

**UNIVERSIDAD TÉCNICA DE MACHALA**

**UNIDAD ACADÉMICA DE INGENIERÍA CIVIL**

**CARRERA DE INGENIERÍA DE SISTEMAS**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE**

**INGENIERO DE SISTEMAS**

**TÍTULO**

“DESARROLLO DEL PLAN DE SEGURIDAD PARA LOS ACTIVOS DE LA INFORMACIÓN EN BASE A LA NORMA ISO 27002:2013 PARA LA EMPRESA DE SEGURIDAD FÍSICA Y ELECTRÓNICA CISEPRO CIA LTDA EN LA CIUDAD DE MACHALA, AÑO 2015”.

**AUTOR:**

SR. IDROVO CÁRDENAS JUAN CARLOS

**MACHALA – EL ORO – ECUADOR**

**2014**

# TÍTULO:

“Desarrollo del plan de seguridad para los activos de la información en base a la norma ISO 27002:2013 para la Empresa de Seguridad Física Y Electrónica CISEPRO CIA LTDA en la ciudad de Machala, Año 2014”

# FORMULACIÓN 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 27002:2013 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.

**PROBLEMAS ESPECÍFICOS:**

**Problema 1:** Carencia de un plan de seguridad para los activos de la información.

**Problema 2:** Inexistencia de políticas, guías y procedimientos relacionados con la seguridad de la información para la concertar los servicios tecnológicos.

**Problema 3:** Inexistencia de un catálogo categorizado de los activos de información.

**Problema 4:** Desconocimiento de las amenazas y vulnerabilidades en los activos de la información.

**Problema 5:** Carencia de controles efectivos de acceso para usuario de red, sistemas operativos, aplicaciones informáticas, informaciones, conexión móvil entre otros.

# 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, amenazados y susceptibles a riesgos como el suscitado en el 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 desestabilidad el funcionar de las mismas.

En consecuencia la Empresa CISEPRO asume la necesidad de impedir que se susciten estas infiltraciones, uno de los factores más influyentes en esta decisión es la cantidad de información voluminosa que maneja en sus diferentes procesos internos dentro de la organización estructural de la empresa.

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 se otorguen permisos de acceso a este basados en procedimientos que permitan asegurar y proteger el medio. Además debido a la tendencia nómada que existe hoy en día en el estilo de vida del talento humano de la empresa conectados a los sistemas de información casi desde cualquier lugar y a través de cualquier medio y aunque existan convenios de confidencialidad para evitar que los empleados lleven consigo parte del sistema de información fuera de la infraestructura segura de la organización.

# OBJETIVOS GENERALES

* Diseñar un plan de seguridad para los activos de la información en base a la norma ISO 27002:2013

# **OBJETIVOS ESPECÍFICOS**

* Elaborar el plan de seguridad para los activos de la información según la estructura específica de la empresa basada en el estándar ISO 27002:2013.
* Identificar los procesos internos en partiendo del organigrama funcional para determinar la situación actual de la seguridad informática, comunicaciones, bienes informáticos entre otros de la Empresa CISEPRO que permita establecer políticas de seguridad, soporte y gestión continua.
* Clasificar los activos de la información para establecer parámetros de seguridad que permitan prevenir riesgos informáticos.
* Construir una directiva de supervisión en los sistemas de información que permita determinar amenazas y vulnerabilidades de la seguridad de los activos de la información.
* Crear controles de acceso de usuario, red, sistemas operativos, aplicaciones informáticas, informaciones, y conexión móvil que mejore el funcionamiento de los procedimientos para prevenir los riesgos informáticos.

# ÍNDICE

[TÍTULO: II](#_Toc399766959)

[FORMULACIÓN DEL PROBLEMA III](#_Toc399766960)

[JUSTIFICACIÓN. IV](#_Toc399766961)

[OBJETIVOS GENERALES VI](#_Toc399766962)

[OBJETIVOS ESPECÍFICOS VI](#_Toc399766963)

[ÍNDICE VII](#_Toc399766964)

[MARCO REFERENCIAL 10](#_Toc399766965)

[1. Marco Histórico. 10](#_Toc399766966)

[1.1. Antecedentes de la Empresa 10](#_Toc399766967)

[1.2. Misión. 10](#_Toc399766968)

[1.3. Visión. 10](#_Toc399766969)

[1.4. Actividad de la Empresa 10](#_Toc399766970)

[1.5. Política Integrada de Calidad, Seguridad, Salud y Medio Ambiente. 12](#_Toc399766971)

[1.6. Ubicación. 13](#_Toc399766972)

[2. Marco Teórico. 16](#_Toc399766973)

[2.1. Información 16](#_Toc399766974)

[2.2. Activos de Información. 16](#_Toc399766975)

[2.3. Estándares. 16](#_Toc399766976)

[2.4. Organización Internacional para la Estandarización. 16](#_Toc399766977)

[2.5 Seguridad Informática. 16](#_Toc399766978)

[2.6. Importancia de la Seguridad Informática. 17](#_Toc399766979)

[2.7. Variables de la Seguridad Informática. 18](#_Toc399766980)

[2.8. Requerimientos de Seguridad Informática. 19](#_Toc399766981)

[2.9. Principales estándares de seguridad informática. 19](#_Toc399766982)

[3. Marco Conceptual. 24](#_Toc399766983)

[3.1. Elementos de Seguridad. 24](#_Toc399766984)

[3.2. Aspectos organizativos de la seguridad informática. 28](#_Toc399766985)

[3.3. Gestión de la Seguridad Informática. 29](#_Toc399766986)

[3.4. Análisis Estratégico del Riesgo. 29](#_Toc399766987)

[3.5. Plan de Seguridad informática 30](#_Toc399766988)

[3.6. Implementación de Seguridades. 31](#_Toc399766989)

[4. Marco Científico. 32](#_Toc399766990)

[4.1. Políticas de Seguridad (Cláusula 5). 32](#_Toc399766991)

[4.2. Organización de la Seguridad de la Información. (Cláusula 6). 33](#_Toc399766992)

[4.3. Gestión de Activos. (Cláusula 7). 33](#_Toc399766993)

[4.4. Seguridad Ligada a los Recursos Humanos. (Cláusula 8). 33](#_Toc399766994)

[4.4. Seguridad Física y del Entorno. (Cláusula 9). 33](#_Toc399766995)

[4.5. Gestión de Comunicación y del entorno. (Cláusula 10). 33](#_Toc399766996)

[4.6. Control de Acceso. (Cláusula 11). 33](#_Toc399766997)

[4.7. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. (Cláusula 12). 33](#_Toc399766998)

[4.8. Gestión de Incidentes en la Seguridad de la Información. (Cláusula 13). 33](#_Toc399766999)

[4.9. Gestión de la Continuidad del Negocio. (Cláusula 14). 33](#_Toc399767000)

[4.10. Cumplimiento. (Cláusula 15). 33](#_Toc399767001)

[5. Marco Tecnológico. 34](#_Toc399767002)

[Estado Actual 34](#_Toc399767003)

[Diseño metodológico preliminar 34](#_Toc399767004)

[Nombres de las personas que participan en el proceso 34](#_Toc399767005)

[Recursos disponibles (Materiales institucionales y Financieros) 34](#_Toc399767006)

[Cronograma 34](#_Toc399767007)

[Bibliografía. 34](#_Toc399767008)

# **E. MARCO REFERENCIAL**

## 1. Marco Histórico.

### 1.1. Antecedentes de la Empresa

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.

### 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.

### 1.3. Visión.

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

### 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 Circuito Cerrado de Televisión 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

### 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.

### 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



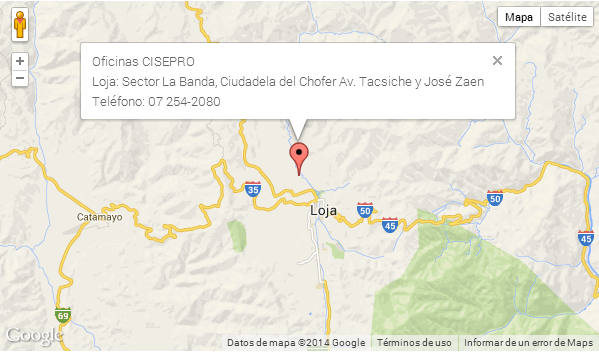
**Sucursal**: Guayas, **Provincia**: Guayas, **Ciudad**: Guayaquil, **Dirección**: Portete y chile esquina, **Teléfono:** 097687941-086895489



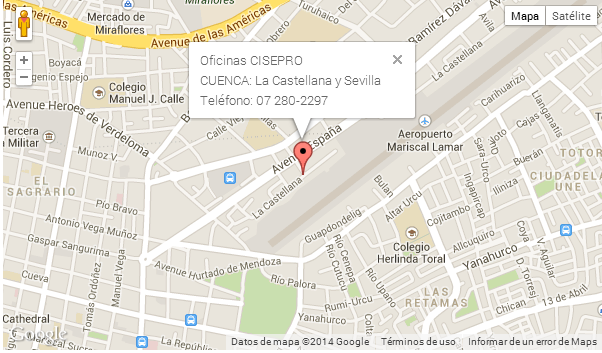
**Sucursal**: Zamora, **Provincia**: Zamora Chinchipe, **Ciudad**: Zamora, **Dirección:** Barrio la Chacra y Avenida del Ejército, **Teléfono:** 072315060



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



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



## 2. Marco Teórico.

### 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. Activos de Información.

Un conjunto de componentes humanos, tecnológicos, hardware, software, entre otros que están ligados al proceso productivo de una empresa.

### 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.

### 2.4. 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 no debieran ser responsables de identificar todos o alguno de dichos de derechos de patente.

### 2.5 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.

### 2.6. 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.

### 2.7. 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.

### 2.8. 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.

### 2.9. Principales estándares de seguridad informática.

***ISO* *17799*:** Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Surgida de la norma británica BS 7799, la norma ISO 17799 ofrece instrucciones y recomendaciones para la administración de la seguridad. La norma 17799 también ofrece una estructura para identificar e implementar soluciones para los siguientes riesgos:

Política de seguridad: escribir y comunicar la política de seguridad de la compañía

Organización de seguridad: definir los roles y las responsabilidades. Monitorear a los socios y a las empresas tercerizadas

Clasificación y control de activos: llevar un inventario de los bienes de la compañía y definir cuán críticos son así como sus riesgos asociados

Seguridad del personal: contratación, capacitación y aumento de concientización relacionadas a la seguridad

Seguridad física y del entorno: área de seguridad, inventarios del equipamiento de seguridad

Comunicación / Administración de operaciones: procedimientos en caso de accidente, plan de recuperación, definición de niveles de servicio y tiempo de recuperación, protección contra programas ilegales, entre otros.

Control de acceso: establecimiento de controles de acceso a diferentes niveles (sistemas, redes, edificios, etc.).

Desarrollo y mantenimiento del sistema: consideración de la seguridad en sistemas desde el diseño hasta el mantenimiento.

Plan de continuidad empresarial: definición de necesidades en términos de disponibilidad, recuperación de tiempo y establecimiento de ejercicios de emergencia

Contratación: respeto por la propiedad intelectual, las leyes y las reglamentaciones de la compañía.

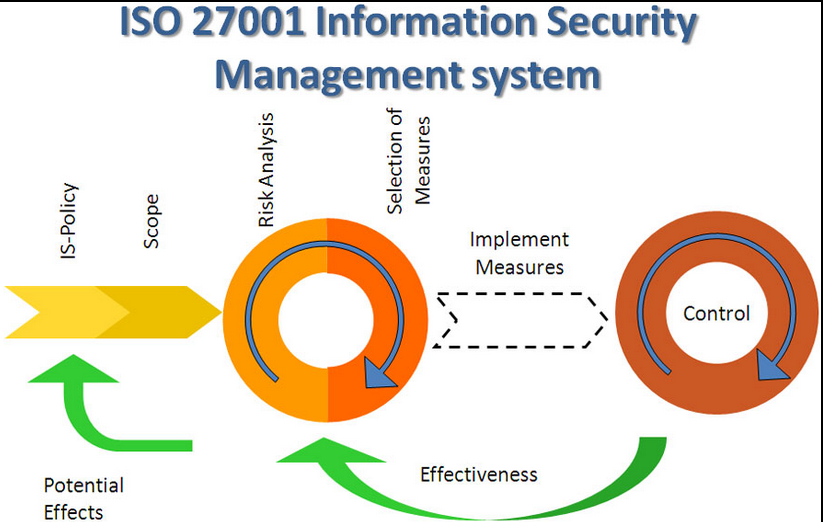


**Figura I: Estándar ISO 17799**

***ISO* *27001*:** La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

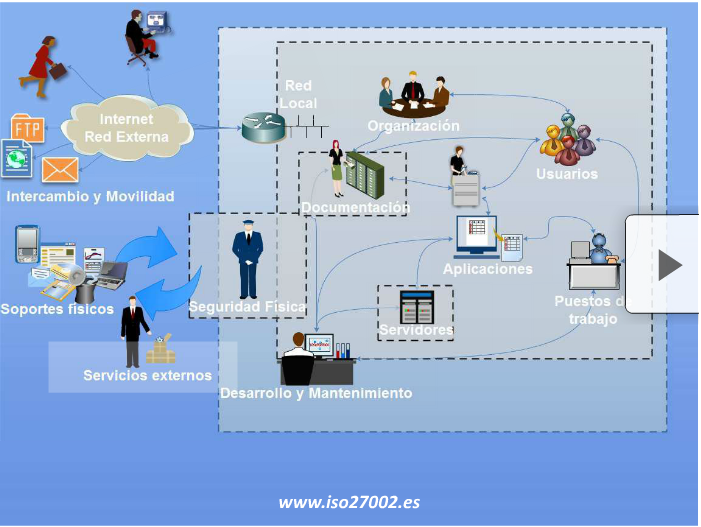
La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma compuesta por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización.

También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible. A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.



**Figura II. Estándar ISO 27002**

**ISO 27002:** es 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 III. Estándar ISO 27002**

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.

## 3. Marco Conceptual.

### 3.1. Elementos de Seguridad.

**Principios de Seguridad:** son las bases fundamentales que debe seguir para alcanzar niveles apropiados de seguridad en un contexto productivo.

**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.

**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.

**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.

**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.

**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.

**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.

**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.

**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.

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.

**Impacto**: Es el resultado de una 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.

**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.

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.

**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 anti-virus
* Firmas Digitales
* Toquen- Electrónicos.
* Seguimientos y análisis de herramientas.
* Fuentes de alimentación redundantes.
* Respaldos de información

**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.

### 3.2. 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.

### 3.3. 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.

### 3.4. 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.

### 3.5. 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.

### 3.6. 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.

## 4. Marco Científico.

Según la normativa ISO 27002:20013 se establece las siguientes clausulas o marco referencial para aplicar un plan de seguridad de activos de información:

### 4.1. 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.

### 4.2. Organización 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.” (Mifsud, 2014)

### 4.3. 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.” (Rivadavia, 2011)

### 4.4. 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:

1) 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.

2) 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.

3) 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. ” (celscam, 2014)

### 4.4. 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.” (celscam, 2014)

### 4.5. Gestión de Comunicación y del entorno. (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 sistema 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”

### 4.6. 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, usuario y contraseña, certificado o tarjeta inteligente, huella dactilar, token de seguridad, etc.

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 de GRUPO AMIAB. 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.” (celscam, 2014)

### 4.7. 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.

1. Estudio de Necesidades.
2. Plan de Desarrollo Tecnológico.
3. Desarrollo o Adquisición de Programas y de Otros Componentes de Programación.
4. Adquisición de Equipo y Componentes para la Red.
5. Solicitud de Propuestas y Contratación.
6. Asignación de un Administrador de Proyecto.
7. Desarrollo de Portales (Páginas Web) para Proveer la Integración y la Publicación de Transacciones Electrónicas.” (Saldaña, 2006)

### 4.8. 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. “ (celscam, 2014)

### 4.9. 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:

a) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.

b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán” (Janices, 2012)

### 4.10. 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)” (celscam, 2014)

## 5. Marco Tecnológico.

## 6. Estado Actual

# F. DISEÑO METODOLÓGICO PRELIMINAR

El marco metodológico preliminar para elaborar el plan de seguridad para los activos de la información para la Empresa de Seguridad Física y Electrónica CISEPRO CIA LTDA se base a los 14 dominios de la norma ISO 27002:2013.

1. POLÍTICAS DE SEGURIDAD.
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
4. GESTIÓN DE ACTIVOS.
5. CONTROL DE ACCESO.
6. CIFRADO.
7. SEGURIDAD FÍSICA Y AMBIENTAL.
8. SEGURIDAD EN LA OPERATIVA.
9. SEGURIDAD EN LAS TELECOMUNICACIONES.
10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
11. RELACIONES CON SUMINISTRADORES.
12. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14. CUMPLIMIENTO.

Destacando los aspectos clave de la actualización de esta norma:

**Fundamentales**

* Compromiso y apoyo de la Dirección de la organización.
* Definición clara de un alcance apropiado.
* Concientización y formación del personal.
* Evaluación de riesgos exhaustiva y adecuada a la organización.
* Compromiso de mejora continua.
* Establecimiento de políticas y normas.
* Organización y comunicación.
* Inclusión de la cláusula o dominio gestión de incidentes de seguridad

# Factores críticos de éxito.

# La concientización del empleado por la seguridad. Principal objetivo a conseguir.

# Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.

# Creación de un sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).

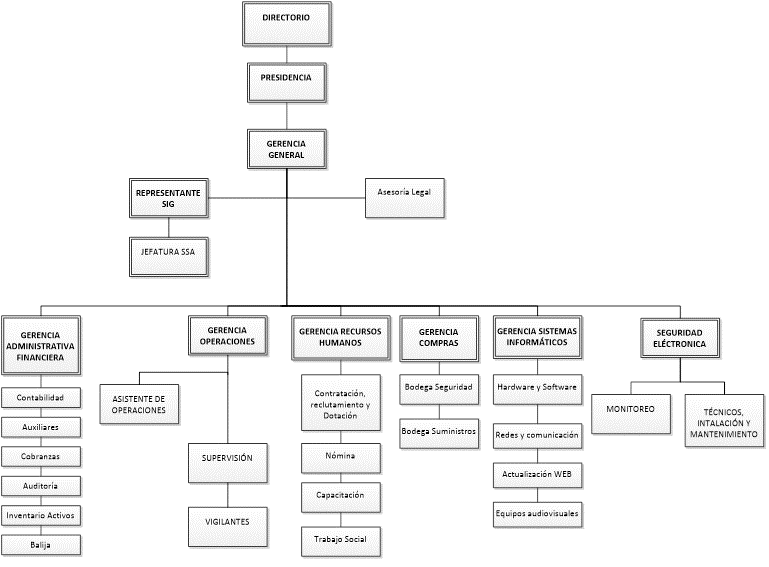
# La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.

# La seguridad no es un producto, es un proceso.

# La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.

# La seguridad debe ser inherente a los procesos de información y de la organización.

# G. NOMBRES DE LAS PERSONAS QUE PARTICIPAN EN EL PROCESO.



**Figura IV: Organigrama Estructural.**

|  |  |
| --- | --- |
| **EMPRESA CISEPRO CIA LTDA** | |
| **CARGO** | **NOMBRES** |
| **PRESIDENTE** | Mayor (r). José Ignacio Navarrete Landázuri. |
| **GERENTE GENERAL** | Ing. José Ignacio Navarrete Madero. |
| **REPRESENTANTE SIG** | Ing. Karen Viviana Navarrete Madero |
| **ASESORÍA LEGAL** | CPA. Guillermo Fernández. |
| **GERENCIA ADMINISTRATIVA FINANCIERA** | Ing. María Belén Armijos |
| **GERENCIA DE OPERACIONES.** | Ec. Pedro Medrano. |
| **GERENCIA DE RECURSOS HUMANOS** | Ing. Karen Viviana Navarrete Madero |
| **GERENCIA DE COMPRAS** | Ing. Karla Navarrete Madero. |
| **GERENCIAS DE SISTEMAS INFORMÁTICOS** | Ing. Jorge Raül Aguirre Vega. |
| **SEGURIDAD ELECTRÓNICA** | Ing. Jorge Raül Aguirre Vega. |

|  |  |
| --- | --- |
| **DEPARTAMENTO DE SISTEMAS** | |
| **HARDWARE Y SOFTWARE** | Ing. Alex Patricio Galarza. |
| **REDES Y COMUNICACIÓN** | Ing. Alex Patricio Galarza. |
| **PAGINA WEB** | Ing. Jorge Raül Aguirre Vega. |
| **SOPORTE TÉCNICO** | Ing. Jorge Raül Aguirre Vega. |

|  |  |
| --- | --- |
| **DESARROLLO DEL PROYECTO** | |
| **DOCENTE AVAL** | **Ing. Rodrigo Fernando Morocho Román.** |
| **ESTUDIANTE INVESTIGADOR** | **Sr. Juan Carlos Idrovo Cárdenas** |

# RECURSOS DISPONIBLES.

## MATERIALES INSTITUCIONALES.

El equipo de trabajo para llevar a cabo desarrollo del plan de seguridad para los Activos de la Información en BASE a la Norma ISO 27002:2013 para la empresa de Seguridad Física y Electrónica CISEPRO CIA LTDA en la ciudad de Machala está conformado de la siguiente forma:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N° DE PERSONAS** | **ROL** | **NOMBRE** | **FUNCIÓN** | **REPRESENTACIÓN GRÁFICA** |
| 1 | Jefe de SGCI | Ing. Karen Navarrete Madero  **Gerente de Recursos Humanos** | Lider | **C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0287005.wmf** |
| 1 | Jefe de Sistemas | Ing. Jorge Aguirre Vega  **Asesor SGCI** | Líder  Asesor | C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0195812.wmf |
| 1 | Investigador | Ing. Juan Carlos Idrovo.  **Analista de Sistemas.** | Diseñador | C:\Program Files (x86)\Microsoft Office\Media\CntCD1\ClipArt2\j0215476.wmf |

###### 

###### MATERIALES FINANCIEROS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ESTIMACIÓN DE COSTOS** | | | | |
| **HARDWARE (A)** | | | | |
| **Cantidad** | **Descripción** | **Valor Unitario** | **Valor Total** | **Iva** |
| 1 | Laptop Inspiron 1764 core i5, 4gb disco 500gb, 18.5 pulgadas LED, mouse wifi. | $1200 | $1200 | si |
| 1 | Comprobador de Cableado | $50 | $50 | si |
| 1 | Ponchadora | $50 | $50 | si |
| 1 | Celular Sansung Galaxy S3 | $700 | $700 | si |
| 1 | Multimetro | $30 | $30 | si |
| 1 | Impresora Epson L310 | $350 | $350 | Si |
| 1 | Metro | $15 | $15 | Si |
| Total A: | | | $2395 |  |
| **SOFTWARE (B)** | | | |  |
| **Cantidad** | **Descripción** | **Valor Unitario** | **Valor Total** | **IVA** |
| 1 | Microsoft Office 2013 | $160 | $160 | **SI** |
| 1 | Microsoft Windows 8.1 | $200 | $200 | **SI** |
| 1 | Microsoft Proyect 2013 | $160 | $160 | **SI** |
| 1 | Wireshark | $0 | $0 | **NO** |
| 1 | Autocad 2014 | $300 | $300 | **SI** |
| 1 | Clonezilla | $0 | $0 | **NO** |
| 1 | Ubuntu | $0 | $0 | **NO** |
| Total B: | | | $820 | **NO** |
| **OTROS (C)** | | | |  |
| **Cantidad** | **Descripción** | **Valor Unitario** | **Valor Total** | **iva** |
| 200 | Horas de Internet | $1 | $200 | Si |
| 4 | Esferos | $0.50 | $2 | SI |
| 30 | Resmas de Papel | $4.50 | $135 | SI |
| 1 | GUIA ISO 27001 | $400 | $400 | SI |
| 1 | TUTOR | $200 | $200 | SI |
| Total C: | | | $937 |  |
| Total=Total A+Total B+Total C | | | $4470 |  |
| **Imprevistos 8%** | | | $357.60 |  |
| **TOTAL DEL PROYECTO** | | | $4827.60 |  |

# CRONOGRAMA

# J. BIBLIOGRAFÍA.