UNIVERSIDAD TÉCNICA DE MACHALA

FACULTAD DE INGENIERÍA CIVIL

ESCUELA DE INFORMÁTICA

INGENIERÍA EN SISTEMAS



<<< TESIS DE GRADO >>>

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

TÍTULO:

“DESARROLLO E IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001:2005 PARA LA EMPRESA DE SEGURIDAD FÍSICA Y ELECTRÓNICA CISEPRO”

AUTOR:

JUAN CARLOS IDROVO CÁRDENAS.

DIRECTOR:

ING. SIST. VERONICA ZAMBRANO CARRIÒN

MACHALA – EL ORO – ECUADOR

2015

# AGRADECIMIENTO

Durante este tiempo, buenos y malos momentos ayudaron a fortalecer mi perfil como futuro profesional, me brindaron una perspectiva de la vida mucho más amplia y me han enseñado a ser más equilibrado pero sin dejar de lado la responsabilidad que tengo ante la sociedad. Al finalizar mis estudios, existen un grupo de personas a las que no puedo dejar de reconocer debido a que durante todo este tiempo estuvieron presentes de una u otra forma guiando para que culminara mi carrera como profesional de Sistemas y que saliera airoso de esta experiencia tan grata.

En primer lugar agradezco a Dios….porque a pesar de que muchas veces puse mis intereses por encima de ti nunca me faltaste y en ti confío. Siempre me ha ayudado a seguir adelante y por ti aún no pierdo la esperanza, sé que todos pueden decepcionarme menos tú y reconozco que sin ti no hubiese podido sobrevivir estos últimos meses. Muchas Gracias.

A mi familia ya que fueron los precursores directos de mi formación académica y que nunca dejaron de confiar en mí, a mi esposa Lía Cecibel Salinas Pineda que estuvo apoyando incondicionalmente y la compañía de nuestra hija Paula Valentina Idrovo Salinas.

A todos el personal del Departamento de Sistemas de la Empresa CISEPRO que supieron respetar y apreciar la tarea que realizaba, donde demostraron su interesa y su atención para que se lleve a cabo este proyecto; Muy preciado hago extenso mi gratitud a la Ing. Sist. Verónica Zambrano Carrión mi directora de tesis, por su paciencia, y valiosa enseñanza compartir sus conocimientos que me ayudaron a esclarecer ciertas dudas y orientarme durante el desarrollo de este proyecto de tesis y finalmente un agradecimiento eterno a la Universidad Técnica de Machala la cual me abrió sus puertas, permitiéndonos poder cumplir la tarea de prepararnos y formarnos de manera eficiente para un futuro competitivo.

¡GRACIAS A TODOS USTEDES!

Egdo. Sist. Juan Carlos Idrovo Cárdenas

# DEDICATORIA

El presente trabajo quiero dedicarle en especial a Dios que me dio la vida y fortaleza necesaria para culminar este proceso, necesario en el desarrollo profesional, además de eso quiero agradecer a mis padres que están siempre ahí cuando más los necesité, con el afán de compartir su conocimiento y experiencias.

# CERTIFICACIÓN.

Ing. Sist. VERONICA ZAMBRANO CARRIÓN., director de la tesis ““DESARROLLO E IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001:2005 PARA LA EMPRESA DE SEGURIDAD FÍSICA Y ELECTRÓNICA CISEPRO” de la autoría del señor egresado de la carrera de Ingeniería de Sistemas JUAN CARLOS IDROVO CÁRDENAS, de la Escuela de Informática, certifico haber revisado el presente trabajo académico, el mismo que cumple con los parámetros establecidos con la institución; en tal virtud autorizo su presentación para el trámite correspondiente.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ING. SIST. VERONICA ZAMBRANO CARRIÓN.

DIRECTORA DE LA TESIS

# SÍNTESIS

.

Pendiente

# SYNTHESIS

Pendiente

# ÍNDICE GENERAL

[AGRADECIMIENTO II](#_Toc404067399)

[DEDICATORIA III](#_Toc404067400)

[CERTIFICACIÓN. IV](#_Toc404067401)

[SÍNTESIS V](#_Toc404067402)

[SYNTHESIS VI](#_Toc404067403)

[ÍNDICE GENERAL VII](#_Toc404067404)

[ÍNDICE FIGURAS XIII](#_Toc404067405)

[ÍNDICE TABLAS XIV](#_Toc404067406)

[INTRODUCCIÓN 15](#_Toc404067407)

[Descripción de campo de Investigación. 15](#_Toc404067408)

[Objetivos. 15](#_Toc404067409)

[Objetivo General. 15](#_Toc404067410)

[Objetivo Específicos. 16](#_Toc404067411)

[Hipótesis. 16](#_Toc404067412)

[Hipótesis Principal. 16](#_Toc404067413)

[Hipótesis Específicas. 16](#_Toc404067414)

[CAPÍTULO I 17](#_Toc404067415)

[1 Marco Referencial. 17](#_Toc404067416)

[1.1 Justificación. 17](#_Toc404067417)

[1.2 Problema. 19](#_Toc404067418)

[1.2.1 Planteamiento Del Problema. 19](#_Toc404067419)

[1.2.1.1 Problema Central. 19](#_Toc404067420)

[1.2.1.2 Problemas Particulares. 19](#_Toc404067421)

[1.3 Preguntas Científicas. 19](#_Toc404067422)

[1.3.1 Pregunta Central. 20](#_Toc404067423)

[1.3.2 Preguntas Particulares. 20](#_Toc404067424)

[1.4 Alcance. 20](#_Toc404067425)

[CAPÍTULO 2 22](#_Toc404067426)

[2 Marco Teórico. 22](#_Toc404067427)

[2.1 Antecedentes de la Empresa 22](#_Toc404067428)

[2.1.1 Información Institucional. 22](#_Toc404067429)

[2.1.2 Misión. 22](#_Toc404067430)

[2.1.3 Visión. 22](#_Toc404067431)

[2.1.4 Actividad de la Empresa 22](#_Toc404067432)

[2.1.5 Política Integrada de Calidad, Seguridad, Salud y Medio Ambiente. 24](#_Toc404067433)

[2.1.6 Ubicación. 25](#_Toc404067434)

[2.1.7 Estructura Organizacional. 28](#_Toc404067435)

[2.1.8 Directorio. 29](#_Toc404067436)

[2.1.9 Gerencia Administrativo-Financiera. 29](#_Toc404067437)

[2.1.10 Gerencia de Operaciones. 29](#_Toc404067438)

[2.1.11 Gerencia de Recursos Humanos. 29](#_Toc404067439)

[2.1.12 Gerencia de Compras. 30](#_Toc404067440)

[2.1.13 Gerencia de Sistemas Informáticos. 30](#_Toc404067441)

[2.1.14 Seguridad Electrónica. 30](#_Toc404067442)

[2.1.15 Arquitectura de Red. 31](#_Toc404067443)

[2.2 Antecedentes Conceptuales. 32](#_Toc404067444)

[2.2.1 Información 32](#_Toc404067445)

[2.2.1.1 Principales Características de la información. 32](#_Toc404067446)

[2.2.1.1.1 Significado. 32](#_Toc404067447)

[2.2.1.1.2 Importancia. 32](#_Toc404067448)

[2.2.1.1.3 Vigencia. 32](#_Toc404067449)

[2.2.1.1.4 Validez. 32](#_Toc404067450)

[2.2.1.1.5 Valor. 32](#_Toc404067451)

[2.2.2 Activos de Información. 33](#_Toc404067452)

[2.2.2.1 Clasificación de los Activos de la Información. 33](#_Toc404067453)

[2.2.3. Estándares. 35](#_Toc404067454)

[2.2.3.1 ISO (Organización Internacional para la Estandarización). 35](#_Toc404067455)

[2.2.3.2 BSI (Instituto de Estandarización Británico). 35](#_Toc404067456)

[2.2.3.3 Principales Estándares de Seguridad Informática. 36](#_Toc404067457)

[2.2.3.3.1 ISO 17799. 36](#_Toc404067458)

[2.2.3.3.2 ISO 27001. 37](#_Toc404067459)

[2.2.3.3.3 ISO 27002. 39](#_Toc404067460)

[2.2.4 Seguridad Informática. 42](#_Toc404067461)

[2.2.4.1 Importancia de la Seguridad Informática. 42](#_Toc404067462)

[2.2.4.2 Variables de la Seguridad Informática. 43](#_Toc404067463)

[2.2.4.3 Requerimientos de Seguridad Informática. 44](#_Toc404067464)

[2.2.4.4 Delitos informáticos. 44](#_Toc404067465)

[2.2.4.4.1 Hackers. 45](#_Toc404067466)

[2.2.4.4.2 Crackers. 45](#_Toc404067467)

[2.2.4.4.2.1 Lammer. 46](#_Toc404067468)

[2.2.4.4.2.2 Trasher. 46](#_Toc404067469)

[2.2.4.4.2.3 Insiders. 46](#_Toc404067470)

[2.2.4.4.5 Virus Informático. 46](#_Toc404067471)

[2.2.4.4.5.2 Métodos de propagación. 49](#_Toc404067472)

[2.2.4.4.5.3 Métodos de Protección. 49](#_Toc404067473)

[2.2.4.4.6 Sabotaje Informático. 49](#_Toc404067474)

[2.2.4.4.7 Fraude Informático. 50](#_Toc404067475)

[2.2.4.4.8 Estafas Electrónicas o Phishing. 50](#_Toc404067476)

[2.2.4.4.9 Espionaje Informático o Sniffing. 50](#_Toc404067477)

[2.2.4.4.10 Infracción a los Derechos del Autor. 50](#_Toc404067478)

[2.2.4.4.11 Infracción del Copyright de Base de Datos. 50](#_Toc404067479)

[2.2.4.4.12 Uso Ilegitimo de Sistemas Informáticos Ajenos: 51](#_Toc404067480)

[2.2.4.4.13 Accesos No Autorizados. 51](#_Toc404067481)

[2.2.4.4.14 interceptación de E-Mails. 51](#_Toc404067482)

[2.2.5 Elementos de Seguridad. 52](#_Toc404067483)

[2.2.5.1 Principios de Seguridad. 52](#_Toc404067484)

[2.2.5.2 La Gestión del Riesgo. 52](#_Toc404067485)

[2.2.5.3 Compromiso. 52](#_Toc404067486)

[2.2.5.4 Funciones y Responsabilidades. 52](#_Toc404067487)

[2.2.5.5 Objetivos, Estrategias y Políticas. 52](#_Toc404067488)

[2.2.5.6 Activos. 52](#_Toc404067489)

[2.2.5.7 Bienes. 52](#_Toc404067490)

[2.2.5.8 Amenazas. 53](#_Toc404067491)

[2.2.5.9 Vulnerabilidad. 53](#_Toc404067492)

[2.2.5.10 Impacto. 54](#_Toc404067493)

[2.2.5.11 Riesgo. 55](#_Toc404067494)

[2.2.5.12 Seguridades. 56](#_Toc404067495)

[2.2.5.13 Limitaciones. 57](#_Toc404067496)

[2.2.6 Aspectos Organizativos de la Seguridad Informática. 57](#_Toc404067497)

[2.2.6.1 Principios Fundamentales de la Seguridad de la Información. 58](#_Toc404067498)

[2.2.6.1.1 Confidencialidad. 58](#_Toc404067499)

[2.2.6.1.2 Integridad. 58](#_Toc404067500)

[2.2.6.1.3 Disponibilidad. 58](#_Toc404067501)

[2.2.7 Gestión de la Seguridad Informática. 59](#_Toc404067502)

[2.2.7.1 Sistema de Gestión de Seguridad de la Información (SGSI). 59](#_Toc404067503)

[2.2.7.2 Mejora Continua (Ciclo Deming). 60](#_Toc404067504)

[2.2.7.2.1 Planificar (Plan - Establecer una planificación) 61](#_Toc404067505)

[2.2.7.2.2 Hacer (Do - Implementar y Utilizar el SGSI). 62](#_Toc404067506)

[2.2.7.2.3 Chequear (Check - Monitorizar y Revisar). 63](#_Toc404067507)

[2.2.7.2.4 Actuar (Act - Mantener y Mejorar). 64](#_Toc404067508)

[2.2.8 Análisis Estratégico del Riesgo. 64](#_Toc404067509)

[2.2.8.1 Identificar los riesgos 65](#_Toc404067510)

[2.2.8.2 Analizar y evaluar los riesgos. 65](#_Toc404067511)

[2.2.8.3 Identificar y Evaluar las Distintas Opciones de Tratamiento de los Riesgos 66](#_Toc404067512)

[2.2.9 Plan de Seguridad informática 67](#_Toc404067513)

[2.2.10 Implementación de Seguridades. 68](#_Toc404067514)

[2.2.10.1 Políticas de Seguridad (Cláusula 5). 68](#_Toc404067515)

[2.2.10.2 Aspectos Organizativos de la Seguridad de la Información. (Cláusula 6). 69](#_Toc404067516)

[2.2.10.3 Gestión de Activos. (Cláusula 7). 70](#_Toc404067517)

[2.2.10.4 Seguridad Ligada a los Recursos Humanos. (Cláusula 8). 70](#_Toc404067518)

[2.2.10.5 Seguridad Física y del Entorno. (Cláusula 9). 71](#_Toc404067519)

[2.2.10.6 Gestión de Comunicación y Operaciones. (Cláusula 10). 72](#_Toc404067520)

[2.2.10.7 Control de Acceso. (Cláusula 11). 74](#_Toc404067521)

[2.2.10.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. (Cláusula 12). 76](#_Toc404067522)

[2.2.10.9 Gestión de Incidentes en la Seguridad de la Información. (Cláusula 13). 77](#_Toc404067523)

[2.2.10.10 Gestión de la Continuidad del Negocio. (Cláusula 14). 78](#_Toc404067524)

[2.2.10.11 Cumplimiento. (Cláusula 15). 79](#_Toc404067525)

[CAPÍTULO 3 80](#_Toc404067526)

[3. Desarrollo de la Propuesta. 80](#_Toc404067527)

[3.1 Implementación de la Norma ISO 27001:2005. 80](#_Toc404067528)

[3.1.1 Desarrollo de Políticas de Seguridad de la Información. 80](#_Toc404067529)

[CAPÍTULO 4 81](#_Toc404067530)

[CONCLUSIONES 82](#_Toc404067531)

[RECOMENDACIONES 83](#_Toc404067532)

[BIBLIGRAFÍA 84](#_Toc404067533)

[GLOSARIO 85](#_Toc404067534)

[ANEXOS 86](#_Toc404067535)

[Anexo 1: Formatos o Modelos de Encuestas para Estableces Políticas de Seguridad Informática. 86](#_Toc404067536)

[Encuesta 1. 86](#_Toc404067537)

[Encuesta 2. 87](#_Toc404067538)

[Encuesta 3. 88](#_Toc404067539)

[Encuesta 4. 89](#_Toc404067540)

# ÍNDICE FIGURAS

[Figura 2.1: Matriz Oficina en Machala. 24](#_Toc403988502)

[Figura 2.2: Oficina en Guayaquil. 24](#_Toc403988503)

[Figura 2.3: Oficina en Zamora. 25](#_Toc403988504)

[Figura 2.4: Oficina en Loja. 25](#_Toc403988505)

[Figura 2.5: Oficina en Cuenca. 26](#_Toc403988506)

[Figura 2.6: Organigrama Funcional 27](#_Toc403988507)

[Figura 2.7: Estándar ISO 17799. 36](#_Toc403988508)

[Figura 2.8. Estándar ISO 27002 38](#_Toc403988509)

[Figura 2.9. Estándar ISO 27002 39](#_Toc403988510)

[Figura 2.10: Ejemplo de vulnerabilidad, una contraseña de usuario. 53](#_Toc403988511)

[Figura 2.11: Ejemplo de Riesgo, La probabilidad de la suplantación por robo de contraseñas. 54](#_Toc403988512)

[Figura 2.12: Principios Fundamentales de la Seguridad de la Información. 58](#_Toc403988513)

[Figura 2.13: Ciclo de vida de la Información 59](#_Toc403988514)

[Figura 2.14: Ciclo de Deming 60](#_Toc403988515)

[Figura 2.15: Gestión del Riesgo 65](#_Toc403988516)

# ÍNDICE TABLAS

[Tabla 2.1: Clasificación de los Activos de la Información 32](#_Toc403754578)

# INTRODUCCIÓN

## Descripción de campo de Investigación.

La Empresa CISEPRO Cia. Ltda. En la provincia de El Oro se ha ido posesionando notablemente en Actividades relacionadas a la Seguridad; abarcando un extenso mercado que le ha permitido asentarse en las demás provincias del Ecuador, aunque el concepto seguridad sea un poco susceptible de alcanzar; esta se ha especializado holísticamente basados en la experiencia adquirida hasta la actualidad, su política interna establecida en estándares, ha aportado su solidez y prestigio. Su principal columna vertebral para las operaciones es su matriz ubicada en la ciudad de Machala desde donde se desarrollan el ejercicio de sus actividades abarcadas en tres ejes principales: Seguridad Física, Seguridad Electrónica, Video – Vigilancia. El desempeño, la ejecución de estos procesos está ligado a la mejora continua y estándares de calidad; en consecuencia existe un denominador común la información.

La información es una variable muy susceptible y vital para la vida de una Empresa dependiendo de su empleo, manipulación permite la proyección o la desestabilización en las actividades de la seguridad, entonces es importante su resguardo; a nivel mundial la información se la protege empleando modelos de seguridad comprobados que permiten mitigar la vulnerabilidad de esta ante los riesgo informáticos, dentro los cuales se destaca los estándares para la administración de la seguridad informática.

El campo de investigación está delimitado en la matriz y es el eje principal de aplicación para la administración de la seguridad, creyendo conveniente emplear el estándar ISO 27001:2005 siguiendo con las normativas vigentes como un modelo a seguir para amenorar la vulnerabilidad de la información a riesgos informáticos; acorde con las políticas CISEPRO.

## Objetivos.

### Objetivo General.

* Diseñar e implementar un plan de seguridad informática basado en la norma ISO 27001:2005 para reducir los riesgos informáticos para evitar la pérdida de información confidencial en la empresa de Seguridad Física y Electrónica CISEPRO.

### Objetivo Específicos.

* Identificar los procesos internos en la Matriz de la Empresa, partiendo del organigrama funcional para establecer la situación actual de la seguridad informática, comunicaciones, bienes informáticos entre otros que permita establecer políticas de seguridad, soporte y gestión continua.
* Determinar el alcance del plan de seguridad informática en la Matriz de la Empresa CISEPRO situada en la ciudad de Machala.
* Analizar las vulnerabilidades para establecer el impacto, efecto e incidencia.
* Evaluar los riesgos informáticos para determinar parámetros de seguridad.
* Crear e implementar controles de acceso de usuario, red, sistemas operativos, aplicaciones informáticas, informaciones, y conexión móvil que mejore el funcionamiento de los procedimientos para prevenir incidentes informáticos.

## Hipótesis.

### Hipótesis Principal.

La implementación de un plan de seguridad informática basada en un estándar ISO 27001:2005 mitigara los riesgos informáticos considerablemente permitiendo tener un control del acceso los activos de la información garantizando la integridad, confiabilidad y disponibilidad.

### Hipótesis Específicas.

* Se identificaran las actividades de cada uno de los procesos de la organización en cada uno de los departamentos para encontrar vulnerabilidades.
* Se determinaran el ámbito de aplicación del plan de seguridad informática, responsabilidades, controles y contingentes
* Se analizaran las amenazas que puedan afectar el negocio de la empresa por tipo de activo de información para comprobar la posibilidad de que se efectúen calculando el nivel del riesgo.
* Evaluando los riesgos informáticos se consigue reducir la probabilidad de materialización de las amenazas, daños potenciales en los sistemas de información consiguiendo que no se den situaciones que permitan producirlas.
* Creando controles, procedimientos de control de cambios que permite establecer un orden, una estructura, una planificación para el tratamiento de la información y su incidencia se mejora la eficacia su gestión.

# CAPÍTULO I

## 1 Marco Referencial.

### 1.1 Justificación.

Hoy por hoy en el Ecuador existe una competencia tecnológica activa entre las diferentes Empresas de Seguridad Física y Electrónica; y como estas poseen una gran variedad de recursos se ven vulnerables y susceptibles a riesgos como el suscitado en el año 2008 al gobierno de nuestro país realizada por la agrupación “anonymous” que se infiltro y colapso el sitio web de la presidencia “www.presidencia.gov.ec” según fuente oficial. Estas acciones desencadenaron que las organizaciones tomen la obligación de protegerse ante los ataques informáticos.

Aunque un porcentaje muy magno de las Empresas en el Ecuador no le dan la debida importancia al tema de seguridad informática por lo que están propensos y expuestos a la probabilidad que se produzcan eventos que alteran el proceso de sus sistemas internos; tales como perdida y fuga de información, confidencial, activos alterados entre otros que desestabiliza el funcionar de las mismas.

En consecuencia la Empresa CISEPRO asume la necesidad de impedir que se susciten estas infiltraciones, debido a estos factores y al volumen de información que se maneja en sus diferentes procesos internos dentro de la organización estructural de la empresa infirieron en la decisión de gestionar un sistema para la seguridad informática

Cabe mencionar que esta empresa al tener implementado un sistema de gestión de calidad (Norma ISO 9001) los procesos son rápidos y eficientes, pero el acceso a la información está expuesto irrupciones, como la información esta considera como el activo de mayor valor dentro del crecimiento Económico de la empresa es necesario priorizar su protección con un plan de seguridad.

Otro factor importante es que desde la aparición del Internet y su empleo masivo por parte de las organizaciones, ha permitido que estas intercambien información en todo momento referente a sus clientes, proveedores, entre otros para la libre competencia. Es entonces que surge la necesidad y la importancia conocer cuáles son los recursos que necesitan la protección, el control, la prevención ante el acceso a los mismos dentro de un sistema de información.

Es fundamental o de vital importancia que los usuarios en un sistema de información empleen permisos para el acceso a estos; basados en procedimientos que permitan asegurar y proteger el medio. Además debido a la tendencia sedentaria que existe en el desempeño del Talento Humano de la Empresa conectados a los sistemas de información durante toda la jornada de trabajo y aunque existan convenios de confidencialidad dentro de la organización estipulados como normativa por parte de los empleados para que no saquen o lleven consigo información fuera de las instalaciones de la Matriz, se dan todavía pérdidas de información y no se ha logrado garantizar la confidencialidad en los activos de la información.

Es conveniente un Sistema de gestión de Seguridad de Información debido a que la información es un activo único que puede impulsar o destruir a la Empresa, si esta gestión se la realiza de una forma adecuada, le permite trabajar con confianza y la libertad de crecer, innovar y ampliar su base de clientes sabiendo que toda su información confidencial seguirá siéndolo.

Con la finalidad de optimizar la seguridad de la información, basado en los hechos anteriores mencionados en la Empresa de Seguridad Física y Electrónica CISEPRO CIA LTDA, el Departamento de Sistemas ha creído conveniente el desarrollo de la siguiente tema: “DESARROLLO E IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001:2005 PARA LA EMPRESA DE SEGURIDAD FÍSICA Y ELECTRÓNICA CISEPRO” que justifica efectuar el proyecto de investigación.

### 1.2 Problema.

#### 1.2.1 Planteamiento Del Problema.

Actualmente la Empresa CISEPRO Cía. Ltda., cuenta con cinco oficinas a nivel de las Provincias de El Oro, Guayas, Loja, Zamora y Morona Santiago, su matriz se encuentra ubicada en el Cantón Machala, Ciudadela El Bosque Sector 5, en la vía Alejandro Castro Benítez; la actividad comercial que presta a la comunidad es el Servicio de Seguridad Física, Electrónica y Video-Vigilancia.

CISEPRO tiene implementado Sistemas de Gestión de Calidad, Medio ambiente, Salud y Seguridad Ocupacional, Sistema de Gestión en Control y Seguridad BASC en base a las normas ISO 9001:2008, ISO 14001:2004, OHSAS 18001, BASC VERSION 3:2008 respectivamente, el empleo de estos estándares ha permitido que gran parte de sus procesos tengan un desempeño eficiente y eficaz basado en la política de la mejora continua certificada por Bureau Veritas organismo internacional auditor de estas normas.

En base a la experiencia y a la aplicación de estas Normativas, los resultados que se ha logrado en un mediano plazo de tiempo, emerge la necesidad de desarrollar un plan para la implementación de la normativa ISO 27001:2005 que permita garantizar la seguridad de los activos de la información en apoyo al desarrollo de la empresa e integración del Ingeniero de Sistemas en su proceso de profesionalidad, por estas razones válidas se planteó el desarrollo de este tema de exploración conforme a las líneas de investigación de la UTMACH, la Unidad Académica de Ingeniería Civil y la Escuela de Informática.

##### 1.2.1.1 Problema Central.

La Empresa se Seguridad Física y Electrónica CISEPRO CIA LTDA no cuenta implementado un Sistema de Seguridad Informática que permita mitigar los riesgos y garantizar la confidencialidad de la Información.

##### 1.2.1.2 Problemas Particulares.

### 1.3 Preguntas Científicas.

* Inexistencia de políticas, guías y procedimientos relacionados con la seguridad de la información para la concertar los servicios tecnológicos.
* Carencia de un plan de seguridad informática lo que ocasiona perdida de información confidencial, ya sea por causas fortuita o planeada.
* Desconocimiento de las amenazas y vulnerabilidades en los activos de la información susceptibles a riesgos convencionales y no convencionales.
* Inexistencia de una matriz de riesgos informáticos y su impacto.
* Carencia de controles efectivos de acceso para usuario de red, sistemas operativos, aplicaciones informáticas, informaciones, conexión móvil entre otros.

#### 1.3.1 Pregunta Central.

¿Con la implementación del plan de seguridad informática se logrará mitigar los riesgos informáticos y la disminuir la probabilidad de su incidencia?

#### 1.3.2 Preguntas Particulares.

* ¿Facilitará el desarrollo del plan de seguridad informática usando un estándar ISO 27001:2005 y su gestión?
* ¿La implementación de un plan de seguridad informática logrará disminuir el impacto de los riesgos informáticos?
* ¿Con los medios existentes se conseguirá aplicar el plan de seguridad informática en la matriz de la Empresa y establecerla como una política?
* ¿Los controles de acceso a los sistemas bastará para dar seguridad a la información que se maneja?
* ¿Se conseguirá la integridad en el acceso a datos?
* ¿Se logrará seguridad y confidencialidad de la información?

### 1.4 Alcance.

Para la implementación del plan de seguridad informática se ha elegido como metodología la normativa ISO 27001 revisión 2005 aunque existen otras versiones esta es la que se certifica a nivel internacional, que provee un modelo para la creación, operación, revisión, mantenimiento y mejora continua de un Sistema de gestión de seguridad informática. El campo de aplicación del modelo abarca la matriz de la Empresa la cual es el principal de todas las operaciones y este contendrá los siguientes dominios ligados respectivamente a un número de objetivos de control establecidos por la norma.

Política de Seguridad que permita proporcionar dirección general y soporte a la seguridad (1 objetivo de control).

Organización Interna que permita manejar la seguridad de la información (2 objetivos de control).

Gestión de los Activos de la información (2 objetivos de control).

Seguridad ligada al Talento Humano (3 objetivos de control).

Seguridad Física y del entorno (2 objetivos de control).

Gestión de las comunicaciones y operaciones (10 objetivos de control).

Control de Acceso (7 objetivos de control).

Adquisición desarrollo y mantenimiento de los sistemas de información. (6 objetivos de control)

Gestión de incidentes en la seguridad de la información (2 objetivos de control).

Gestión de la continuidad del negocio. (1 objetivo de control)

Cumplimiento (3 objetivos de control).

# CAPÍTULO 2

## 2 Marco Teórico.

### 2.1 Antecedentes de la Empresa

#### 2.1.1 Información Institucional.

CISEPRO Cia. Ltda. Es una empresa de Seguridad Física, Electrónica y video vigilancia que se fundó el 23 de Mayo de 1991 en tendencia a una respuesta mundial de protección privada a: personas, bienes e información en el Ecuador uno de los países de mayor riesgo en el incremento organizado de la delincuencia. A partir del año 2008 su diseño implantó una administración técnica y moderna de mejoramiento continuo, en donde todo el personal participa activamente en base a las necesidades del cliente y su satisfacción.

#### 2.1.2 Misión.

Servicio al Cliente basado en el talento humano velando por su seguridad y salud, procesos de calidad y tecnología de punta mejorando constantemente.

#### 2.1.3 Visión.

Ser un grupo empresarial de Seguridad y negocios a fines con mejoramiento continuo.

#### 2.1.4 Actividad de la Empresa

La actividad económica de la empresa se basa en la prestación del servicio de seguridad dividida en dos categorías.

* ***Seguridad Física:*** Basado en al talento humano entrenado disponible que se encuentra en condiciones de proveer un servicio de vigilancia de calidad, apoyados en procedimiento legales para reforzar la seguridad de las instalaciones en las cuales se ofrece este servicio; permitiendo de esta manera asistir directamente al cliente y prevenir las pérdidas derivadas de robos y daños, generados en los espacios protegidos. Consiguiendo promover ambientes más seguros para un desempeño exitoso. Esto vigilantes a su se encuentran controlados por supervisores encargados de verificar el cumplimiento operativo de los procedimientos que rigen la vigilancia física que complementa el servicio con una central de monitoreo que laboran las 24 horas del día. El talento humano que conforma la nómina de la empresa pasa por un programa de selección y entrenamiento de acuerdo a estándares internacionales.
* ***Seguridad Electrónica:*** Esta se encuentra dividida en los siguientes grupos de servicios.
* ***Cercos Eléctricos:*** Conformado por una barrera de cables finos desnudos instalados sobre postes aislados, los cuales forman una protección perimetral inteligente, sensible y agresiva, a alturas variables que repele la incursión de intrusos de una manera segura lo suficientemente dolorosa para evitar la intrusión.
* **Controles de Acceso:**mecanismo que en función de la identificación ya autentificada permite acceder a un espacio, básicamente un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, etiqueta de proximidad o biometría) y a su vez controlando el recurso (puerta, torniquete o talanquera) por medio de un dispositivo electrónico.
* **Sistemas contra incendio:** conjunto de redes de medios electrónicos pasivos que permiten la detección de humo para la prevención de un incendio en lugares vulnerables o susceptibles al fuego.
* ***Circuitos cerrados de Televisión:*** Tecnología de video empleada para supervisar circuitos compuesto por una o más cámaras de vigilancia conectadas a uno o más monitores de vídeo o televisores, que reproducen las imágenes capturadas por las cámaras en una diversidad de ambientes y actividades.
* ***Sistemas de Alarmas:*** Tecnología de seguridad pasiva montada a partir de dispositivos de alerta instalados permanentemente o autónomos que son capaces de advertir una situación anormal frente a posibles problemas en tiempo real; capaces de reducir el tiempo de ejecución de acciones a tomar en función del problema suscitado, reduciendo las perdidas.
* ***Sistemas de Video Vigilancia:*** Tecnología de vigilancia visual que combina los beneficios analógicos de los CCTV[[1]](#footnote-1) con las ventajas digitales de las redes de comunicación, permitiendo la supervisión local y/o remota de imágenes y audio así como el tratamiento digital de las imágenes, para aplicaciones como el reconocimiento de matrículas o reconocimiento facial entre otras dada su versatilidad, funcionalidad, sencillez y optimización de las infraestructuras con la supervisión de un sistema de monitoreo.
* ***Sistemas de Monitoreo:*** Consiste en una instalación dotada de una serie de equipos informáticos y talento humano que permiten el monitoreo de las señales generadas por los dispositivos electrónicos montados ya sea en un sistema de alarma, incendio, circuitos cerrados de televisión, entre otros

#### 2.1.5 Política Integrada de Calidad, Seguridad, Salud y Medio Ambiente.

“CISEPRO es una empresa de Servicios de Vigilancia, Seguridad Física y Electrónica, que trabaja con altos estándares de calidad y seguridad, mejorando continuamente sus procesos para satisfacer las exigencias de sus clientes.

Controla además permanentemente las instalaciones, previniendo el uso de drogas, alcohol y lavado de activos. La organización tiene el compromiso de mejorar el ambiente de trabajo y prevenir los riesgos para sus colaboradores, visitantes, contratistas, subcontratistas y además controla los impactos ambientales generales en su actividad, siempre apegados a la legislación ecuatoriana y otras aplicables.

CISEPRO declara al talento humano como el valor más importante de la empresa, cumpliendo el compromiso de trabajar mejorando continuamente sus sistemas de calidad, seguridad y salud ocupacional, para satisfacer las necesidades del cliente y la prevención de la salud del trabajador. Obligación de proteger la seguridad y salud de los trabajadores, con su participación en los órganos de representación.

Adopta la Filosofía de mejora continua, cuya acción preventiva se basa en el cumplimiento de procesos, normas y requisitos legales aplicables a la seguridad y salud en el trabajo con su mejora permanente. La línea jerárquica es la responsable de la prevención de los accidentes considerada tan importante como la calidad o productividad. El plan de prevención se concreta con los programas de acción a ser conocido por todas las personas y su participación permanente.”[[2]](#footnote-2)

#### 2.1.6 Ubicación.

La empresa cuenta con oficinas a nivel de las Provincias de El Oro, Guayas, Loja Zamora y Morona Santiago su matriz se encuentra ubica en la Ciudad de Machala.

**Sucursal**: Matriz, **Provincia**: El Oro, **Ciudad**: Machala, **Dirección**: Avenida Alejandro Castro Benítez junto al bosque sector 5, **Teléfono:** 072790424-072790364.



Figura 2.1: Matriz Oficina en Machala.[[3]](#footnote-3)

**Sucursal**: Guayas, **Provincia**: Guayas, **Ciudad**: Guayaquil, **Dirección**: Portete y chile esquina, **Teléfono:** 097687941-086895489.



Figura 2.2: Oficina en Guayaquil.[[4]](#footnote-4)

**Sucursal**: Zamora, **Provincia**: Zamora Chinchipe, **Ciudad**: Zamora, **Dirección:** Barrio la Chacra y Avenida del Ejército, **Teléfono:** 072315060.



Figura 2.3: Oficina en Zamora.[[5]](#footnote-5)

**Sucursal**: Loja, **Provincia**: Loja, **Ciudad**: Loja, **Dirección:** Sector La Banda, ciudadela del chofer Avenida Tacsiche y José Zaen, **Teléfono:** 072542080.

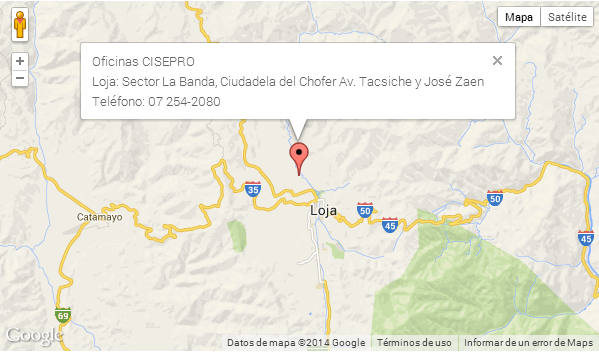


Figura 2.4: Oficina en Loja.[[6]](#footnote-6)

**Sucursal**: Azuay, **Provincia**: Azuay, **Ciudad**: Cuenca, **Dirección:** La Castellana y Sevilla, **Teléfono:** 072802297.

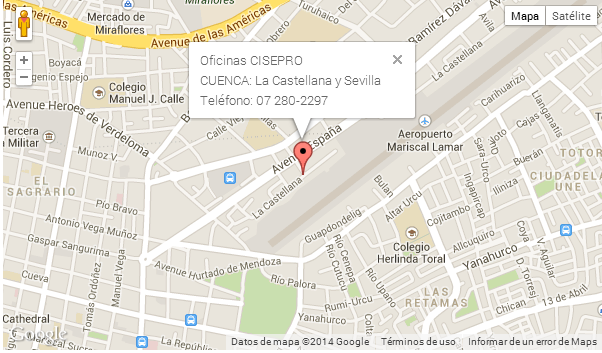


Figura 2.5: Oficina en Cuenca.*[[7]](#footnote-7)*

#### **2.1.7 Estructura Organizacional.**

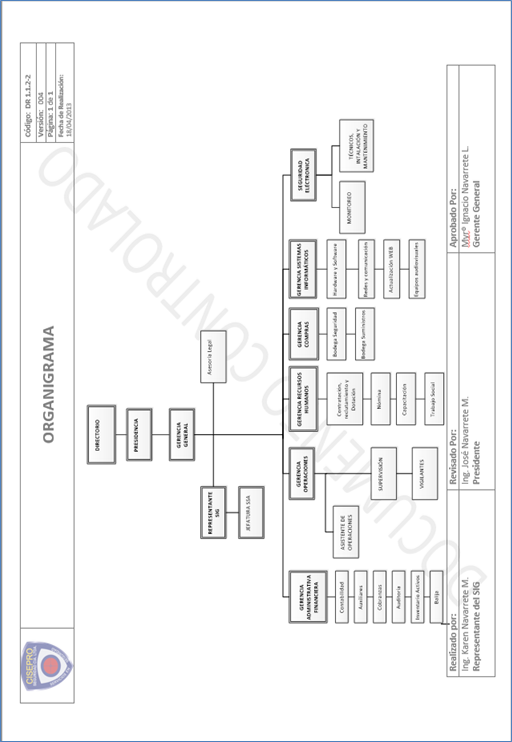


Figura 2.6: Organigrama Funcional[[8]](#footnote-8)

### 2.1.8 Directorio.

Conformado por la Presidencia gobernada por la Sra. Belén Armijos de Navarrete, Gerencia General por el Mayor (R) José Ignacio Navarrete Landázuri, incluyendo sub-gobiernos los cuales son: Representante del SIG[[9]](#footnote-9) presidido por la Ing. Karen Viviana Navarrete Madero, La Jefatura de SSA[[10]](#footnote-10) presidida por el Ing. José Ignacio Navarrete Madero y un Asesor Legal regido por el Dr. Vinicio Pasos.

#### 2.1.9 Gerencia Administrativo-Financiera.

Esta gerencia la gobierna el Ing. José Ignacio Navarrete Madero, el cual es el encargado de planificar, administrar, verificar todas las actividades administrativas de la empresa además es el encargado de dirigir a:

* **Contabilidad.-** Conformado por un contador.
* **Auxiliares.-** Conformado por dos auxiliares contable; el primero encargado de la facturación, fondos y Retenciones; el segundo administra cajas y compras.
* **Cobranzas.-** Conformado por una Tesorera encargada de la Cartera, bancos pagos entre otros y un cobrador.
* **Auditoria.-** Conformado por un Auditor Interno del SIG.
* **Inventario de Activos.-** Administrado por el encargado del Módulo de Activos Fijos.
* **Valija.-** Designado a un auxiliar de servicios.

#### 2.1.10 Gerencia de Operaciones.

Encargada de toda la logística operacional del personal de seguridad física, además de la asignación de puntos estratégicos y supervisión general, este departamento lo gobierna Economista Pedro Medrano, para su apoyo consta además de un auxiliar de operaciones.

#### 2.1.11 Gerencia de Recursos Humanos.

Este departamento coordina con gerencia de operaciones el proceso de contratación del talento humano y todo lo relacionado con la actividad del mismo desde su ingreso a la empresa hasta la culminación de su contrato laboral, internamente está conformado por:

* **Registro de Talento Humano.-** Encargado del Registro, carnetización y administración de carpetas del talento humano.
* **Roles y Horas Extra.-** Encargado de la elaboración de los roles y administración de bitácoras de supervisión.
* **Seguridad Social y seguro de vida.-** Encargado de los Pagos de la Seguridad Social y beneficio de seguro de vida personal para el empleado.
* Trabajadora Social.- Encargado de la logística social y seguimiento del personal.
* **Obligaciones legales y contratos laborales.-** Encargado de realizar contratos del personal y actas de finiquito.

#### 2.1.12 Gerencia de Compras.

Designado para la administración de las bodegas y compras de suministros en general es decir el encargado de proveer a todos los departamentos.

#### 2.1.13 Gerencia de Sistemas Informáticos.

La gerencia de Sistemas Informáticos está encargada de administrar y desarrollar Software para mejorar los procesos internos de los diferentes departamentos, este departamento está conformado por:

* **Jefe de Sistemas.-** Encardo de Administrar el desarrollo de los Sistemas Informáticos y dirigir el personal de Sistemas.
* **Analista de Sistemas I y II.-** Encargados de diseñar, desarrollar, implementar y capacitar los módulos de software a todo el talento humano que lo emplee; además de eso están encargados de la administración de los servidores y demás logística asociadas a Hardware, Software, Redes de datos entre otros vinculados a este departamento.

#### 2.1.14 Seguridad Electrónica.

Gobernado por el mismo encargado de la gerencia de sistemas, este departamento se encarga del monitoreo de los clientes de seguridad electrónica y video vigilancia; además, está encargado de la instalación de los diferentes productos y servicios; este departamento consta de:

* **Monitoristas (3 encargados).-** Desempeñan la labor de vigilar la Central de Monitoreo y Video Vigilancia.
* **Técnicos de Seguridad Electrónica (3 agentes).-** Encargados de la Instalación de los productos de Seguridad Electrónica y Video vigilancia.

#### 2.1.15 Arquitectura de Red.

La red informática de la Empresa CISEPRO emplea una topología de Estrella la cual compone el siguiente equipamiento.

* 26 PC’s[[11]](#footnote-11) Distribuidas en los Diferentes departamentos de la Matriz.
* 4 Servidores divididos en:
  + 2 Servidor de Base de Datos
    - **DATABASE**: Servidor SQL SERVER 2008.
    - **SERVIDOR**: Servidor SQL SERVER 2005.
  + 3 Servidores de Procesamiento de Señales.
    - **PROCESADOR**: SEGURE VERSION 2010
    - **SISTEMAS**: SIGMA VERSION 2013
    - **LPL**: SIGMA 90
* 3 terminales móviles empleadas por los supervisores.
* Cable UTP categoría 6.
* Dos enlaces de fibra óptica que se interconectan a un Router.[[12]](#footnote-12)
* 1 Router TP-Link dos Antenas 4 puertos.
* 5 Router D-Link 6 puertos.
* 1 Switch[[13]](#footnote-13) D-Link DES-1228.
* 1 UPS[[14]](#footnote-14) ANDOLAS DE 11 KWA.
* 1 Central Telefónica Panasonic Serie: KX-TEM82.
* 1 Disco Duro de Respaldo Marca WDC 2TB en Red.
* 2 Impresoras RICOH C3000 conectas a un nodo de red.

### 2.2 Antecedentes Conceptuales.

#### 2.2.1 Información

Es un conjunto de datos procesados que cambia de estado, forma, consigna de acuerdo a su manipulación y propagación en un medio de intercambio.

##### 2.2.1.1 Principales Características de la información.

2.2.1.1.1 Significado.

Esta concepción depende de cómo cada persona evalúa el contenido de una información ¿Qué significado?, ¿Qué quiere decir?, para esto cada receptor extrae la información de acuerdo al lenguaje de comunicación (idioma) o sistema empleado para descifrar el mensaje.

###### **2.2.1.1.2** Importancia.

Basado en la relación trivial emisor – información – receptor se refiere a como el receptor cambia su actitud después de interpretar el significado de la información infiriendo internamente el esquema mental y modificando las expectativas futuras en un grado cuantitativo del contenido de la información, ¿Cuánto es importante?, ¿Cuánto es su relevancia?

###### 2.2.1.1.3 Vigencia.

Relativo al tiempo, es la vigencia en un determinado lapso de tiempo de la información. ¿Cuál es la dimensión de espacio - tiempo? , ¿La información es actual o desfasada?

###### 2.2.1.1.4 Validez.

Relativo a la fiabilidad, en otras palabras saber si la información es verdadera o falsa ¿La información será Fiable?, ¿La información tiene sentido alguno y lógica alguna?

###### 2.2.1.1.5 Valor.

Relativo a la cuantía, como esta información es valorable para el receptor, ¿Cómo es útil?, ¿Cómo es rentable? Dependiendo de la comprensión y su significado dentro de un contexto.

#### 2.2.2 Activos de Información.

Un conjunto de componentes humanos, tecnológicos, hardware, software, entre otros que están ligados al proceso productivo de una empresa; ósea todo aquello que tenga valor para la organización y por lo tanto se necesita proteger.

##### 2.2.2.1 Clasificación de los Activos de la Información.

|  |  |  |
| --- | --- | --- |
| **ACTIVOS DE INFORMACIÓN** | **CONCEPTO** | **EJEMPLOS** |
| Información Física | Un conjunto de datos que ocupan un espacio físico. | * Documentos. * Libros * Roles de Pago. * Contratos. |
| Información Digital | Un conjunto de datos que no ocupan un espacio físico, sino un espacio digital. | * Documentos digitalizados. * Archivos PDF’s[[15]](#footnote-15) * Documentos de Ofimática. * Archivos de datos. * Información de Una base de datos. * Contratos. * Acuerdos. * Documentación del sistema. |
| Software | Conjunto de instrucciones y rutinas que permiten a una personar mediante un computador realizar una determinada tarea. | * Sistemas Operativos. * Software Utilitario. * Sistema Contable SYSCISEPRO 2014. * Herramientas de Ofimática. * Sistemas Manejadores de Bases de Datos. * Aplicaciones de Software Específico. * Herramientas de Desarrollo. |
| Hardware | Conjunto de elemento físicos que componen un sistema informático, activos físicos que por su criticidad son considerados activos de información. | * Equipos de Computación. * Equipos de Comunicación. * Discos Duros Removibles. * Unidades de Respaldo. * Unidades de Almacenamiento. |
| Servicios de Información | Servicios prestados por empresa dedicadas a este ámbito que permiten acceder a una información determinada y manipularla. | * Bibliotecas Virtuales * Google Docs. * Microsoft Office online |
| Servicios de Comunicación | Todo medio que permite el envío y recepción de información; algunos pueden ser prestados por Empresas que ofrecen estos servicios especializados. | * Correo Electrónico. * Redes Locales (Carpetas Compartidas). * Servidores Samba. |
| Servicios de Almacenamiento | Servicios prestados por empresas para almacenar archivos en la nube (internet). | * Mega. * Google Drive. * One Drive. |
| Personas | Por su comprensión, habilidades, experiencia y criticidad para el procesamiento de información, son consideradas activos de información. | * Personal de la Organización. * Personal Subcontratado. * Clientes. * Usuarios. |
| Otros | Se refiere a la valoración que se le da una empresa al estar en funcionando en un mercado determinado. | * Imagen. * Reputación de la Organización. |

Tabla 2.1: Clasificación de los Activos de la Información

#### 2.2.3. Estándares.

Consiste en el establecimiento de un modelo de Normas, criterios, reglas que deben cumplirse para generar estabilidad de los procedimientos específicos de un contexto a fin de asegurar su calidad, eficacia y eficiencia.

##### 2.2.3.1 ISO (Organización Internacional para la Estandarización).

Es la organización Internacional para la estandarización que regula una serie de normas para fabricación, comercio, comunicación entre otras ramas industriales. Esta fue creada en 1947, luego de la Segunda Guerra Mundial y se convirtió en un organismo dedicado a promover el desarrollo de normas y regulaciones internacionales para la fabricación de todos los productos, exceptuando los que pertenecen a la rama de la eléctrica y la electrónica. Así, se garantiza calidad y seguridad en todos los productos, a la vez que se respetan criterios de protección ambiental.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. Los anteproyectos de los Estándares Internacionales adoptados por el comité técnico son presentados a los organismos nacionales para su votación. La publicación de un Estándar Internacional requiere de la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto. Se presta atención a la posibilidad que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC[[16]](#footnote-16) no debieran ser responsables de identificar todos o alguno de dichos de derechos de patente.

##### 2.2.3.2 BSI (Instituto de Estandarización Británico).

Es un organismo que colabora con ISO para proveer normativas o estándares para emplearlos como modelos que permitan mejorar el desempeño productivo de una Empresa en diferentes ámbitos y procesos, según Memorándum de Acuerdo reconoce el estatus de BSI como el representante del Reino Unido en las organizaciones internacionales de normalización.

*“Article 1: Introduction and definition*

*1.1. "The United Kingdom Govemment ("the Govemment") and the British Standards ("BSI") make the following memorandum of understanding which records their joint and several commitments and intentions regarding th "role of nbs", the contents of this memorandum are to be rea subject to the provision of the consolidated royal charter and bye-laws granted en 1981, as amended 198,1992, 1994 and 1998 (the royal charter)*

*for the purpose of this memorandum*

*1.2. for the purpose of the memorandum:*

*(i) "British Standards" and "other standardisation products"*

*(ii) Participation by BSI in European and international standards bodies, and other international activity undertakern in the interests of BSI as the United Kindom's NBS*

*(iii) promotion, marketing, distribution and information activities concerned withj brithish standards, BSi other standardisation products, and standardisation generally;*

*(iv) support and corporate infrastucture activities intended, wholly or in part, to enable (i)- (ii) above”[[17]](#footnote-17)*

##### 2.2.3.3 Principales Estándares de Seguridad Informática.

###### 2.2.3.3.1 ISO 17799.

“Establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Los objetivos señalados proporcionan una guía general sobre los objetivos comúnmente aceptados de gestión de la seguridad de la información. ISO / IEC 17799: 2005 contiene las mejores prácticas de los objetivos de control y controles en las siguientes áreas de gestión de seguridad de la información:

* La política de seguridad;
* Organización de la seguridad de la información;
* Gestión de activos;
* Recursos humanos de seguridad;
* Seguridad física y ambiental;
* Las comunicaciones y la gestión de las operaciones;
* Control de acceso;
* Los sistemas de información de adquisición, desarrollo y mantenimiento;
* Información de gestión de incidentes de seguridad;
* Gestión de la continuidad del negocio;
* Cumplimiento.

Los objetivos de control y controles de la norma ISO / IEC 17799: 2005 están destinados a ser implementado para cumplir con los requisitos identificados por una evaluación de riesgos. ISO / IEC 17799: 2005 pretende ser una base común y guía práctica para la elaboración de normas de seguridad de la organización y las prácticas eficaces de gestión de la seguridad, y para ayudar a construir la confianza en las actividades interinstitucionales.”[[18]](#footnote-18)

Figura 2.7: Estándar ISO 17799.[[19]](#footnote-19)

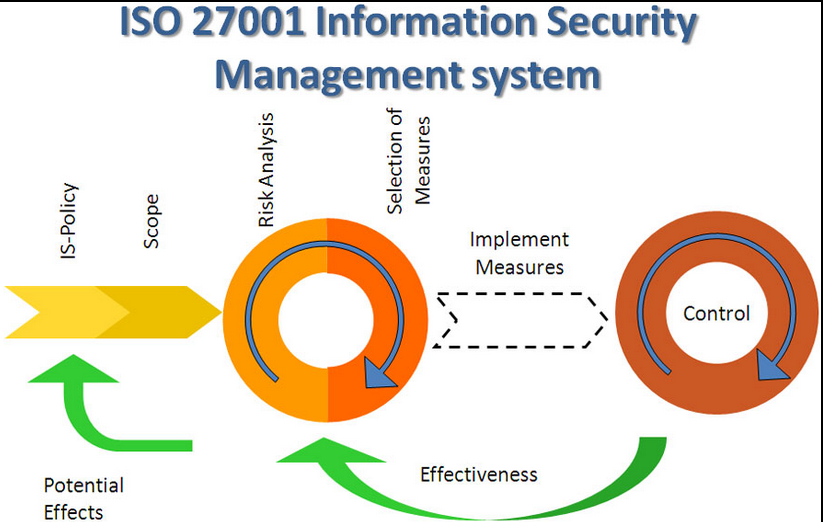
###### 2.2.3.3.2 ISO 27001.

“Cubre todos los tipos de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). ISO / IEC 27001: 2005 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información documentado en el contexto de los riesgos globales de negocio de la organización. Especifica los requisitos para la aplicación de los controles de seguridad adaptados a las necesidades de las organizaciones individuales o partes de los mismos.

ISO / IEC 27001: 2005 está diseñado para garantizar la elección de controles adecuados y proporcionados de seguridad que protegen los activos de información.

ISO / IEC 27001: 2005 está destinado a ser adecuado para diferentes tipos de uso, incluyendo los siguientes:

* Usar dentro de las organizaciones para formular requisitos y objetivos de seguridad;
* Usar dentro de las organizaciones como una forma de garantizar que los riesgos de Seguridad están cuestan gestionado con eficacia;
* Usar dentro de las organizaciones para asegurar el cumplimiento con las leyes y reglamentos;
* Utilizar dentro de una organización, como marco para el proceso de implementación y gestión de controles para asegurar que se cumplen los objetivos de seguridad específicos de una organización;
* Definición de nuevos procesos de gestión de seguridad de la información;
* Identificación y clarificación de los procesos de gestión de seguridad de la información existente;
* Usar por la gestión de las organizaciones para determinar el estado de las actividades de gestión de seguridad de la información;
* Usar por los auditores internos y externos de las organizaciones para determinar el grado de cumplimiento de las políticas, directrices y normas adoptadas por una organización;
* Utilizar las organizaciones para proporcionar información relevante acerca de las de seguridad de la información, directivas, normas y procedimientos a los socios comerciales y otras organizaciones con las que interactúan por razones operativas o comerciales;
* Implementación de seguridad de la información empresarial propicio;
* Utilizar las organizaciones para proporcionar información relevante sobre seguridad de la información a los clientes.”[[20]](#footnote-20)

Figura 2.8. Estándar ISO 27002[[21]](#footnote-21)

###### 2.2.3.3.3 ISO 27002.

**E**s un popular estándar internacionalmente reconocido de buenas prácticas para la seguridad de la información, remonta su historia de más de 30 años para los precursores de la Estándar Británico 7799. Al igual que la dirección y la gestión de riesgos, la gestión de seguridad de la información es un tema muy amplio, con derivaciones a través de todas las organizaciones. Seguridad de la información, y por lo tanto la norma ISO 27002, es importante para todo tipo de organizaciones, incluyendo empresas comerciales de todos los tamaños hasta gigantes multinacionales, departamentos, organizaciones benéficas, sin fines de lucro y del gobierno casi autónomo cuerpos - de hecho, cualquier organización que maneja y depende de la información.

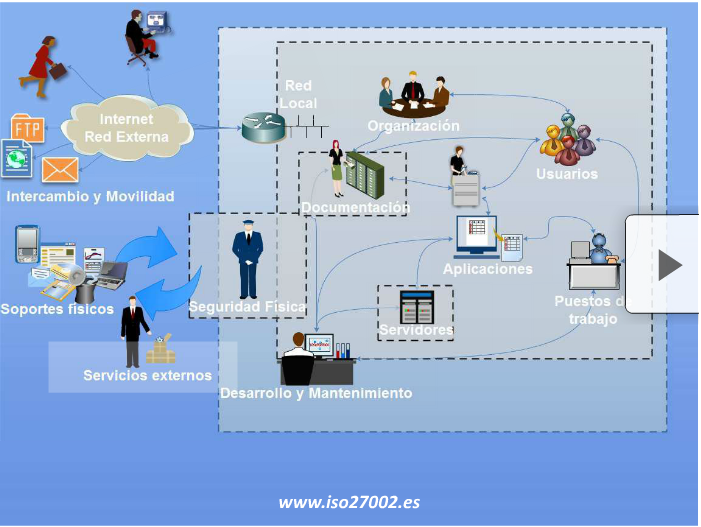


Figura 2.9. Estándar ISO 27002[[22]](#footnote-22)

Los requerimientos por riesgo de seguridad de la información y de control específicos pueden diferir en detalles, pero hay un montón de puntos en común, por ejemplo, la mayoría de las organizaciones tienen que hacer frente a los riesgos de seguridad de información en relación con sus empleados, además de los contratistas, los consultores y los proveedores externos de servicios de información.

El estándar se refiere explícitamente a la seguridad de la información, es decir, la seguridad de todas las formas de información (por ejemplo, datos informáticos, la documentación, el conocimiento y la propiedad intelectual) y no sólo de TI / sistemas de seguridad o "cyber-seguridad", como es la moda del día. Debido a que la información es un activo no menos importante que otros activos comerciales, es esencial para cualquier negocio u organización contar con las medidas adecuadas de protección de la información, especialmente en la actualidad, donde la información se difunde a través de miles y miles de redes interconectadas. Esto multiplica la cantidad de amenazas y vulnerabilidades a las que queda expuesta la información.

La información puede existir en muchas formas, por ejemplo puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, hablada en una conversación, etc. Sea cual sea la forma en la que se tenga la información, debe estar en todo caso protegida. La seguridad de la información se logra implementando un conjunto adecuado de controles, políticas, procesos, procedimientos, estructuras organizacionales, y otras acciones que hagan que la información pueda ser accedida sólo por aquellas personas que están debidamente autorizadas para hacerlo.

Es significativo y preciso para las empresas realizar una evaluación de riesgos para identificar amenazas para los activos, así como también para conocer y analizar la vulnerabilidad y la probabilidad de ocurrencia de accesos, robo o alteración de la información, y el impacto potencial que esto llegaría a tener. Una vez se hayan identificado los riesgos, se procede a seleccionar controles apropiados a implementar para asegurar que los riesgos se reduzcan a un nivel aceptable. Este Estándar Internacional va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo. Este Estándar contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

* Políticas de Seguridad
* Organización de la Seguridad de la Información
* Gestión de Activos.
* Seguridad Ligada a los Recursos Humanos.
* Seguridad Física y del Entorno.
* Gestión de Comunicación y del entorno.
* Control de Acceso.
* Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
* Gestión de Incidentes en la Seguridad de la Información.
* Gestión de la Continuidad del Negocio.
* Cumplimiento.

#### 2.2.4 Seguridad Informática.

Es la aplicación de medidas para proteger, prevenir, todo activo de información que este vulnerable ante la probabilidad que surja un riesgo basado en una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles amenazas a la infraestructura o a la información. Al hablar de la función de la informática generalmente se tiende hablar de nuevas tecnologías, nuevas aplicaciones, nuevos dispositivos de hardware nuevas formas de elaborar información más consistente. La base para la existencia de los elementos anteriores es la información.

La información es un activo importante que tiene valor para un organización y en consecuencia necesita ser protegido adecuadamente, la información puede existir en muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente transmitida por correo o utilizando los medios electrónicos o hablada en conversaciones cualquiera que sea la forma que tome la información, o el medio por el cual se comparten o se almacena, siempre se debe protegerla apropiadamente.

No se existen una conceptualización estricta o cerrada de lo que se entiende por seguridad informática, puesto que esta abarca múltiples disciplinas y muy diversas áreas relacionadas con los sistemas de información, áreas que van desde la protección física hasta la protección lógica, diversos tipos de amenazas contra los que debemos protegernos como los cortes eléctricos, hasta errores intencionados de los usuarios, pasando por los virus informáticos, el robo, destrucción o modificación de la información.

Por lo tanto, la seguridad informática se debe entender cómo, la interrelación de diferentes etapas, que al final del proceso garanticen elementos esenciales al interior de sus sistemas como son: confidencialidad, disponibilidad e integridad de la información. Dependiendo del tipo de sistema informático con el que tratemos (empresarial militar, gubernamental, entre otros), el orden de importancia de estos tres factores es diferente, e incluso entran en juego otros elementos como la autenticidad o el no repudio.

##### 2.2.4.1 Importancia de la Seguridad Informática.

La información y los procesos son activos comerciales importantes, la confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener una ventaja competitiva, rentabilidad, conformidad legal e imagen comercial.

La seguridad informática se logra implementando un conjunto de controles adecuados; que podrías ser políticas, procedimientos, estructuras organizacionales y funciones de software. Se necesita estos controles para asegurar que se cumpla los objetivos de seguridad específicos de la organización.

Cada vez más organizaciones y sus sistemas se enfrentan a amenazas contra su seguridad desde un rango amplio de fuentes; incluyendo fraude por medio de computadoras, espionaje, sabotaje, vandalismo, virus informático, incendio o inundaciones. La dependencia en los sistemas y servicios de información significa que las organizaciones son más vulnerables a las amenazas de la seguridad. Muchos sistemas de información no han sido diseñados para ser seguros, la seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser respaldada por una gestión y procedimientos apropiados. El punto de partida para un sistema de seguridad informática es la realización del diagnóstico de la situación inicial, para luego poder proyectar las soluciones a cada caso mediante políticas de seguridad.

##### 2.2.4.2 Variables de la Seguridad Informática.

**Confidencialidad**.- Denominada también privacidad es la necesidad de que la información solo sea conocida por personas autorizadas, asegura que la información no pueda estar disponible por o para otras personas, entidades o procesos no autorizados. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño o volverse obsoleta.

En áreas de seguridad el secreto asegura que los usuarios puedan acceder a la información que les está permitida en base a su grado o nivel de autoridad normalmente impuesta por disposiciones administrativas, este aspecto de la seguridad es particularmente importante cuando hablamos de empresas de seguridad privada.

Entre los procedimientos más utilizados para salvaguardar la confidencialidad tenemos:

* El uso de técnicas de control de acceso.
* El cifrado de la información confidencial o de las comunicaciones.

**Integridad*.-*** Esta garantiza que la información debe ser modificada creada y borrada solo por el personal autorizado y dicha modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dad por anomalías en el hardware, software, virus informáticos o por la modificación realizada por parte de personas que se infiltran en el sistema.

Esta propiedad permite asegurar que no se ha falseado la información, el problema de la integridad no solo se refiere a modificaciones intencionada, sino también a cambio accidentales o ni intencionados.

**Disponibilidad**.- Es la capacidad de la información al estar en el lugar, momento y forma en que es requerido por el usuario autorizado para ser procesada en un periodo de tiempo aceptable. Esto requiere que la misma se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente respetando formatos para su recuperación satisfactoria en caso de fallo. Lo opuesto a disponibilidad, y uno de los posible métodos de ataque a un sistema informático, se denomina “denegación de servicio”.

Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados.

**Autenticidad**.- Permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidad.

**No-Repudio**.- Dentro de un sistema de información la característica del no-repudio permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

##### 2.2.4.3 Requerimientos de Seguridad Informática.

La identificación de los requerimiento de seguridad permite determinar cuáles de los activos de la empresa tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, considerando el grado en que el riesgo puede ser controlado y definiendo los servicio y las medidas de seguridad que se deben implementar para proteger un determinado entorno de la organización. Los riesgos se clasifican por el nivel de importancia y por la severidad de la perdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

##### 2.2.4.4 Delitos informáticos.

Los delitos informáticos actualmente se los asocia directamente a las personas que los cometen, comparándolos con un delito común; supongamos como patrón una situación en la de que se suscite un asalto o robo hacia un individuo determinado este escenario se ve afectado por un delincuente el cual vulnera la seguridad de la persona y se apropia de los bienes de esta para beneficiarse; basado en esta analogía podríamos decir que un delito informático es la apropiación o el plagio de un activo de la información por una persona, medio, proceso al cual no le pertenece o no tiene permisos pertinentes.

###### 2.2.4.4.1 Hackers.

“Hacker es un vocablo utilizado por los informáticos para referirse a un experto en varias o alguna rama técnica relacionada con la informática tales como: programación, redes de computadora, sistemas operativos, etc. Es una persona apasionada por descubrir o aprender nuevas cosas y entender el funcionamiento de estos para bien o mal. Pueden romper seguridades en los sistemas de una empresa por diversión o explorar datos privados, pero la ética hacker no permite divulgar esos datos privados ya que sería un acto de vandalismo.”[[23]](#footnote-23); basado en lo mencionado por Cadme Ruiz & Duque Pozo un hacker es un entusiasta con conocimientos muy enriquecidos en informática capaz de vulnerar la seguridad informática, que su mayor anhelo es infringir e irrumpir en los activos de la información de una determinada entidad; que aunque este sabe que está cometiendo un delito informático no le importa la ética informática, los hackers son los más temibles en la nube, ya que aunque se puede detectar su intrusión con los métodos actuales obtener su identidad, su origen son un tanto complicado de determinar.

###### 2.2.4.4.2 Crackers.

“Es una persona con grandes conocimientos informáticos y con un propósito de luchar en contra de lo que está prohibido, empieza a investigar la forma de bloquear o traspasar protecciones hasta lograr su objetivo. Los crackers usan programas propios o bajados del internet gratuitamente, con esos programas se intenta desbloquear claves de acceso con generadores automáticos de claves”[[24]](#footnote-24); tienen la misma finalidad que los hackers con la diferencia que solo tienen conocimientos básicos en informática y más bien se valen de herramientas elaboraras por los hackers para ejecutar un delito informático o una infiltración no autorizada, estos tienen una conciencia de la acción que están causando o ejecutando.

2.2.4.4.2.1 Lammer.

“Es una persona con poco conocimiento informático, que consiguen herramientas ya creadas para atacar ordenadores. Ejecutan aplicaciones sin saber que están causando grandes daños.”[[25]](#footnote-25); difieren de los crackers ya que prácticamente realizan delitos informáticos sin saber que lo están haciendo, por el hecho de ejecutar aplicaciones informáticas sin ningún tipo de conocimiento o respaldo de la acción que realicen.

2.2.4.4.2.2 Trasher.

“Son personas que buscan basura informática en papeleras de reciclaje, números de tarjetas de crédito, claves de acceso, cuentas bancarias, entre otros; para cometer estafas y actividades fraudulentas a través del internet.”[[26]](#footnote-26), a juicio propio de las conceptualizaciones anteriores un Trasher teniendo el conocimiento de un Hacker busca el lucro de sus infiltraciones en los activos de la información.

2.2.4.4.2.3 Insiders.

“Crackers corporativos, empleados de la empresas que las atacan desde dentro, movidos usualmente con motivos de venganza”[[27]](#footnote-27), su incidencia es reincidente por lo que su nivel de delito es mayor, comparándolo con los entes de delitos informáticos son los maliciosos y ofensivos ante un SGSI.

###### 2.2.4.4.5 Virus Informático.

Los virus informáticos son un tipo más del conjunto de software malicioso, es decir son programas informáticos cuyos objetivos es vulnerar un sistema informático causando daño, que puede ir desde una simple molestia hasta la pérdida de valiosa información.

**2.2.4.4.5.1 Tipos de Virus.**

Según Gonzalo Armas “existen muchas formas de tipificar a los virus, dependiendo de su propósito o fin para el cual fueron desarrollados pero el destaca los siguientes:

**“De Archivo:** Este tipo de virus se encarga de infectar programas o archivos ejecutables (con extensiones EXE o COM) agregándose al principio o final de los mismos. Al realizar la ejecución de uno de estos programas, de forma directa o indirecta, el virus se activa cargándose en memoria para infectar otros archivos y produciendo los efectos dañinos que le caractericen en cada caso.” [[28]](#footnote-28)

**“De Sobre escritura:** A diferencia del virus de archivo, este tipo de virus se caracteriza por no respetar la información contenida en los archivos que infecta, haciendo que estos queden inservibles posteriormente. Aunque la desinfección es posible, no existe posibilidad de recuperar los archivos infectados, siendo la única alternativa posible la eliminación de éstos. Una característica interesante es que los archivos infectados por virus de sobre escritura no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio archivo infectado cosa poco probable. Esto es debido a que dicho tipo de virus se coloca encima del contenido del archivo infectado, no se incluye de forma adicional en una sección del mismo. El efecto que producen estos virus sobre los archivos infectados, es la pérdida parcial o total de su contenido y ésta será irrecuperable.”[[29]](#footnote-29)

**“De macros:** A diferencia de los tipos de virus comentados anteriormente, los cuales infectan programas (archivos EXE o COM), estos virus realizan infecciones sobre los archivos (documentos, planillas electrónicas, presentaciones y/o bases de datos) que contienen macros. Una macro no es más que un micro programa que el usuario asocia al archivo que ha creado con determinados software. Éste no depende del sistema operativo sino de acciones determinadas que el usuario puede realizar dentro del documento que la contiene. “

**“Virus que infectan el sector de arranque (boot):** El término Boot o Boot Sector representa lo que también se denomina "sector de arranque". Se trata de una sección muy importante en un disco (disquete o disco duro), en la cual se guarda la información sobre las características del mismo y que incluye un programa que permite arrancar el computador desde ese disco, determinando previamente si existe sistema operativo en el mismo. El virus de Boot se aloja en dicho sector, por lo que el contenido del disco no estará en peligro a no ser que se intente arrancar el computador con dicho disco.” [[30]](#footnote-30)

**Gusanos (Worms):** Un gusano es un malware que tiene la propiedad de duplicarse ya sea en la memoria RAM y/o a través de redes (Internet por ejemplo). A diferencia de un virus, un gusano no precisa alterar los archivos de programas. Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

**“Troyanos:** Los denominados “troyanos” recogen su nombre del famoso caballo de la mitológica guerra de Troya, en el cual los soldados griegos se escondieron dentro un gigantesco caballo de madera de apariencia inofensiva para de esa manera poder ingresar a la fortificada ciudad de Troya.”[[31]](#footnote-31)

“**Bombas lógicas:** Es un programa informático que se instala en un computador y permanece oculto hasta cumplirse una o más condiciones pre programadas para entonces ejecutar una acción. Una bomba lógica no se reproduce por si sola, por lo tanto no puede catalogársela como virus.”[[32]](#footnote-32)

“**Stealth (ocultamiento):** Son un conjunto de técnicas que buscan hacer pasar inadvertido al virus o a sus efectos ante los antivirus, por ejemplo: o No modificar ni la fecha, ni el tamaño original del archivo al infectarlo o Modifica directamente la FAT y la tabla de interrupciones o Se instalan por encima de los 640 Kb de memoria RAMo Evita que se muestren mensajes de error, cuando el virus intenta hacer algo no permitido por el sistema.” [[33]](#footnote-33)

**“Encriptación y Polimórficos:** En el caso de virus encriptados, el virus mediante un algoritmo de encriptación hace ilegible su código, en el caso de los virus polimórficos, este algoritmo cambia de una infección a otra. Sin embargo, el virus no puede codificarse completamente a sí mismo, ya que necesita contar con una parte (no cifrada) que le permita realizar su propia decodificación. Esto es utilizado por los programas antivirus para realizar la detección de los virus que utilizan estas técnicas.”[[34]](#footnote-34)

**“Armouring:** La técnica de armadura busca evitar que pueda revelarse el contenido de un archivo infectado, de esta manera puede evitar que sea revelada su firma. No obstante esta situación será advertida por los antivirus y el usuario podrá decidir qué hacer con los archivos que no pueden ser analizados.” [[35]](#footnote-35)

**“Tunneling:** Los virus utilizan esta técnica para eludir la protección de los antivirus residentes en la memoria, los cuales monitorean todo lo que sucede en la computadora para interceptar las actividades típicas de los virus. El antivirus residente está “a la escucha” de todas las acciones potencialmente peligrosas del sistema y en caso de encontrar actividad sospechosa como modificar un ejecutable detecta al virus, en cambio si se trata de hacer algo no sospechoso el antivirus permite terminar dicha acción. El virus que utiliza la técnica de tunneling pretende saltear esta protección del antivirus haciendo un “túnel” o eludiendo su protección.”[[36]](#footnote-36)

**“Residentes en Memoria:** El virus se oculta en la memoria RAM, infectando a todo archivo ejecutable que se cargue en memoria, si bien el contenido de la RAM se borra al reiniciar el computador, muchos de estos virus modifican el registro para ser cargados por el sistema operativo al reiniciar.”[[37]](#footnote-37)

2.2.4.4.5.2 Métodos de propagación.

* Memoria secundaria.- Se refiere a todo hardware que permite el almacenamiento e intercambio de información digital.
* Redes Locales.- Cuando se comparte archivos o programas a través de un medio de red local dentro de una entidad.
* Internet.- La nube el cual es el más común por su empleo en el intercambio de información.

2.2.4.4.5.3 Métodos de Protección.

Un antivirus es el método común, más tradicional de protección de los sistemas de información, estos consisten en programa diseñados para detectar y eliminar los virus, que se ejecuten en memoria periódicamente detectar las amenazas en un sistema informático.

###### 2.2.4.4.6 Sabotaje Informático.

“Define al sabotaje informático como la acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional mediante el empleo natural de las tecnologías de la información. Es común que tales atentados a los datos y los programas los realicen trabajadores de la misma empresa, e incluso los propietarios de los programas.”[[38]](#footnote-38)

###### 2.2.4.4.7 Fraude Informático.

“Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.” [[39]](#footnote-39)

###### 2.2.4.4.8 Estafas Electrónicas o Phishing.

“Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea” [[40]](#footnote-40)

###### 2.2.4.4.9 Espionaje Informático o Sniffing.

“Se trata de una técnica por la cual se puede ‘escuchar’ todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet. Esto se hace mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red, así como la interactuación con otros usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios, entre otros.).” [[41]](#footnote-41)

###### 2.2.4.4.10 Infracción a los Derechos del Autor.

“La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.” [[42]](#footnote-42)

###### 2.2.4.4.11 Infracción del Copyright de Base de Datos.

“No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan «downloads» de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.”[[43]](#footnote-43)

###### 2.2.4.4.12 Uso Ilegitimo de Sistemas Informáticos Ajenos:

“Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometido por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo. En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.” [[44]](#footnote-44)

###### 2.2.4.4.13 Accesos No Autorizados.

“La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.” [[45]](#footnote-45)

###### 2.2.4.4.14 interceptación de E-Mails.

“En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.” [[46]](#footnote-46)

**2.2.4.4.15 Pornografía Infantil.**

“Se refiere a todo material visual o auditivo que utilice niños, destinado a la gratificación sexual del usuario. Incluye producción, distribución y utilización de este tipo de material”[[47]](#footnote-47)

#### 2.2.5 Elementos de Seguridad.

##### 2.2.5.1 Principios de Seguridad.

Son las bases fundamentales que debe seguir para alcanzar niveles apropiados de seguridad en un contexto productivo, para lo cual se vale de los principios de la seguridad de la información en el apartado [2.2.6.1](#_2.2.6.1_Principios_Fundamentales).

##### 2.2.5.2 La Gestión del Riesgo.

Los activos de la información dentro de un contexto empresarial deben ser resguardados mediante la protección de garantías. Estas deben ser escogidas y gestionadas sobre un marco metodológico de gestión de riesgo, que evalué la organización, los bienes, las amenazas, vulnerabilidades y el impacto que producen las mismas, para atender los riesgos y tomar decisiones en cuanto a las limitaciones.

##### 2.2.5.3 Compromiso.

Es la obligación que adquiere todo la estructura de una empresa para especificar los beneficios de la implementación de un plan de seguridad informática.

##### 2.2.5.4 Funciones y Responsabilidades.

Son los roles y responsabilidades de acuerdo a los cargos ocupacionales y mapas de procesos de todo el conjunto que conforman el contexto de una empresa.

##### 2.2.5.5 Objetivos, Estrategias y Políticas.

Los riesgos para la seguridad de los activos de la información deben ser manejados considerando los objetivos, estrategias y políticas de la organización.

##### 2.2.5.6 Activos.

En relación con la seguridad de la información, se define con cualquier información o sistema relacionado con el tratamiento, procesamiento de la misma que tenga un valor para la empresa.

##### 2.2.5.7 Bienes.

La gestión apropiada de los activos es trascendente para el éxito de la empresa, y es una de las principales responsabilidad de todos los niveles de gestión.

Los activos de la información son lo suficientemente valioso para justificar con un alto grado de protección, estos pueden incluir:

* Activos Físicos.
* Información.
* La capacidad de proporcionar un producto o servicio, personas.
* Bienes intangibles, entre otros.

Desde el matiz de seguridad, no se puede aseverar que implementar y mantener un plan de seguridad informática se garantice el éxito de la protección de los activos de la información, pero esta práctica se debe medir en factores de tiempo, costo en comparación con los bienes.

##### 2.2.5.8 Amenazas.

Los activos están sujetos a diversos tipos de amenazas. Una amenaza tiene el potencial de causar daño a un activo y por lo tanto a una organización. Este daño puede ocurrir a partir de un ataque a la información, causando destrucción no autorizada, divulgación, modificación, la corrupción y la falta de disponibilidad o pérdida.

Una amenaza tiene que explotar una vulnerabilidad existente del activo con el fin de perjudicar a los activos. Las amenazas pueden ser de origen ambiental o humano y, este último caso, puede ser accidental o deliberada. Amenazas tanto accidental como intencionada deben ser identificadas, su nivel, probabilidad de ocurrencia evaluada. Los datos estadísticos disponibles sobre muchos tipos de las amenazas ambientales pueden ser obtenidos y utilizados por una organización, mientras se evalúa las amenazas.

Las amenazas tienen características que definen sus relaciones con los elementos de seguridad. Al definir las amenazas se debe tomar en cuenta el entorno y la cultura en la que se encuentra la empresa. Las amenazas pueden ser calificadas en términos tales como Alta. Media y Baja, en función del resultado de evaluación de amenazas.

##### 2.2.5.9 Vulnerabilidad.

Una debilidad de un bien, o grupo de bienes, que puede ser explotado por una o más amenaza se conoce como una vulnerabilidad. Las vulnerabilidades asociadas con bienes incluyen debilidades en el diseño físico, organización, procedimientos, talento humano, gestión, administración, hardware, software, información entre otros.



Figura 2.10: Ejemplo de vulnerabilidad, una contraseña de usuario.[[48]](#footnote-48)

Una vulnerabilidad puede existir en ausencia de amenazas correspondientes. Una vulnerabilidad no es más que una condición o un conjunto de condiciones que pueden permitir que una amenaza afecte a un activo. Vulnerabilidades que surgen de diferentes fuentes deben ser consideradas, por ejemplo, los intrínsecos o extrínsecos al activo. Las vulnerabilidades deben ser evaluadas individualmente y en conjunto para considerar el contexto operacional,

Dentro de un sistema u empresa específica, no todas las vulnerabilidades serán susceptibles a una amenaza. Vulnerabilidades que tienen un peligro son de interés inmediato. Sin embargo, como el medio ambiente puede cambiar impredeciblemente, todas las vulnerabilidades deben ser controladas para identificar a los que se han expuesto a nuevas o reincidentes amenazas.

Evaluar las vulnerabilidades es el examen de las debilidades que pueden ser explotadas por las amenazas identificadas. Esta evaluación debe tener en cuenta el medio ambiente y las garantías existentes. La medida de una vulnerabilidad de un sistema particular o bien, es una declaración de la facilidad con la que el sistema o bien puede resultar perjudicado. Las vulnerabilidades pueden ser calificadas en términos cualitativos tales como Alta, media y baja en función del resultado de la evaluación de la vulnerabilidad.

##### 2.2.5.10 Impacto.

Es el resultado de un incidente de seguridad de la información causada por una amenaza, que afecta a los bienes. El impacto podría ser la destrucción de cientos de activos, daños en los sistemas informáticos y compromiso de confidencialidad, integridad disponibilidad no repudio, la rendición de cuentas, autenticidad o fiabilidad. Impacto indirecto incluye posibles pérdidas financieras y la perdida d cuota de mercado o imagen de la empresa. La medición del impacto permite un equilibrio que se hizo entre los resultados previstos de un incidente y el costo de garantías de protección contra el incidente. Se debe tener en cuenta la probabilidad de ocurrencia de un incidente, las mediciones cuantitativas y cualitativas del impacto pueden lograr de varias formas, como:

* Establecer el costo financiero.
* Asignar una escala empírica de la gravedad, por ejemplo, del 1 al 10
* El uso de adjetivos seleccionados de una lista predefinida, por ejemplo, alta, media, baja.

##### 2.2.5.11 Riesgo.

Es la posibilidad de que una amenaza se aprovecha de las vulnerabilidades de un activo o grupo de activos y por lo tanto cause daño a la organización. Amenazas simples o múltiples pueden explotar una o múltiples vulnerabilidades. Para describir los riesgos dentro de la empresa se debe plantear escenarios mediante los cuales se pueda explotar una determinada vulnerabilidad o un grupo de vulnerabilidades que exponen los bines de daño mediante una o varias amenazas, caracterizando el riesgo por una combinación de dos factores, la probabilidad de que el incidente que se produzca y sus consecuencias.



Figura 2.11: Ejemplo de Riesgo, La probabilidad de la suplantación por robo de contraseñas.[[49]](#footnote-49)

Cualquier cambio en los bienes, las amenazas, vulnerabilidades y garantías pueden tener efectos significativos sobre los riesgos. La detección temprana o el conocimiento de los cambios aumentan la oportunidad para tomar las medidas adecuadas para tratar los riesgos.

La detección temprana o el conocimiento de los cambios aumentan la oportunidad para tomar las medidas adecuadas para tratar los riesgos. Opciones para el tratamiento de riesgo incluyen la cobertura de riesgos, reducción de riesgos, el riesgo transferencia y aceptación de riesgos.

##### 2.2.5.12 Seguridades.

Son prácticas, procedimientos o mecanismos que pueden proteger contra una amenaza, reducir la vulnerabilidad, limitar el impacto de un incidente de seguridad de la información, detectar los incidentes y facilitar la recuperación.

Una selección apropiada de las seguridades es esencial para un plan de seguridad implementado correctamente. Una medida de seguridad puede servir para múltiples propósitos, por el contrario, una función puede requerir varias seguridades. Estas estrategias pueden ser consideradas para llevar a cabo una o más de las siguientes funciones.

* La prevención.
* La disuasión.
* Detección.
* Limitación.
* Corrección.
* La recuperación.
* El seguimiento.
* Concienciación.

Ejemplos de seguridades específicas:

* Políticas.
* Procedimientos.
* Mecanismos de Control.
* Software Antivirus.
* Firmas Digitales.
* Toquen- Electrónicos.
* Seguimientos y análisis de herramientas.
* Fuentes de alimentación redundantes.
* Respaldos de información

##### 2.2.5.13 Limitaciones.

Se deben describir las restricciones que son normalmente establecidas o reconocidas por la administración de la organización y la influencia del entorno en que opera la organización. Algunos ejemplos de restricciones que se deben considerar son:

* Organización.
* Negocio.
* Financiero.
* Medio ambiente.
* Talento Humano.
* Tiempo.
* Legal.
* Técnica.
* Cultural.
* Social.
* Empresarial.
* Infraestructura.

Estos factores deben ser considerados en la selección o aplicación de seguridades, periódicamente, las limitaciones existentes y nuevas deben ser revisadas.

#### 2.2.6 Aspectos Organizativos de la Seguridad Informática.

“La seguridad informática es un tema interdisciplinario y relevante para diferentes contextos en una organización. Una distribución adecuada y delimitación de responsabilidades debe garantizar que todas las tareas importantes se realizan de una manera eficiente.

Aunque este objetivo se puede lograr a través de diversos esquemas de organización, depende del tamaño y de la estructura de una organización, para lo cual se puede utilizar los siguientes medios:

Un comité de seguridad de tecnologías de información que generalmente resuelve los problemas interdisciplinarios y aprueba las directrices y normas.

Un oficial de seguridad de tecnologías de información quien actué como el centro de todos los aspectos de seguridad en una organización.

Tanto el comité como el oficial de seguridad de tecnologías de información, deben tener bien definidos los deberes y ser lo suficientemente claros como para asegurar el compromiso con la política corporativa de seguridad.

La organización facilitara unas líneas claras de comunicación. La responsabilidad y la autoridad del oficial de seguridad de la empresa. La realización de estas tareas puede ser complementada con la utilización de consultores externos.” (Buitrago, Bonilla, & Murillo, 2012)

##### 2.2.6.1 Principios Fundamentales de la Seguridad de la Información.

###### 2.2.6.1.1 Confidencialidad.

La confidencialidad indica que se debe garantizar que los activos sean solo accedidos por los usuarios con acceso autorizado por la organización, personal, proceso o entidad autorizada. En consecuencia puedan obtener la información requerida con las autorizaciones adecuadas. La seguridad que se implanta debe asegurar que no se viole este principio.

###### 2.2.6.1.2 Integridad.

Este principio protege y Garantizar la precisión, calidad, veracidad, imparcialidad y completitud del activo en cuanto a la exactitud y totalidad de los datos y los métodos de procesamiento ingresados por los usuarios con acceso autorizado. La pérdida de integridad en la información puede deberse a errores humanos, intrusiones intencionadas, o por la vulneración de los activos de la información por métodos inapropiados, estos en ocasiones peligrosos.

###### 2.2.6.1.3 Disponibilidad.

Indica que el activo sea oportuno, es decir garantizar que los usuarios, entidad o proceso previamente autorizados puedan consultar y usar a la información y sus activos asociados cuando lo requieran. Los recursos deben estar disponibles cuando se necesite emplearlos.

Figura 2.12: Principios Fundamentales de la Seguridad de la Información.[[50]](#footnote-50)

#### 2.2.7 Gestión de la Seguridad Informática.

La planificación y gestión de la seguridad es el proceso general de establecer y mantener un programa de seguridad de las tecnologías de la información en la empresa. Este proceso debe adaptarse de acuerdo a la forma de gestión, tamaño empresarial y diseño organizacional. Las revisiones se las hacen conjuntamente con las actividades y funciones. Para definir correctamente la gestión de la seguridad informática se debe tener claro los objetivos de la empresa y se debe crear una estructura organizacional que apoye con éxito de los mismos.

##### 2.2.7.1 Sistema de Gestión de Seguridad de la Información (SGSI).

“SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

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

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.”[[51]](#footnote-51)

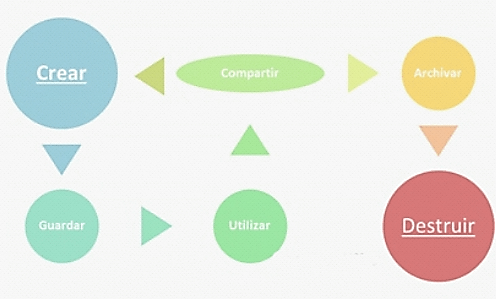
En base los principios de seguridad de la información se deben adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Figura 2.13: Ciclo de vida de la Información[[52]](#footnote-52)

##### 2.2.7.2 Mejora Continua (Ciclo Deming).

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001:2005, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

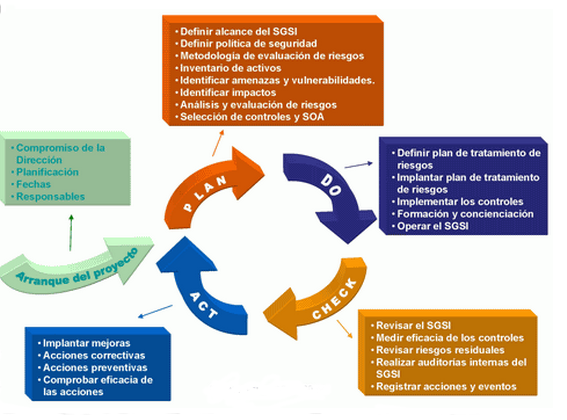


Figura 2.14: Ciclo de Deming[[53]](#footnote-53)

###### 2.2.7.2.1 Planificar (Plan - Establecer una planificación)

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado). Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes...) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, entre otros.

* La política del SGSI es normalmente un documento muy general, una especie de "declaración de intenciones" de la Dirección pero que:
* Incluya el marco general y los objetivos de seguridad de la información de la organización;
* Tener en cuenta los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información;
* Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
* Establezca los criterios con los que se va a evaluar el riesgo;
* Esté aprobada por la dirección.

Definir el enfoque de evaluación de riesgos mediante una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio. El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar grados de subjetividad que falseen la valoración de los riesgos. Existen numerosas metodologías estandarizadas para la evaluación de riesgos y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia. ISO 27001:2005 no impone ninguna para que cada organización pueda aplicar la que estime más oportuno y funcional según el esfuerzo de análisis y recursos que pueda aplicar. Como documento de apoyo ISO 27005 sí profundiza en directrices sobre la materia.

###### 2.2.7.2.2 Hacer (Do - Implementar y Utilizar el SGSI).

• Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

• Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

• Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

• Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

• Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

• Gestionar las operaciones del SGSI.

• Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

• Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

• Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

###### 2.2.7.2.3 Chequear (Check - Monitorizar y Revisar).

* Ejecutar procedimientos de monitorización y revisión para:
  + Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  + Identificar brechas e incidentes de seguridad;
  + Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
  + Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
  + Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
* Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
* Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
* Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, entre otros.
* Realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
* Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo las adecuadas y posibles mejoras en el proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
* Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
* Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

###### 2.2.7.2.4 Actuar (Act - Mantener y Mejorar).

* Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas y materializadas. en relación a la cláusula 8 de ISO 27001:2005 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
* Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
* Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.
* PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

#### 2.2.8 Análisis Estratégico del Riesgo.

Cualquier organización que desee mejorar la seguridad debería poner en marcha una estrategia para la gestión de riesgos que sea adecuada para su entorno, y establecer los medios para hacer frente a los riesgos de manera efectiva. Es necesaria estrategia una estrategia que centre sus esfuerzos de seguridad en donde se precise así como un enfoque de costos y el tiempo requerido.

No es cuestión de recursos o de tiempo efectivo para llevar a cabo revisiones detalladas en todos los sistemas, ni es eficaz, para hacer frente a graves riesgos. Por tanto, un enfoque que ofrezca un equilibrio entre estos extremos implica la realización de exámenes de alto nivel para determinar las necesidades de seguridad de tecnologías de información de los sistemas de análisis, a una profundidad consistente con estas necesidades. Los requerimientos de seguridad de cualquier organización dependen de su tamaño, del tipo de negocio que está haciendo y de su entorno y la cultura. El análisis de riesgo corporativo como opción estratégica para ser seleccionados, debe estar directamente relacionado con estos hechos.

En algunas situaciones, una organización puede decidir no hacer nada o aplazar la aplicación de las garantías. Esta decisión de la gerencia solo debe hacerse después de que la organización ha completado su examen de alto nivel. No obstante, si se toma una decisión, la admisión debe ser plenamente consciente de los riesgos e impactos adversos de los que pueden ser responsables, y aun la probabilidad de un incidente no deseado que tenga lugar.

Sin ese conocimiento, la organización sin darse cuenta puede estar en violación de las leyes o reglamentos y puede exponerse a una posible perdida. La Decisión y la justificación para no hacer algo o para posponer la aplicación de las garantías deben adoptarse solo después de una serie consideración sobre estos asuntos y otros posibles efectos adversos basándose en los resultados de los exámenes de alto nivel.

##### 2.2.8.1 Identificar los riesgos

* Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
* Identificar las amenazas relevantes asociadas a los activos identificados;
* Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
* Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

##### 2.2.8.2 Analizar y evaluar los riesgos.

* Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
* Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
* Estimar los niveles de riesgo;
* Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

##### 2.2.8.3 Identificar y Evaluar las Distintas Opciones de Tratamiento de los Riesgos

* Aplicar controles adecuados (mitigación);
* Aceptar el riesgo (de forma consciente), siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
* Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
* Transferir el riesgo total o parcialmente a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.



Figura 2.15: Gestión del Riesgo[[54]](#footnote-54)

#### 2.2.9 Plan de Seguridad informática

Un plan de seguridad es un documento que define las acciones coordinadas para llevar a cabo una política de seguridad de tecnologías de información dentro de una organización. Este plan debe contener las principales acciones que se emprenderán en corto, mediano y largo plazos, y los costos asociados, en términos de inversiones: costos de operación, la carga de trabajo, entre otras., un calendario del tiempo. Debe, en consecuencia, incluir:

* Una arquitectura de seguridad global y su diseño
* Una breve reseña del sistema de tecnologías de información para mantener la coherencia con los objetivos de seguridad de la organización, deberá proteger e impedir que se produzcan un máximo de pérdidas financieras, la vergüenza, el deterioro de la imagen de la empresa, entre otras.
* La identificación de las garantías correspondientes a los riesgos evaluados, se conserva y debe ser aprobada por la administración.
* Una evaluación del nivel real de confianza en las garantías que incluya la determinación de su eficacia.
* Una descripción general de la evaluación de los riesgos residuales en el contexto del sistema dado su aplicación.
* La identificación y definición de acciones prioritarias con sus respectivas garantías con el fin de aplicarlas.
* Un plan de trabajo detallado para la aplicación de garantías, incluidos las prioridades, el presupuesto y los horarios.
* Las actividades de control de proyectos, que incluyan: La comisión de recursos y asignación de responsabilidades, la definición de los procedimientos de los informes de progreso, la conciencia de seguridad y los requisitos de capacitación para el talento humano y los usuario finales.
* Requisitos para el desarrollo de operativos de seguridad y procedimientos de administración.

Además, el plan debe incluir los procedimientos que definen las condiciones u acciones para la validación de cada uno de los puntos anteriores, incluyendo la modificación del propio plan.

#### 2.2.10 Implementación de Seguridades.

Después de haber establecido un plan de seguridad informático, es necesario ponerlo en práctica. Se debe tener en cuenta los objetivos durante la implementación de seguridad. Asimismo, debe asegurarse que:

* El costo de las garantías permanezca dentro del rango aprobado.
* Las garantías se ejecuten correctamente como lo exige el plan de seguridad.
* Las garantías son operadas y administradas como lo requiere el plan de seguridad.

La mayoría de las garantías técnicas debe complementarse con los procedimientos operativos y administrativos, y no se pueden imponer medios puramente técnicos. Por tanto, los procedimientos deben ser apoyados y ejecutados por la línea gerencial.

La concienciación sobre la seguridad y la formación también se consideran una medida de garantías debido a su importancia, la conciencia de seguridad.

Cualquier cambio significativo en un sistema o servicio debe conducir a un nuevo control, volver a comprobar y luego aprobación del sistema o servicio.

Según la normativa ISO 27001:2005 se establece los siguientes dominios o marco referencial para aplicar un plan de seguridad de activos de información:

##### 2.2.10.1 Políticas de Seguridad (Cláusula 5).

**“Objetivo**: Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.

**Principios**: La Dirección debería establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.

* Debe contener un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices.
* Determinar la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización.
* La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.”[[55]](#footnote-55)

##### 2.2.10.2 Aspectos Organizativos de la Seguridad de la Información. (Cláusula 6).

“Cuando hablamos de seguridad de la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores.

Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca 'por el camino'. Si es más fácil acceder a ella también es más fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.”[[56]](#footnote-56)

##### 2.2.10.3 Gestión de Activos. (Cláusula 7).

“Es pre-requisito para la administración de riesgos adquirir y mantener conocimiento sobre todos los Activos de Información de la Empresa, sus responsables y depositarios. Los activos de información deben ser clasificados y rotulados de acuerdo con la sensibilidad y criticidad de la información que contienen, con el objeto de determinar cómo han de ser tratados y protegidos. La clasificación debe ser revisada para determinar si el valor de la información ha variado con el tiempo para ser reclasificada, o si se ha tornado obsoleta para ser eliminada.”[[57]](#footnote-57)

##### 2.2.10.4 Seguridad Ligada a los Recursos Humanos. (Cláusula 8).

“El objetivo de este procedimiento es asegurar que todo el personal interno y externo conoce y aplica las medidas de seguridad establecidas por la empresa.

* Dentro de este procedimiento es necesario definir:
* Escenarios posibles (antes, durante y después de la contratación) y actividades a realizar.
* Perfiles de usuario para cada área de la empresa con respecto a la seguridad.
* Roles que intervienen en el proceso.
* Responsabilidades de los roles.
* Documentación y registros a generar.
* Documentación y plantillas de referencia.

La seguridad ligada a los recursos humanos se gestionará a tres niveles:

* **Antes de la contratación.-** Los responsables de cada área junto con la Dirección de la organización deben definir los perfiles de cualificación que definen las funciones y responsabilidades de seguridad de la organización, adecuados a los requisitos del puesto a ocupar, en los que se especificará las competencias que deben cubrir las personas que ocupen el puesto de trabajo en cuestión. La selección de personal se realizará siguiendo estos perfiles e informando de las obligaciones y responsabilidades al empleado, junto a los términos y condiciones de contratación.
* **Durante la contratación.-** Durante la vida laboral, todo el personal de la entidad deberá recibir una formación y concienciación adecuada y actualizada de las políticas y procedimientos de seguridad, adaptadas según el puesto de trabajo y las necesidades de seguridad que vayan siendo detectadas por parte de los responsables del área al que pertenezca el empleado. La formación debe incluir requisitos de seguridad, responsabilidades legales y controles de negocio, así como formación en el uso correcto de los recursos de tratamiento de la información.
* **Tras finalizar la contratación o el cambio de puesto de trabajo.-** En los casos relacionados con el cese del puesto de trabajo, todos los empleados, contratistas y externos deben devolver todos los activos (componentes software, documentos corporativos y equipos prestados) de la organización que tengan en su posesión y estén relacionados con su empleo. Asimismo, se deberán revocar todos los privilegios al usuario cesado en todos los entornos de producción o accesibles desde el exterior de la organización. En los casos relacionados con el cambio de puesto de trabajo dentro de la organización el Administrador del Sistema deberá revocados todos los privilegios excesivos que el usuario tuviera en el puesto actual respecto al nuevo puesto a desempeñar. ”[[58]](#footnote-58)

##### 2.2.10.5 Seguridad Física y del Entorno. (Cláusula 9).

“El objetivo de este procedimiento es proteger los recursos de tratamiento de la información crítica y sensible de la organización, a través de áreas restringidas y perímetros de seguridad definidos mediante adecuadas barreras de seguridad y controles de entrada. Dentro de este procedimiento es necesario definir:

• Elementos físicos y ambientales a proteger.

• Medidas de protección.

• Roles que intervienen en el proceso.

• Responsabilidades de los roles.

• Elementos a proteger.

• Medidas de protección.

• Documentación y registros a generar.

• Documentación y plantillas de referencia.

Dentro de las medidas principales a realizar para protección de los elementos físicos se encuentran:

**Áreas Seguras:** Prevenir los accesos físicos no autorizados, los daños y las interferencias a las instalaciones de la organización y a la información: accesos sólidos y protegidos a las instalaciones, detección de condiciones ambientales adversas (fuego principalmente), detección de accesos no autorizados (alarmas, sensores de movimientos, cámaras...), medidas de protección de accesos (llaves, tarjetas, lectores de huella...) e información física, etc.

**Definición de Áreas de Trabajo:** En función de la finalidad a la que se destinan los espacios o áreas de trabajo, se pueden establecer los siguientes tipos de áreas: públicas, internas, restringidas, etc.

**Activos de Información:** Debe asegurarse la protección de los activos de la empresa, especialmente los de información: protegiendo los soportes extraíbles, los armarios y cajoneras, no dejando accesible ningún tipo de información clasificada como interna o confidencial, etc.

**Protección de los Sistemas:** Prevenir la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la organización: áreas seguras para servidores de aplicaciones, datos y redes, sistemas SAI para los sistemas clave de la empresa, protección de los sistemas o soportes a extraer fuera de la organización, destrucción de los datos incluidos en soportes a desechar, etiquetado y documentado de equipos y cables, etc.”[[59]](#footnote-59)

##### 2.2.10.6 Gestión de Comunicación y Operaciones. (Cláusula 10).

“El objetivo de este procedimiento es establecer las responsabilidades y procedimientos para la gestión y operación de todos los recursos de información.

* Dentro de este procedimiento es necesario definir:
* Tareas a realizar y periodicidad de las tareas.
* Roles que intervienen en el proceso.
* Responsabilidades de los roles.
* Normas de uso de los recursos lógicos de la empresa.
* Documentación y registros a generar.
* Documentación y plantillas de referencia.

Las áreas prioritarias que deben gestionarse dentro de este procedimiento son:

* **Actualización de los sistemas:** Es clave la correcta gestión de la actualización de los sistemas críticos de la empresa para asegurar su disponibilidad. Son especialmente sensibles a estos cambios son: servidores, aplicaciones de gestión, bases de datos, firewall, redes, etc.
* **Protección de los sistemas frente a código malicioso o descargable:** Es clave proteger los sistemas frente a este tipo de ataques para asegurar su confidencialidad/integridad. Para ello se recurrirá a herramientas antivirus y actualizaciones de los sistemas.
* **Seguridad de las redes:** Es clave proteger las redes y comunicaciones de la organización para asegurar la confidencialidad/integridad/disponibilidad de los datos y sistemas de la empresa. Para ello es necesario implantar algún sistema cortafuegos y definir correctamente las reglas de acceso tanto de entrada como de salida a los sistemas, denegando por defecto todo lo que no esté explícitamente permitido. Especial atención hay que tener en los accesos desde el exterior a los servicios y servidores de la empresa. En caso que sea necesario acceder desde el exterior a estos servicios por un trabajador deben definirse VPN e incluso controlar los equipos a través de reglas que equipos concretos pueden conectarse. Es recomendable a su vez:
  + Realizar revisiones periódicas del material disponible: firewall, enrutadores, conmutadores, cableado, etc.
  + Activar y revisar el visor de sucesos de los sistemas críticos de la empresa de forma periódica. Para facilitar esta tarea es posible utilizar herramientas para monitorización de los sistemas o generar scripts para extraer información resumida de los logs de sistema.
* **Registro de actividades:** Al igual que la monitorización de los sistemas críticos de la empresa puede ser necesario monitorizar el resto de recursos de la empresa: uso de la red, aplicaciones instaladas, inicio y fin de las sesiones de trabajo, acceso y-o modificación de información crítica, etc. En caso de registrar actividades relacionadas de los trabajadores de la empresa es necesario que estos estén informados de forma explícita del uso que puede hacerse de los recursos de la empresa y que la actividad podrá ser monitorizada por la empresa.
* **Copias de seguridad:** Es clave la correcta gestión de las copias de seguridad de la organización para poder asegurar la integridad/disponibilidad de los datos y los sistemas de la empresa. Es necesario definir el qué (elementos a respaldar), el cuándo (con qué frecuencia se realizará), el dónde (lugar de almacenamiento) y el cómo (proceso para realizar el respaldo). Los puntos claves del procedimiento de copias de seguridad deben responder a dichas preguntas, asegurando que:
  + Los datos y sistemas claves de la organización están protegidos: documentos, bases de datos, configuraciones de servidores y servicios, imágenes de sistemas operativos y servidores, Se haga con la suficiente periodicidad, teniendo en cuenta esfuerzo vs riesgo. Algunos datos se copiarán diariamente, otros semanalmente y quizá otros mensual o semestralmente. Se almacenen las copias en lugar seguro. Es habitual que existan al menos dos niveles de copia. Una dentro de las oficinas de la empresa y otra fuera de la oficina.
  + A la hora de realizar las copias hay diversas maneras de hacerlo, cada una con sus pros y contras. Es necesario que la empresa defina el tipo de copia de seguridad que se realizará. Pueden ser incrementales, completas, automatizadas o manuales, también puede realizarse una copia de los datos mediante herramientas de sincronización que solo realiza la copia cuando el fichero ha sido modificado en origen. Es necesario verificar que las copias finalizan correctamente y realizar pruebas de restauración periódicas para verificar que el sistema de respaldo funciona correctamente. Existen diversas aplicaciones software libre para automatizar los backups: rsync, bacula, amanda, etc”[[60]](#footnote-60)

##### 2.2.10.7 Control de Acceso. (Cláusula 11).

“El objetivo de este procedimientos es proteger los sistemas lógicos de la empresa para asegurarse que solo los usuarios definidos tenga acceso lógico a los datos y sistemas.

Todos los sistemas de la empresa dispondrán de un sistema de autenticación de los usuarios, de forma general será a través de usuario y contraseña. Si bien pueden implantarse otros sistemas como son el uso de certificados digitales o tarjetas inteligentes, lectores de huella, etc

* Dentro de este procedimiento es necesario definir:
* Niveles de control de acceso
* Medidas de protección a implantar y tareas a realizar.
* Roles que intervienen en el proceso.
* Responsabilidades de los roles.
* Normas de acceso lógico a los recursos de la empresa.
* Normas para la creación y gestión de contraseñas.
* Documentación y registros a generar.
* Documentación y plantillas de referencia.

Entre las actividades principales a realizar dentro de este procedimiento destacan:

* **Definición de los niveles de acceso:** Los niveles de acceso lógico a los sistemas suelen ser habitualmente tres: red, sistema operativo y aplicación/datos. Para cada uno de los niveles es necesario definir explícitamente, especialmente a nivel de red 10, los recursos que serán controlados.
* **Definición de las medidas técnicas a implantar:** Existen diversas medidas para controlar los accesos, la mayor parte de ellas a través de algún tipo de sistema de autenticación 11: ip/mac[[61]](#footnote-61), usuario y contraseña, certificado o tarjeta inteligente, huella dactilar, token[[62]](#footnote-62) de seguridad, entre otros. A nivel de red existen otro tipo de medidas más allá de la autenticación, como puede ser la segregación de redes, filtrado de conexiones, enrutamiento, etc.
* **Definición de los permisos de acceso:** La definición de los permisos de usuarios debe hacerse mediante roles o grupos, asignando a cada rol o grupo un conjunto de permisos sobre el acceso lógico a los sistemas; cada usuario estará asignado a un rol o grupo. Es recomendable seguir una política de mínimo privilegio (need to know), en función de las necesidades de cada puesto de trabajo.
* **Definición y difusión de políticas de acceso:** Algunas de las políticas básicas que deben definirse son la gestión de contraseñas y las políticas de acceso a datos. Estas políticas deben ser conocidas explícitamente por los empleados. También es habitual que se definan las sanciones por el incumplimiento de estas políticas. A la hora de implantar los niveles de acceso, como ya se ha indicado, se contempla:
* **Acceso a nivel de Red:** Se debe controlar el acceso a los servicios en red, tanto internos (red local) como externos (internet). La empresa debe establecer las políticas que controlen el uso del entorno de red (correo electrónico, navegación web, DNS, etc.), así como las políticas de filtrado de conexiones en los equipos de seguridad perimetral (firewalls).
* **Acceso a nivel de sistema operativo:** Segundo nivel de control de acceso que permite a los empleados utilizar los sistemas operativos de la red.
* **Acceso a nivel de aplicaciones y datos:** Tercer nivel en el control de acceso al sistema de información se debe definir una política de control de acceso de los usuarios para prevenir el acceso no autorizado a la información y a las aplicaciones. En cuanto a la política de contraseñas los principales elementos a tener en cuenta para su correcta gestión son:
  + Contraseñas fuertes: más de 6 u 8 caracteres, incluir números, letras, números y caracteres no habituales.
  + Renovación periódica de las contraseñas.
  + No revelación de las contraseñas.
  + Bloqueo de los equipo cuando no vayan a ser usado.
  + Almacenamiento seguro. No escribir las contraseñas en post-it o papel, no almacenar en los navegadores, no revelar nunca la contraseña a otro usuario, etc En este caso la mejor opción es utilizar una herramienta de gestión de contraseñas.”[[63]](#footnote-63)

##### 2.2.10.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. (Cláusula 12).

“El proceso de adquisición consiste de varios pasos dirigidos a obtener los equipos y los programas de tecnología de información que puedan satisfacer las necesidades de la entidad, a un costo razonable. Mediante este proceso se analizan y se identifican las necesidades a ser atendidas y la forma de atender las mismas.

* Estudio de Necesidades.
* Plan de Desarrollo Tecnológico.
* Desarrollo o Adquisición de Programas y de Otros Componentes de Programación.
* Adquisición de Equipo y Componentes para la Red.
* Solicitud de Propuestas y Contratación.
* Asignación de un Administrador de Proyecto.
* Desarrollo de Portales (Páginas Web) para Proveer la Integración y la Publicación de Transacciones Electrónicas.” [[64]](#footnote-64)

##### 2.2.10.9 Gestión de Incidentes en la Seguridad de la Información. (Cláusula 13).

“El objetivo de la Gestión de Incidencias es resolver de la manera más rápida y eficaz posible, cualquier incidente o no conformidad relacionada con la seguridad de los sistemas. Dentro del procedimiento es necesario definir:

* Fases y actividades a realizar para la gestión de Incidencias.
* Flujo básico de una incidencia:
* Registro, Clasificación, Diagnóstico y Resolución.
* Roles que intervienen en el proceso
* Responsabilidades de los roles.
* Sistema de clasificación de incidencias: niveles de incidencias y criticidad.
* Estructura del registro de incidencias: campos para documentar la incidencia.
* Documentación y registros a generar.
* Documentación y plantillas de referencia.

Este procedimiento puede estar integrado dentro del procedimiento general de gestión de incidencias implantado en la empresa. Debe existir un teléfono de emergencia o persona de contacto para la atención de incidencias que se utilizará siempre que los canales habituales dejen de estar operativos. A continuación se incluyen algunos ejemplos de incidencias de seguridad:

* Pérdida de servicio, equipos o instalaciones
* Fallos o sobrecargas del sistema
* Incumplimiento de políticas o directrices
* Incumplimientos de los acuerdos de seguridad física
* Cambios del sistema no controlados
* Fallos del software o del hardware
* Violaciones de acceso
* Eventos que afecten a la identificación y autenticación de los usuarios
* Eventos que afecten a los derechos de acceso a los datos
* Eventos que afecten a los procedimientos de copias de seguridad y recuperación.
* Incidencias que afecten a la gestión de soportes. “[[65]](#footnote-65)

##### 2.2.10.10 Gestión de la Continuidad del Negocio. (Cláusula 14).

“***Generalidades***: La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo. El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

***Objetivo***: Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro. Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

* Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
* Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
* Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.”[[66]](#footnote-66)

##### 2.2.10.11 Cumplimiento. (Cláusula 15).

“El objetivo de este procedimientos es identificar los requisitos legales, reglamentarios y contractuales de seguridad a los que están sujetos los sistemas de información.

* Dentro del procedimiento es necesario definir:
* Requisitos legales a cumplir.
* Tareas a realizar para cumplir los requisitos legales
* Roles que intervienen en el proceso
* Responsabilidades de los roles.
* Documentación y registros a generar.
* Documentación y plantillas de referencia.

Los principales requisitos legales en el marco de la regulación española son:

* Derechos de propiedad intelectual.
* Protección de los registros y privacidad de la información personal (LOPD)”[[67]](#footnote-67)

# CAPÍTULO 3

## 3. Desarrollo de la Propuesta.

### 3.1 Implementación de la Norma ISO 27001:2005.

#### 3.1.1 Desarrollo de Políticas de Seguridad de la Información.

Para poder gestionar este dominio de control se empleó como instrumento de recopilación de hechos, incidencia y fortalezas la encuesta formal que se aplicó al universo del Departamento de Sistemas de la Empresa ver **Anexo 1;** posteriormente se procedió a realizó un análisis para la interpretación de la tabulación de datos obtenidos.

# CAPÍTULO 4

# CONCLUSIONES

# RECOMENDACIONES

# BIBLIGRAFÍA

# GLOSARIO

# ANEXOS

## Anexo 1: Formatos o Modelos de Encuestas para Estableces Políticas de Seguridad Informática.

**OBJETIVO:** Determinar los requisitos del negocio para proporcionar una guía clara o marco legal de políticas de Seguridad informática que permita mitigar los riesgos en los activos de la información bajando la probabilidad del impacto en los incidentes informáticos.

### Encuesta 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FECHA:** | **17/11/2014** | **ENCUESTA N°:1** | | |
| **DATOS INFORMATIVOS.**  **NOMBRE: ………………………………………………………………………………………...**  **CARGO: …………………………………………………………………………………………..**  **DEPARTAMENTO:……………………………………………………………………………...** | | | | |
| **DOMINIO** | **05** | **Políticas de Seguridad de la Información.** | | |
| 1. **¿Actualmente la Empresa CISEPRO cuenta con Políticas de Seguridad implementadas?** | | | Si ( ) | No ( ) |
| 1. **¿Existen controles para administrar la seguridad de los activos de la información?** | | | Si ( ) | No ( ) |
| 1. **¿Las políticas que se desarrollan dentro de la Organización son de Conocimiento del Talento Humano?** | | | Si ( ) | No ( ) |
| 1. **¿Es conveniente que las Políticas de Seguridad de la Información se mantengan continuamente actualizando?** | | | Si ( ) | No ( ) |
| 1. **¿Para fortalecer un sistema de Seguridad Informático se necesita manejar versiones para el establecimiento de Políticas de Seguridad Informática** | | | Si ( ) | No ( ) |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Firma** | | | | |

### Encuesta 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FECHA:** | **17/11/2014** | **ENCUESTA N°:2** | | |
| **DATOS INFORMATIVOS.**  **NOMBRE: ………………………………………………………………………………………...**  **CARGO: …………………………………………………………………………………………..**  **DEPARTAMENTO:……………………………………………………………………………...** | | | | |
| **DOMINIO** | **06** | **Aspectos Organizativos de la Seguridad.** | | |
| 1. **¿La Empresa de Seguridad Física y Electrónica CISEPRO cuenta con un departamento que se encargue del proceso de Seguridad Informática?** | | | Si ( ) | No ( ) |
| 1. **¿Para administrar la Seguridad Informática la Empresa a contrato servicios de accesoriamente por parte de expertos?** | | | Si ( ) | No ( ) |
| 1. **¿Los servicios de asesoramiento contratados por la Empresa CISEPRO permiten garantizar los principios de Seguridad de la Información (Confiabilidad, disponibilidad e integridad)?** | | | Si ( ) | No ( ) |
| 1. **¿Al adquirir un servicio de asesoramiento profesional pertinente a la Seguridad de la Información, se exige la creación de normativas?** | | | Si ( ) | No ( ) |
| 1. **¿En el intercambio de información con otras entidades la empresa emplea acuerdos de Confidencialidad?** | | | Si ( ) | No ( ) |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Firma** | | | | |

### Encuesta 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FECHA:** | **17/11/2014** | **ENCUESTA N°:3** | | |
| **DATOS INFORMATIVOS.**  **NOMBRE: ………………………………………………………………………………………...**  **CARGO: …………………………………………………………………………………………..**  **DEPARTAMENTO:……………………………………………………………………………...** | | | | |
| **DOMINIO** | **07** | **Gestión de Activos** | | |
| 1. **¿La Empresa CISEPRO cuenta actualmente con un inventario de activos?** | | | Si ( ) | No ( ) |
| 1. **¿El inventario de activos esta automatizado mediante software?** | | | Si ( ) | No ( ) |
| 1. **¿Periódicamente se actualiza el inventario de activos?** | | | Si ( ) | No ( ) |
| 1. **¿Se ha implementado controles en la seguridad del inventario de activos?** | | | Si ( ) | No ( ) |
| 1. **¿El inventario es accesible para el Talento Humano?** | | | Si ( ) | No ( ) |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Firma** | | | | |

### Encuesta 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FECHA:** | **17/11/2014** | **ENCUESTA N°:4** | | |
| **DATOS INFORMATIVOS.**  **NOMBRE: ………………………………………………………………………………………...**  **CARGO: …………………………………………………………………………………………..**  **DEPARTAMENTO:……………………………………………………………………………...** | | | | |
| **DOMINIO** | **08** | **Seguridad Ligada a los Recursos Humanos** | | |
| 1. **¿El Personal de la Empresa reporta los incidentes informáticos al momento que se suscitan, a la autoridad pertinente?** | | | Si ( ) | No ( ) |
| 1. **¿Los usuarios del Sistema SYSCISEPRO notifican los incidentes informáticos al emplear esta herramienta contable al departamento de Sistemas?** | | | Si ( ) | No ( ) |
| 1. **¿Periódicamente se suscitan incidentes en el intercambio de información entre los usuarios del sistema?** | | | Si ( ) | No ( ) |
| 1. **¿Existen Procedimientos para tratar los incidentes informáticos entre los usuarios del sistema?** | | | Si ( ) | No ( ) |
| 1. **¿Existen políticas para mitigar las incidencias informáticas?** | | | Si ( ) | No ( ) |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Firma** | | | | |

1. **CCTV**: Circuito Cerrado de Televisión. [↑](#footnote-ref-1)
2. **Fuente**: Archivo CISEPRO 2014. [↑](#footnote-ref-2)
3. **Fuente**: Archivo CISEPRO 2014. [↑](#footnote-ref-3)
4. 3 [↑](#footnote-ref-4)
5. **Fuente**: Archivo CISEPRO 2014. [↑](#footnote-ref-5)
6. 6 [↑](#footnote-ref-6)
7. **Fuente**: Archivo CISEPRO 2014. [↑](#footnote-ref-7)
8. **Fuente**: Archivo CISEPRO 2014. [↑](#footnote-ref-8)
9. **SIG**: Sistema Integrado de Gestión. [↑](#footnote-ref-9)
10. **SSO**: Salud y Seguridad Ocupacional. [↑](#footnote-ref-10)
11. **PC´s:** Personal Computer, Traducción: Computador Personal. [↑](#footnote-ref-11)
12. **Router**: Dispositivo empleado para proporcionar conectividad a nivel de red, que emplea un mecanismo de enrutamiento de paquetes a nivel 3 del modelo OSI. [↑](#footnote-ref-12)
13. **Switch**: es un dispositivo digital lógico conmutador de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. [↑](#footnote-ref-13)
14. **UPS**: Uninterruptible Power Supply, Traducción: Sistema de alimentación ininterrumpida. [↑](#footnote-ref-14)
15. **PDF:** es un formato de almacenamiento de documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto). Fue inicialmente desarrollado por la empresa Adobe Systems, oficialmente lanzado como un estándar abierto el 1 de julio de 2008 y publicado por la Organización Internacional de Estandarización como ISO 32000-1 [↑](#footnote-ref-15)
16. **IEC**: International Electrotechnical Commission, Traducción: La Comisión Electrotécnica Internacional. [↑](#footnote-ref-16)
17. (BSI, The British Standards Institution 2014, 2009) [↑](#footnote-ref-17)
18. (ISO 27000.es, 2005) [↑](#footnote-ref-18)
19. **Fuente**: http://www.cxo-community.com/articulos/blogs/blogs-metodologia-legislacion/4811-la-leyenda-iso-17799-la-seguridad-de-los-activos-de-informacion-parte-2.html. [↑](#footnote-ref-19)
20. (ISO 27000.es, 2005) [↑](#footnote-ref-20)
21. **Fuente**: http://www.iso-27001-it-security-management.com/. [↑](#footnote-ref-21)
22. **Fuente**: http://www.iso27002.es [↑](#footnote-ref-22)
23. (Cadme Ruiz & Duque Pozo, 2012) [↑](#footnote-ref-23)
24. 23 [↑](#footnote-ref-24)
25. (Cadme Ruiz & Duque Pozo, 2012) [↑](#footnote-ref-25)
26. 25 [↑](#footnote-ref-26)
27. 25 [↑](#footnote-ref-27)
28. (Armas, 2008) [↑](#footnote-ref-28)
29. 28 [↑](#footnote-ref-29)
30. 28 [↑](#footnote-ref-30)
31. (Armas, 2008) [↑](#footnote-ref-31)
32. 31 [↑](#footnote-ref-32)
33. 31 [↑](#footnote-ref-33)
34. 31 [↑](#footnote-ref-34)
35. 31 [↑](#footnote-ref-35)
36. (Armas, 2008) [↑](#footnote-ref-36)
37. 36 [↑](#footnote-ref-37)
38. (Herrera Bravo, 2001) [↑](#footnote-ref-38)
39. (Galarza Ramirez, 2011) [↑](#footnote-ref-39)
40. 39 [↑](#footnote-ref-40)
41. (Jose Antonio, 2003) [↑](#footnote-ref-41)
42. (Armas, 2008) [↑](#footnote-ref-42)
43. (Armas, 2008) [↑](#footnote-ref-43)
44. (Soto Campos , 2004) [↑](#footnote-ref-44)
45. (Jose Antonio, 2003) [↑](#footnote-ref-45)
46. 45 [↑](#footnote-ref-46)
47. (Instituto Interamericano del Niño, 2002) [↑](#footnote-ref-47)
48. **Fuente**: http://deloitteblog.co.za/tag/deloitte-school-of-risk-management/ [↑](#footnote-ref-48)
49. **Fuente**: http://www.abc.es/20111118/tecnologia/abci-diez-consejos-seguridad-informatica-201111181236.html. [↑](#footnote-ref-49)
50. **Fuente**: http://ean.edu.co/index.php?option=com\_content&view=article&id=2597&Itemid=1280 [↑](#footnote-ref-50)
51. (ISO 27000.es, 2005) [↑](#footnote-ref-51)
52. **Fuente:** http://www.iso27000.es/sgsi.html [↑](#footnote-ref-52)
53. **Fuente:** http://www.iso27000.es/sgsi.html [↑](#footnote-ref-53)
54. **Fuente:** http://www.iso27000.es/sgsi.html [↑](#footnote-ref-54)
55. (iso27002.es, 2014) [↑](#footnote-ref-55)
56. (Mifsud, 2014) [↑](#footnote-ref-56)
57. (Rivadavia, 2011) [↑](#footnote-ref-57)
58. (CELSCAM, 2014) [↑](#footnote-ref-58)
59. (CELSCAM, 2014) [↑](#footnote-ref-59)
60. (Buitrago, Bonilla, & Murillo, 2012) [↑](#footnote-ref-60)
61. **IP/MAC**: Internet Protocol/ Media Access Control, Traducción: Protocolo de Internet/ Control de Acceso al Medio. [↑](#footnote-ref-61)
62. **Token:** es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación [↑](#footnote-ref-62)
63. (CELSCAM, 2014) [↑](#footnote-ref-63)
64. (Saldaña, 2006) [↑](#footnote-ref-64)
65. (CELSCAM, 2014) [↑](#footnote-ref-65)
66. (Janices, ICIC, 2012) [↑](#footnote-ref-66)
67. (CELSCAM, 2014) [↑](#footnote-ref-67)