| **Pregunta 10** | 0% | 100% | **100%** | 0% | 100% | **100%** | 20% | 80% | **100%** |
| **Pregunta 11** | 8,33% | 91,67% | **100%** | 0% | 100% | **100%** | 60% | 40% | **100%** |
| **Pregunta 12** | 8,33% | 91,67% | **100%** | 60% | 40% | **100%** | 100% | 0% | **100%** |
| **Pregunta 13** | 8,33% | 91,67% | **100%** | 40% | 60% | **100%** | 80% | 20% | **100%** |
| **Pregunta 14** | 58,33% | 41,67% | **100%** | 60% | 40% | **100%** | 80% | 20% | **100%** |
| **Pregunta 15** | 33,33% | 66,67% | **100%** | 20% | 80% | **100%** | 100% | 0% | **100%** |
| **Pregunta 16** | 33,33% | 66,67% | **100%** | 40% | 60% | **100%** | 80% | 20% | **100%** |
| **Pregunta 17** | 41,67% | 58,33% | **100%** | 80% | 20% | **100%** | 100% | 0% | **100%** |
| **Pregunta 18** | 8,33% | 91,67% | **100%** | 40% | 60% | **100%** | 80% | 20% | **100%** |
| **Pregunta 19** | 0% | 100% | **100%** | 60% | 40% | **100%** | 60% | 40% | **100%** |
| **Pregunta 20** | 0% | 100% | **100%** | 60% | 40% | **100%** | 60% | 40% | **100%** |
| **Pregunta 21** | 33,33% | 66,67% | **100%** | 60% | 40% | **100%** | 80% | 20% | **100%** |
| **Pregunta 22** | 66,67% | 33,33% | **100%** | 80% | 20% | **100%** | 100% | 0% | **100%** |
| **Pregunta 23** | 50% | 50% | **100%** | 40% | 60% | **100%** | 100% | 0% | **100%** |
| **Pregunta 24** | 8,33% | 91,67% | **100%** | 40% | 60% | **100%** | 80% | 20% | **100%** |
| **Pregunta 25** | 8,33% | 91,67% | **100%** | 40% | 60% | **100%** | 100% | 0% | **100%** |
| **Pregunta 26** | 50% | 50% | **100%** | 60% | 40% | **100%** | 100% | 0% | **100%** |
| **Pregunta 27** | 16,67% | 83,33% | **100%** | 20% | 80% | **100%** | 20% | 80% | **100%** |
| **PROMEDIO** | 26,23% | 73,77% | **100%** | 46,67% | 53,33% | **100%** | 77,04% | 22,96 | **100%** |

**Elaborado por:** Investigador




**Elaborado por:** Investigador

**Interpretación:**

**Empresa 1:** Con el 73,77% de información procesada, se evidencia que en la empresa 1, existen debilidades en ámbitos de seguridad de la información, siendo las debilidades más importantes: equipos que no reciben mantenimiento periodicamnte, no poseen software legal en su totalidad, no existe normativas formales en materia de seguridad de la información, no existe capacitación en temas de seguridad, no existen controles para navegar en internet, no existe control en el uso del correo electrónico, no se entrega manual de funciones y responsabilidades, la información en los repositorios no se mantiene exacta, no es completa, no se garantiza el almacenamiento de los datos, el acceso oportuno a la información no es oportuno, la actualización de los datos tiene inconveniente al no estar disponible cuando se requiera, no se identifica a los responsables de los cambios y el momento que se realiza, la información no es comprobable, se manifiesta que la información no es verdadera.

Con el 26,33% de la información procesada, se evidencia que en la empresa 1, si cuenta con software antivirus, es necesario que la empresa implante una normativa de seguridad de la información, bajo autorización se accede a la información, se realiza respaldos continuos de los datos.

**Empresa 2:** Con el 53,33 de información procesada, se evidencia que en la empresa 2, existen debilidades en ámbitos de seguridad de la información, siendo las debilidades más importantes: los equipos de desarrollo no reciben mantenimiento periódicamente, no se capacita al personal en temas de seguridad de la información, no existe control para

navegar en internet y para el uso del correo electrónico, el cabio de contraseñas no está sujeto a política alguna, no se entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información, la información en los repositorios no es completa, el acceso oportuno a la información no es garantizado, no se identifica quien realiza los cambios en los datos, cuando ocurren eventos relacionados con la seguridad de la información no hay a quien reportarlo.

Con el 46,67% de la información procesada, se evidencia que en la empresa 2 si cuenta con software antivirus, existen políticas en temas de seguridad de la información, pero es necesario que la empresa invierta en la implantación de una normativa de seguridad, los datos en los repositorios se mantienen exactos, bajo autorización se accede a la información disponible, la información está disponible para ser actualizada, se sabe en qué momento se actualizo la información, es posible comprobar el contenido de la información que se maneja, es verdadera, se respaldan los datos constantemente.

**Empresa 3:** Con el 22,96% de información procesada, se evidencia que en la empresa 2, existen debilidades en ámbitos de seguridad de la información, siendo las debilidades más importantes: no existe control para navegar en internet, no existen políticas para el cambio de contraseñas.

Con el 77,04% de la información procesada, se evidencia que en la empresa 2 los equipos de desarrollo reciben mantenimiento periódicamente, poseen software antivirus, cuenta son software legal, existe normativas y capacitan en temas de seguridad de la información, al personal, existe control en el uso de correo electrónico, se hace entrega de un manual de funciones y responsabilidades en ámbito de seguridad de la información, la información en los repositorios se mantiene exacta, se garantiza el almacenamiento, es completa, la información está disponible solo para accesos autorizados, el acceso a la información es garantizado, disponible para ser actualizada, se conoce quien y en qué momento se cambió la información, además es comprobable, es verdadera, se respalda y en caso de ocurrir eventos relacionados con seguridad de la información se sabe a quién reportarlo.