UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

ANALISIS Y EVALUACION DEL RIESGO DE LA INFORMACION BASADO EN ISO/IEC 27001:2005

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Andrés Arancibia Rojas
Profesor Guía : Roberto Caru Cisternas

Santiago – Chile
Septiembre, 2015

Dedicatoria

Este trabajo se lo dedico a mis padres y hermanos, sin quienes jamás habría alcanzado todas las metas que hasta ahora he visto en mi vida y también en forma muy especial a mi prometida futura esposa, quien fue mi apoyo fundamental en este proceso.

Agradecimientos

Agradezco infinitamente y primeramente a Dios y sus milagrosas manifestaciones, que me permitieron seguir cuando todo me decía que no. A mis padres y hermanos, por su constante amor, comprensión y apoyo incondicional siempre.

ÍNDICE

1.0 INTRODUCCION

La Empresas PYME hoy en día desconocen el grado de vulnerabilidad al cual se encuentran expuestas, y no valoran en su real medida todos los activos de información que poseen.

Cada día son más frecuentes los robos de contraseñas, pérdida de datos e información confidencial, las cuales representan sólo algunas de las consecuencias que pude sufrir una empresa, si no le dedica la atención y tiempo necesario a su seguridad informática.

Existen varias alternativas que ayudan a las Organizaciones a evaluar el nivel de seguridad de la información que poseen, tales como normativas, metodologías, aplicativos y herramientas en línea. Muchas o casi todas estas alternativas están sólo disponibles en otros idiomas, o bien, están diseñadas para satisfacer las normativas legales del país donde fueron diseñadas, y en ese aspecto no siempre se pueden aplicar en un ciento por ciento.

En la presente Tesis se ha elegido para evaluar los riesgos de seguridad de la empresa la normativa ISO 27001, la cual está en español, es genérica en todos sus aspectos, por lo cual se puede amoldar y aplicar a cualquier Organización independiente de la Legislación del país que la rige.

Se pretende medir el nivel de seguridad de una Empresa PYME, aplicando para ello la ISO 27001:2005, para demostrar que el grado de vulnerabilidad y posibles ataques a la Empresa es alto, y con ello conseguir que la Gerencia tome conciencia de esta situación, y por ende, asuma un grado de maduración frente al tema que permita a futuro implementar un plan para elevar el nivel de seguridad a unos grados aceptables y de esta manera no poner en riesgo algo tan vital para la Organización como lo es la continuidad del negocio de la misma.

1.1 Motivación

Al egresar de la carrera, los conocimientos adquiridos permiten identificar los vacíos que existen en el resguardo y protección de la información, así como también la relevancia que ésta tiene como activo principal de la Organización.

La motivación se basa en aplicar los conocimientos adquiridos y concientizar a la gerencia de la Organización de la importancia de tomar medidas que apoyen la aplicación de políticas de seguridad de la información al interior de la misma, y al mismo tiempo, crear conciencia en el personal de la Organización de la importancia que esta reviste.

1.2 Justificación

Los activos de información son recursos que representan una gran importancia y costos vitales para las organizaciones. Si estos activos llegaran a fallar o tener algún daño, quedaría fuera de línea el negocio y esto implica poner en riesgo incluso la continuidad del mismo. Lo anterior implica que para tomar las acciones apropiadas en Seguridad de la información, estas decisiones deben estar basadas y de acuerdo primero con los objetivos organizacionales, y equilibradas en los costos de implementación versus el daño probable del resultado de fallas en la seguridad.

En la presente Tesis, se medirá el grado de vulnerabilidad de la organización, tomando para ello como base los once dominios a los cuales hace referencia la normativa ISO / IEC 27001:2005. Lo anterior le permitirá a la empresa la toma de decisiones inherentes a los riegos descubiertos mediante el análisis que se efectuará.
En lo sucesivo, cuando se indique “ISO 27001”, nos estaremos refiriendo a la norma ISO/IEC 27001:2005. Del mismo modo, cuando nos refiramos a “ISO 27002”, estaremos haciendo referencia a la Norma ISO/IEC 27002:2005.

1.3 Hipótesis

Se pretende demostrar que el grado de vulnerabilidad, ataques y amenazas a los activos de la Organización es alto, y eso conlleva a niveles de riesgo que ponen en peligro la continuidad del negocio que estas llevan a cabo.

1.4 Objetivo General

- Poner en antecedentes a la Gerencia de la Empresa de los riesgos que implica el no contar con políticas adecuadas para el resguardo apropiado de la información de esta. Lo anterior, sustentado en el análisis y evaluación de riesgo que se efectuará.

1.5 Objetivos Específicos

- Entender la norma ISO 27001, su enfoque, y forma de aplicabilidad en el contexto de la presente tesis.

- Comprender los beneficios de implementar políticas de seguridad en base a la norma ISO 27001.

- Comprender y entender las buenas prácticas en Seguridad de la información, contempladas en la norma ISO 27002.

- Generar un estudio de análisis y evaluación de riesgo de la Información en base a la Normativa ISO 27001.

1.6 Alcances

- Efectuar análisis y evaluación de riesgo de la seguridad de la información de la Empresa.

- Obtención de resultados del análisis y evaluación de riesgos de la Información de la Empresa.

- Tabulación de los resultados obtenidos en gráfica tipo radar con informe gerencial.

2.0 MARCO TEÓRICO REFERENCIAL

2.1 ¿Qué es la seguridad?

La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen.

La seguridad está finamente ligada a la certeza. Para entender esta definición, hay que aclarar que no existe la seguridad absoluta, más bien, lo que se intenta es minimizar el impacto y/o riesgo. Por tal motivo, cuando hablamos de seguridad, debemos hacerlo en término de niveles, y lo que se intenta y se debe hacer es llevar a cabo una organización efectiva a fin de lograr llegar a los niveles más altos.

La técnica para llegar a una correcta organización está sustentada en cuatro pilares que hacen que la información se encuentre protegida. La seguridad de la información está basada en resguardar o proteger estos cuatro aspectos:

a) **La confidencialidad:** La información puede ser accedida únicamente por las personas que tienen autorización para hacerlo.

b) **La integridad:** Cuando nos referimos a integridad, queremos decir que estamos totalmente seguros de que la información no ha sido borrada, copiada o alterada, no sólo en su trayecto, sino también desde su origen.

c) **La disponibilidad**: En este punto se hace referencia al método de precaución contra posibles daños tanto en la información como en el acceso a la misma: ataques,

accidentes o, simplemente, descuidos que pueden ser factores que obligan a diseñar métodos para posibles bloqueos.

d) **La autenticidad:** Algunos profesionales de la seguridad no incluyen este ítem cuando hablan de los pilares, sino que sólo nombran los tres anteriores. Particularmente creemos que no se puede soslayar este concepto, debido al hecho de que integridad nos informa que un registro de una BD no ha sido modificado ni editado, y la autenticidad nos informa que el registro en cuestión es real.

Aparte de los aspectos mencionados, pueden estar también involucradas otras propiedades como la Responsabilidad, No-repudio y Confiabilidad.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor de amenazas y vulnerabilidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en videos o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales

y funciones de software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

2.1.1 ¿Es necesaria la Seguridad de la Información?

La información, los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad, disponibilidad y autenticidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones, sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben

implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

2.1.2 ¿Qué necesitamos proteger?

Cuando hablamos de seguridad informática muchas veces se confunde diciendo seguridad de Internet, y estos términos no son sinónimos. Informática comprende otro contexto, como la seguridad física, mientras Internet sólo se limita a hablar del entorno a que se refiere. Por tales motivos, la seguridad informática intenta proteger cuatro elementos:

a) **Hardware**: El hardware se encuentra compuesto por el conjunto de elementos físicos del sistema informático.
b) **Software:** El software consiste en el conjunto de sistemas lógicos que hacen funcional al hardware, tales como el Sistema Operativo, aplicaciones, programas, utilitarios, etc.
c) **Datos:** Conjunto de sistemas lógicos que tienen como función manejar el software y el hardware (registros, entradas en BD, paquetes en la red, etc.)
d) **Elementos fungibles**: Son elementos que se gastan o se desgastan con el uso continuo (impresoras, DVDs, insumos en general). Algunos administradores de seguridad no consideran estos elementos para protegerlos, pero en la realidad forman parte de lo que se debe cuidar.

2.1.3 ¿De qué nos protegemos?

Esta pregunta es tan amplia como su respuesta. Hay muchas clasificaciones que van variando según los autores e investigadores del tema, pero la gran mayoría tiene un punto de vista en común: “nos protegemos de las personas”.

A esta altura de los tiempos y con las sociedades que evolucionan, suena raro decir que nos estamos cuidando de nosotros mismos y, más aun sabiendo que esos elementos que protegemos son, en su mayoría, cosas creadas por nosotros. El factor más importante que incita a las personas a cometer actos en contra de los cuatro pilares (integridad, disponibilidad, confidencialidad y autenticidad), es sin duda, el poder. Este poder reside en los datos y en la información.

2.1.4 Conceptos principales en Seguridad de la Información

- **Seguridad Informática:** es el área de la informática que tiene como objetivo proteger la infraestructura computacional incluyendo la información contenida. Actualmente existen protocolos, estándares, reglas, métodos y leyes que permiten minimizar riesgos de la infraestructura o de la información. La Seguridad informática abarca software, bases de datos, metadatos, archivos y todo lo que la organización valore como activo y signifique un riesgo, es decir, en cuanto al tipo de información que se conoce como privilegiada o confidencial.

- **Política:** Intención y dirección general expresada formalmente por la gerencia.

- **Seguridad de la Información:** se entiende por seguridad de la información a todas aquellas medidas preventivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, integridad y disponibilidad de la

información; además, también puede involucrar otras propiedades de las ya mencionadas, como autenticidad, responsabilidad, no repudio y confiabilidad.

2.2 Qué es una ISO/IEC

Es un estándar, una norma, publicada por la Comisión Electrónica Internacional (IEC) y la Organización Internacional para la Estandarización (ISO).

2.2.1 Historia de la ISO

La Organización Internacional de Normalización o ISO (del griego, ἴσος (isos), 'igual'), nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

La ISO es una red de los institutos de normas nacionales de 164 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra (Suiza) que coordina el sistema. La Organización Internacional de Normalización (ISO), con sede en Ginebra, está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento.

Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país. El contenido de los

estándares está protegido por derechos de copyright y para acceder a ellos el público corriente debe comprar cada documento.

Está compuesta por representantes de los organismos de normalización (ON) nacionales, que produce diferentes normas internacionales industriales y comerciales. Dichas normas se conocen como normas ISO y su finalidad es la coordinación de las normas nacionales, en consonancia con el Acta Final de la Organización Mundial del Comercio, con el propósito de facilitar el comercio, el intercambio de información y contribuir con normas comunes al desarrollo y a la transferencia de tecnologías.

La Organización ISO está compuesta por tres tipos de miembros:

- Miembros simples, uno por país, recayendo la representación en el organismo nacional más representativo.

- Miembros correspondientes, de los organismos de países en vías de desarrollo y que todavía no poseen un comité nacional de normalización. No toman parte activa en el proceso de normalización pero están puntualmente informados acerca de los trabajos que les interesen.

- Miembros suscritos, países con reducidas economías a los que se les exige el pago de tasas menores que a los correspondientes.

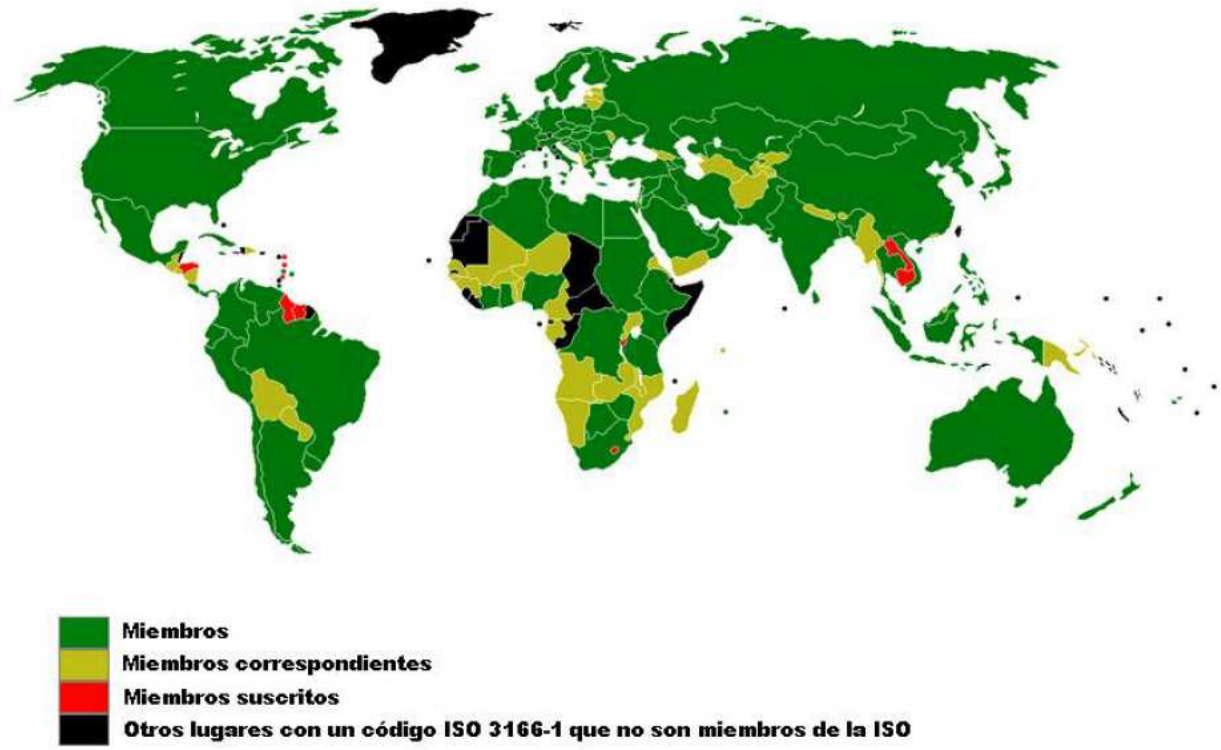


Imagen 2.1 – Presencia de la ISO a nivel mundial

2.2.2 Organización de la ISO

El trabajo de ISO es muy descentralizado, se lleva a cabo mediante una jerarquía de unos 2850 comités, trabajos en grupo y otros subcomités. En estos comités los representantes de las industrias, consumidoras, autoridades gubernamentales y organizaciones internacionales de todo el mundo trabajan juntos con el fin de obtener una resolución con todos de acuerdo de los problemas de estandarización a nivel global.

2.2.3 Visión global de la ISO en la actualidad

La ISO considera los siguientes puntos:

a) Mejora de la calidad, seguridad, medio ambiente y protección de los consumidores, así como el uso racional de los recursos naturales.
b) Difusión global de las tecnologías y de las buenas prácticas.
c) Contribuir al progreso económico y social.

A través de la red y la colaboración de sus miembros de los organismos nacionales, enlaces internacionales, la cooperación regional y las organizaciones asociadas, ISO constituye una plataforma líder para la producción de mercado de referencia a nivel mundial y estándares internacionales. Los mecanismos de ISO, la creación de consenso, la cobertura multi-sectorial y la capacidad de difundir de manera eficiente y promover su gama de productos son mundialmente reconocidos.

2.3 Normativas que conforman la ISO Serie 27000

A semejanza de otras normas ISO, la ISO 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044, las cuales se detallan a continuación:

- **ISO/IEC 27000:** Publicada el 1 de Mayo de 2009. Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del proceso Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000.

- **ISO/IEC 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifica por auditores externos los SGSIs de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

- **ISO/IEC 27002:** Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005

- **ISO/IEC 27003:** Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO/IEC 27004:** Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

- **ISO/IEC 27005:** Publicada el 4 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- **ISO/IEC 27006:** Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- **ISO/IEC 27007:** Publicada en 2011. Consiste en una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

- **ISO/IEC 27008:** Publicada en 2011. Consiste en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

- **ISO/IEC 27010:** Publicada en 2012. Es una norma en 2 partes, que consistirá en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.

- **ISO/IEC 27011:** Publicada el 15 de Diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información

en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU.

- **ISO/IEC 27012:** Publicada en 2011. Consiste en un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

- **ISO/IEC 27013:** Publicada en 2012. Consiste en una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

- **ISO/IEC 27014:** Publicada en 2012. Consiste en una guía de gobierno corporativo de la seguridad de la información.

- **ISO/IEC 27015:** Publicada en 2012. Consiste en una guía de SGSI para organizaciones del sector financiero y de seguros.

- **ISO/IEC 27031:** Publicada en 2011. Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- **ISO/IEC 27032:** Publicada en 2011. Consiste en una guía relativa a la ciberseguridad.

- **ISO/IEC 27033:** Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales; 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de redes de referencia; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP; 27033-7, redes inalámbricas.

- **ISO/IEC 27034:** Publicada en 2010. Consiste en una guía de seguridad en aplicaciones informáticas.

- **ISO/IEC 27035:** Publicada en 2011. Consiste en una guía de gestión de incidentes de seguridad de la información.

- **ISO/IEC 27036:** Publicada en 2012. Consiste en una guía de seguridad de outsourcing (externalización de servicios).

- **ISO/IEC 27037:** Publicada en 2012. Consiste en una guía de identificación, recopilación y preservación de evidencias digitales.

- **ISO 27799:** Publicada el 12 de Junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

2.3.1 Beneficios de la ISO Serie 27000

- Garantía de los controles internos y cumplimiento de requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Pone de manifiesto el respeto a las leyes y normativas que sean de aplicación.
- Fiabilidad de cara al cliente demostrando que la información está segura.
- Identificación, evaluación y gestión de riesgos.
- Evaluaciones periódicas que ayudan a supervisar el rendimiento y las posibles mejoras.
- Se integra con otros sistemas de gestión

- Reducción de costos y mejora de procesos
- Aumento de la motivación y satisfacción del personal al contar con unas directrices claras.

Día a día son más las organizaciones que se interesan por obtener certificaciones en este tipo de normas, requisito que les permite competir con otras entidades, consiguiendo un mejor posicionamiento y por ende capacidad de negociación con clientes que piden que sus proveedores estén certificados.

2.3.2 ISO/IEC 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 redactada 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.

2.3.2.1 Beneficios que entrega la Norma ISO 27001

Evidentemente, el hecho de utilizar la norma ISO 27001 u obtener su certificación, no prueba que la organización sea 100 % segura. A decir verdad, la seguridad completa no existe a menos de una inactividad total. No obstante, la adopción de la norma internacional proporciona innegablemente ventajas que todo buen gerente debería tener en cuenta.

- **Aspecto Organizacional**

  Compromiso: el registro permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles y probar la diligencia razonable de sus administradores.

- **Aspecto Legal**

  Conformidad: el registro permite demostrar a las autoridades competentes que la organización observa todas las leyes y normativas aplicables. En este aspecto, la norma es complementaria de otras normas y legislaciones ya existentes, por ejemplo HIPAA, Privacy Act of 1974, Computer Security Act of 1987, National Infrastructure Act of 1996, Gramm-Leach-Bliley Act of 1999, Government Information Security Reform Act of 2001.

- **Aspecto Funcional**

  Gestión de los riesgos: obtención de un mejor conocimiento de los sistemas de información, sus fallas y los medios de protección. Garantiza también una mejor disponibilidad de los materiales y datos.

- **Aspecto Comercial**

  Credibilidad y confianza: los socios, los accionistas y los clientes se tranquilizan al constatar la importancia que la organización concede a la protección de la información. Una certificación también puede brindar una diferenciación sobre la competencia en el mercado. Algunas licitaciones internacionales ya comienzan a pedir una gestión ISO 17799.

- **Aspecto Financiero**

  Reducción de los costos vinculados a los incidentes y posibilidad de disminución de las primas de seguro.

- **Aspecto Humano**

  Mejora la sensibilización del personal a la seguridad y a sus responsabilidades en la organización.

Una empresa certificada con la norma técnica ISO/IEC 27001 puede ganar frente a los competidores no certificados. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa certificada. Además una empresa certificada tendrá en cuenta lo siguiente:

a) Mayor seguridad en la empresa.
b) Planeación y manejo de la seguridad más efectivo.
c) Alianzas comerciales y e-commerce más seguras.
d) Mayor confianza en el cliente.
e) Auditorias de seguridad más precisas y confiables.
f) Menor Responsabilidad civil.

2.3.2.2 Ventajas de implementar la Norma ISO 27001

La implementación de la norma ISO/IEC 27001 proporciona las siguientes ventajas:

- Reduce el impacto de los riesgos, que en caso de materializarse las amenazas, puedan representar pérdidas (de capital, de facturación, de oportunidades de negocio, por reposición de los daños causados, reclamaciones de clientes, sanciones legales, etc), al aumentar la seguridad efectiva de los sistemas de información, con una mejor planificación y gestión de la seguridad.

- Garantías de continuidad del negocio basándose en el Plan de Contingencias.

- Mejora de la imagen de la organización y aumento del valor comercial de la empresa y sus marcas.

- Incremento de los niveles de confianza de clientes, proveedores, accionistas y socios.

- Mejora del retorno de las inversiones, al tener mejor criterio según los riesgos residuales aceptados y ahorro de tiempo y dinero al reducir o eliminar actividades o inversiones de escasa o nula aplicabilidad a los niveles de riesgo identificados en el negocio.

- Cumplimiento de la legislación y normativa vigentes, tales como de Protección de datos de Carácter personal, de Servicios de la Sociedad de la Información o de Propiedad Intelectual.

2.3.3 ISO/IEC 27002

La norma ISO/IEC 27002 contiene las recomendaciones para el aseguramiento de la información que se basan en las mejores prácticas de seguridad, esta norma es

una evolución del estándar británico BS 7799 en su primera versión, no es certificable pero debe ser adoptado por las organizaciones que quieran obtener la certificación ISO/IEC 27001:2005; cubre aspectos como el manejo de equipos, la administración de políticas, los recursos humanos y los aspectos legales entre otros. Esta norma está conformada por 11 dominios, 39 objetivos de control en donde constan los 133 controles recomendados para la seguridad de la información. Los dominios son los siguientes:

- **Política de seguridad:** proporciona a la gerencia la dirección y soporte para la seguridad de la información.

- **Organización de la seguridad de la información:** La organización interna, tiene como objetivo manejar la seguridad de la información y mantener la seguridad de la información y los medios de procesamiento de información de la organización.

- **Gestión de activos**: El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

- **Seguridad de los recursos humanos:** Contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.

  El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

- **Seguridad física y ambiental**: Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

- **Gestión de comunicaciones y operaciones:** Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

- **Control de acceso:** Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

- **Sistemas de información, adquisición, desarrollo y mantenimiento:** La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

- **Gestión de incidentes de seguridad de la información:** Recomienda trabajar con reportes de los eventos y debilidades de la seguridad de la información.

- **Gestión de la continuidad del negocio:** Desarrollo de planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales en caso de alguna falencia.

- **Conformidad:** Prioriza el cumplimiento de requisitos legales para evitar violaciones a cualquier ley, regulación estatutaria, reguladora o contractual, y cualquier requerimiento de seguridad.

La medición y evaluación de la presente tesis será en base a la normativa ISO 27001 y 27002, las cuales establecen los dominios, objetivos de control y controles, los cuales están resumidos a continuación:

Objetivos de Control y Controles

Nº	Dominio	Objetivos	Controles
5	Política de Seguridad	1	2
6	Organización de la seguridad de la información	2	11
7	Gestión de activos	2	5
8	Seguridad de RR.HH.	3	9
9	Seguridad física y ambiental	2	13
10	Gestión de comunicaciones y operaciones	10	32
11	Control de acceso	7	25
12	Adquisición, desarrollo y mantenimiento de sistemas	6	16
13	Gestión de incidentes de seguridad de la información	2	5
14	Gestión de la continuidad comercial	1	5
15	Conformidad	3	10
Totales		**39**	**133**

Imagen 2.2 - Objetivos de Control y Controles de la Norma ISO/IEC 27002

2.3.3.1 Trazabilidad en la ISO 27002:2005

De acuerdo al análisis anterior, debemos profundizar sobre el concepto de trazabilidad. La trazabilidad es un concepto relevante relacionado con la Seguridad de la Información. Tener en cuenta la trazabilidad o el tracking consiste en preocuparse sobre el propio ciclo de vida de la información y los activos que la contienen y gestionan, sobre la huella de sus acciones, sobre su ciclo de vida. De esta manera es importante por ejemplo de dónde viene un disco duro, dónde va una persona que sepa información de nuestra Organización, o quién introdujo aquel registro. En la norma ISO 15489-1:2001 se cita la trazabilidad como un valor fundamental en la seguridad de la información: ***"Creación, incorporación y conservación de información sobre el movimiento y uso de documentos (activos)"***, algo que paradójicamente, La ISO 27001 no cita textualmente en ningún momento.

Hoy en día en un entorno de proveedores y suministradores cada vez más difuso, la trazabilidad es todavía más importante. Por ello no vendría mal aumentar los 133 controles existentes en la ISO 27001 para enfatizar esta característica en el sistema de gestión de Seguridad de la Información, SGSI. Cierto es que dicha propiedad se encuentra inherente en la implementación de los controles, pero es conveniente darle mayor importancia a dicho concepto.

Sobre los 133 controles de ISO 27001 la realidad es que pocas Organizaciones han ampliado o dado más importancia al tema de la trazabilidad, ya que esto da la sensación de ampliar demasiado los controles, pero no es así, puesto que adicionando tan solo dos controles en las secciones 7 y 13.2 de la ISO 27001, podríamos tener resuelto este tema no cubierto por esta norma, como se detalla a continuación:

A.7 Gestión de activos		
A.7.3 Trazabilidad de los activos *Objetivo:* Gestionar el movimiento de activos para analizar sus riesgos y garantizar que puedan localizarse siempre que sea necesario.		
A.7.3.1	Ubicaciones y movimientos	*Control*: Implementar mecanismo de trazabilidad que permitan registrar los identificadores de activos, su ubicación, así como las razones del posible movimiento de cambio de propietario o de su nivel de seguridad analizando previamente los riesgos que dichos movimientos pudieran acarrear sobre la seguridad de los mismos

A.13.2 Gestión de incidentes de seguridad de la información y mejoras		
A.13.2.4	Trazabilidad de los incidentes	*Control:* Se deben definir los pasos a realizar en las respuestas a incidentes y eventos de seguridad relevantes asignando previamente roles determinados, registrando los plazos en los que tienen que efectuarse las acciones predefinidas o correctivas y preventivas y las fechas en las que dichas acciones han de ejecutarse.

La ISO 27002 nos habla que los controles seleccionados pueden ser escogidos a partir de este estándar, de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas conforme sea apropiado. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y del enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales relevantes.

2.4 IEC

La Comisión Electrotécnica Internacional es una organización sin fines de lucro, no gubernamental internacional de normas que prepara y publica estándares internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas - conocidos colectivamente como "electrotecnia". La IEC cubre una amplia gama de tecnologías de generación, transmisión y distribución de electrodomésticos y equipos de oficina, semiconductores, fibra óptica, baterías, energía solar, nanotecnología y energía marina, así como muchos otros. La IEC también gestiona tres sistemas mundiales de evaluación de la conformidad que certifican si los equipos, sistemas o componentes se ajustan a las normas internacionales.

2.4.1 Historia de la IEC

La IEC celebró su reunión inaugural el 26 de junio de 1906, tras las conversaciones entre la Institución Británica de Ingenieros Eléctricos, el Instituto Americano de Ingenieros Eléctricos y otros. En la actualidad, 82 países son miembros, mientras que otro 82 participan en el Programa de Países Afiliados, que no es una forma de adhesión, pero está diseñado para ayudar a los países industrializados que se involucren con la IEC. Originalmente ubicada en Londres, la comisión se trasladó a su

actual sede en Ginebra en 1948. Cuenta con centros regionales en Asia-Pacífico, América Latina y América del Norte.

Hoy en día, la IEC es la organización internacional líder a nivel mundial en su campo, y sus normas son adoptadas como normas nacionales de sus miembros. El trabajo es realizado por cerca de 10.000 expertos eléctricos y electrónicos de la industria, el gobierno, la academia, los laboratorios de ensayo y otras personas interesadas en el tema.

La IEC fue instrumental en el desarrollo y distribución de normas para las unidades de medida, en particular Gauss, Hertz y Weber. También propusieron por primera vez un sistema de normas, el sistema Giorgi, que en última instancia se convirtió en el SI o sistema de unidades internacionales.

En 1938, publicó un vocabulario multilingüe internacional para unificar la terminología eléctrica. Este esfuerzo continúa y el Vocabulario Electrotécnico Internacional sigue siendo un importante trabajo en la industria eléctrica y electrónica.

El CISPR - en inglés, el Comité Internacional Especial de Perturbaciones Radioeléctricas - es uno de los grupos fundados por el IEC.

La IEC colabora estrechamente con la Organización Internacional de Normalización y la Unión Internacional de Telecomunicaciones. Además, trabaja con varias de las principales organizaciones de normalización, incluyendo el IEEE con el que firmó un acuerdo de cooperación en 2002, que fue modificado en 2008 para incluir el trabajo de desarrollo conjunto.

2.4.1.1 Visión

Que las normas de la IEC y los programas de evaluación de la conformidad sean la clave del comercio internacional.

2.4.1.2 Misión

La misión de la IEC es ser reconocida mundialmente como el proveedor líder de normas, los sistemas de evaluación de la conformidad y servicios relacionados necesarios para facilitar el comercio internacional y aumentar el valor del usuario en los campos de la electricidad, electrónica y tecnologías asociadas. Para lograr lo anterior, han sido formulados los siguientes objetivos:

- Conocer las necesidades del mercado mundial eficientemente.
- Promover el uso de sus normas y esquemas de aseguramiento de la conformidad a nivel mundial.
- Asegurar e implementar la calidad de productos y servicios mediante sus normas.
- Establecer las condiciones de intemperabilidad de sistemas complejos.
- Incrementar la eficiencia de los procesos industriales.
- Contribuir a la implementación del concepto de salud y seguridad humana.
- Contribuir a la protección del ambiente.
- Dar a conocer los nuevos campos electrónicos.

2.4.2 Alcance mundial

La IEC seguirá fomentando la participación de las nuevas industrializaciones y economías en transición en la familia IEC. Los países candidatos se identificarán y se facilitará la pertenencia para los que quieran y de esta manera:

a) promover y apoyar la aplicación nacional de la IEC y sustituir progresivamente las normas nacionales divergentes (debido a que estén confusas o no estén de acuerdo).

b) formación de un comité nacional plenamente representativo electrotécnico.

c) participar activamente en los trabajos técnicos.

3.0 MARCO METODOLÓGICO

3.1 Tipo de estudio

Para poder realizar el análisis y evaluación de riesgos de la seguridad de la información necesitamos conocer la infraestructura tecnológica de la Empresa que será analizada en base a los once dominios de medición de acuerdo a la siguiente investigación.

3.1.1 Tipo de investigación descriptiva

Podremos decir que este proyecto es de investigación descriptiva debido a que necesitamos observar, inspeccionar, estudiar, entender y medir las actividades, procedimientos y características fundamentales que se tienen actualmente en la Empresa para poder comprobar los riesgos que existen en ella por falta de políticas.

3.2 Fuentes y técnicas para la recolección de información

Este es el punto que reviste mayor dificultad, debido a que la norma ISO 27001 si bien define once áreas o dominios que se pueden medir, no indica cómo hacerlo. Por lo anterior, se ha tenido que estudiar a fondo cada objetivo de control, qué se debe cumplir en cada uno de ellos, y cómo se debe cumplir. Una vez que se conoce a cabalidad cual es el objetivo, se debe medir en base a varias técnicas, como por ejemplo:

a) Entrevistas
b) Formularios
c) Cuestionarios
d) Indagaciones
e) Observación
f) Inspecciones
g) Consulta a Sistemas

h) Chek list

Estos métodos o técnicas permiten identificar los atributos o requerimientos de cada uno de los 133 puntos de control que establece la normativa ISO/IEC 27001/2005 y de esta forma cuantificarlos y convertirlos a indicadores que provean la base de resultado para la toma de decisiones en relación a cuáles serán las directrices en seguridad de la información que definirá la Organización.

3.3 Tratamiento de los riesgos de seguridad

De lo visto anteriormente, y una vez que se han obtenido las mediciones pertinentes en cada área o dominio, la Empresa debe definir ante cada punto de control si adopta medidas tendientes a reducir o mitigar los riesgos inherentes. Para ello, primero se debe determinar un criterio para determinar si se pueden aceptar los riesgos o no.
Los riesgos pueden ser aceptados si por ejemplo se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo considerando el costo para la empresa. Estas decisiones deben ser registradas.

Por cada uno de los riesgos definidos después de la evaluación de riesgo se necesita tomar una decisión de tratamiento de riesgo con las siguientes opciones:

a) Aplicar los controles apropiados para reducir los riesgos.
b) Aceptar los riesgos consciente y objetivamente siempre que cumplen claramente con la política y el criterio de aceptación de la organización.
c) Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.
d) Transferir los riesgos asociados a otros grupos, por ejemplo, aseguradores o proveedores.

Si la opción escogida es aplicar los controles (a), estos controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

- Que esté dentro del marco de la legislación y regulaciones nacionales e internacionales.
- Que cumpla o esté de acuerdo con los objetivos organizacionales.
- Que esté de acuerdo a los requerimientos y restricciones operacionales.
- Que el costo de la implementación y operación este en relación y proporcion a los riesgos que se están reduciendo y en relación a los requerimientos y restricciones de la organización.
- Que exista equilibrio entre la inversión en la implementación y operación de los controles versus el daño probable del resultado de fallas en la seguridad.

3.4 Evaluando los riesgos de seguridad.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debería ser equilibrado con el daño comercial probable resultado de las fallas en la seguridad.

Los resultados de la evaluación de riesgo ayudan a guiar y determinar la gestión apropiada y las prioridades de manejar los riesgos de seguridad e implementar los controles seleccionados para protegerse contra esos riesgos.

Una vez identificado los riesgos de seguridad, identificado los requerimientos, y tomado las decisiones para el tratamiento de los riesgos, se deben seleccionar los controles apropiados y se debieran implementar para asegurar que se reducirán a un nivel aceptable.

La selección de los controles depende de las decisiones organizacionales basadas en el criterio de aceptación de riesgo, opciones de tratamiento de riesgo y enfoque general para la gestión del riesgo.

3.5 Punto de inicio de la seguridad de la información

Estos controles se aplican en la mayoría de las organizaciones y en la mayoría de los escenarios:

3.5.1 Controles esenciales:

a) Protección de la data y privacidad de la información.
b) Protección de los registros organizacionales.
c) Derechos de propiedad intelectual.

3.5.2 Controles considerados práctica común para la seguridad de la información:

a) Documentos de la política de seguridad de la información.
b) Asignación de responsabilidades de la seguridad de la información.
c) Conocimientos, educación y capacitación en seguridad de la información.
d) Procesamiento correcto en las aplicaciones.
e) Gestión de la vulnerabilidad técnica.
f) Gestión de la continuidad comercial.
g) Gestión de los incidentes y mejoras de la seguridad de la información.

3.6 Alcance de la evaluación del riesgo en la Organización

El alcance del análisis y evaluación de riesgos a aplicar en la Organización, considerará los siguientes dominios definidos en la ISO 27001:

a) Política de seguridad.
b) Organización de la seguridad de la información.
c) Gestión de activos.
d) Seguridad de los recursos humanos.
e) Seguridad física y ambiental.

f) Gestión de comunicaciones y operaciones.
g) Control de acceso.
h) Adquisición, desarrollo y mantenimiento de sistemas de la información.
i) Gestión de incidentes de seguridad de la información.
j) Gestión de la continuidad comercial
k) Conformidad

Cabe mencionar que cada una de estas 11 cláusulas tienen una o varias categorías de seguridad, las cuales en suma son 39, cada una con un objetivo de control, que establece lo que se debiera lograr, y uno o más controles que se pueden aplicar para lograr el objetivo de control y de las cuales se desprenden 133 controles a aplicar.

Para evaluar el riesgo, primero debemos identificar el riesgo, luego cuantificarlo, y priorizar sobre estos riesgos, todo lo anterior, comparado con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. A su vez, los riesgos estimados son comparados con un criterio de riesgo.

Estos resultados nos guían y determinan la gestión y prioridades para manejar los riesgos, para luego implementar los controles seleccionados, dependiendo cual sea la decisión tomada por la empresa para el tratamiento de cada riesgo en particular.

3.7 Desarrollo de resultados del análisis y evaluación de riesgos de seguridad de la información

El desarrollo del resultado del análisis y evaluación de riesgos de seguridad de la información proviene de la recopilación de información, hallazgos y análisis de la situación actual de cada área de la organización, basándonos en los controles de la ISO 27002 correspondientes a los once dominios de la norma.

3.8 Análisis de la situación actual

Hoy en día la amenaza más importante contra nuestra información, la encontraremos dentro de la misma empresa donde trabajamos. Ya sea por accesos indebidos o no autorizados a la información corporativa que son realizados por los empleados de la misma.

Adicionalmente se suman los ataques de virus informáticos que son ocasionados intencionalmente o por desconocimiento de los mismos empleados, en sentido general, las empresas de nuestro país se inclinan más preocupándose por los agentes externos que por los internos.

Lo importante es que las empresas realicen una evaluación de riesgos formal, para poder tener conocimiento de la importancia que tienen estos riesgos, y del mismo modo saber cuáles áreas de su empresa se encuentran mayormente vulnerables frente a potenciales amenazas. El resultado de este análisis reflejará en que punto de seguridad se encuentran en cada uno de los once dominios o áreas.

3.9 Creación de un Plan

En este punto, describiremos la creación de una correcta y eficiente planificación para asegurar los activos de información que actualmente posee la Organización, no sólo de los ataques, sino para cuidarlos de los errores humanos que se puedan cometer sin tener un método establecido.
Una política de seguridad es un plan que se basa en prioridades. Estas prioridades se apoyan en jerarquías de importancia, empezando desde lo menos importante a proteger y terminando, obviamente, en lo más sensible para la organización.
Para empezar a armar una política de seguridad, primero hay que determinar qué es lo que se desea proteger y cuáles son las prioridades de los elementos. El segundo paso es saber de quién hay que protegerse. Si bien el grado de paranoia dependerá de cuán

importante sea la empresa y qué tan sensible sean los activos de información, no dejando de lado que lo primordial es el cómo. El tercer paso a considerar es el riesgo. Aquí tiene mucha importancia el enfoque que se utiliza. Es en vano preocuparse por la seguridad de la base de datos de afiliados, si a éstos no le damos la seguridad necesaria para que crean que la organización es segura. En el cuarto procedimiento, debemos implementar medidas de seguridad para proteger los recursos de la organización. El último paso es el de mejorar. Cuando hablamos de mejorar, nos referimos a que un recurso de la empresa puede funcionar en forma más eficiente. Para saber en qué momento un recurso tiene fallas o si salió al mercado una versión más nueva (por consiguiente, pueden existir fallas conocidas), es necesario realizar un método de verificación y enumeración de los recursos, con su versión y fecha, a fin de efectuar una revisión periódica.

3.9.1 Responsabilidades

Todo aquello que se haga, sin duda repercutirá en el futuro de la organización. Por tal motivo, se debe crear una política de seguridad concientizada, formada por personas o grupos que se especialicen en diferentes áreas dentro de la rama de la computación.
Si bien un plan de seguridad es una cuestión muy delicada, lo importante es saber escuchar sugerencias de todo tipo de persona, ya que cada empleado posee una opinión formada acerca de qué tipo de recursos necesita y que cosa estaría dispuesto a hacer por medio de procedimientos.

3.9.2 Riesgos

Los frutos de la implementación se relacionan con el menor impacto a nivel de riesgo. Es difícil saber dónde invertir cuando hablamos de un tema tan general como lo es la seguridad, pero una cosa que hay que tener en claro es que se sale beneficiado siempre y cuando sepamos dirigir la mirada hacia el punto correcto. Es por eso que, para estar informado en este tema, hay que estar actualizado. Los ataques externos son numerosos, pero los ataques internos son menos vistos y conllevan una mayor

peligrosidad. Porque a diferencia de los ataques externos, los empleados que trabajan para la empresa se convierten en atacantes cuando ven una brecha abierta, y muchas veces no la andan buscando.

3.9.3 Identificar los Bienes y/o Recursos de la Organización

Como mencionamos anteriormente, una política de seguridad no es sólo para proteger la información y/o datos. Por tal razón, se crearon categorías para confeccionar un inventario más ordenado. Estas categorías son seis y sirven para identificar los bienes y/o recursos de la organización:

- **Datos**: Tiene que proteger todos los datos, pero la manera de hacerlo no es tomando todos los archivos sueltos, sino determinando el origen de los mismos, dónde se guardan, como llegan, respaldos, etc.

- **Software**: se ha de proteger todos los programas o códigos de los mismos que fueron hechos por la organización o que son licenciados o pagados por ella.

- **Hardware**: No se puede usar las mismas técnicas para proteger un software que para un hardware, ya que para los elementos tangibles se usan otros mecanismos como los que se establecen para la seguridad física.

- **Instructivos/documentos**: se trata de todo instructivo, documentación, tutorial, manual y lo que tenga que ver con la implementación de equipos, software o reglas de la empresa. La política de seguridad también integra esa categoría. Nadie debe alterar estos procedimientos sin autorización de las personas responsables.

- **Elementos fungibles**: Todos los elementos fungibles deben ser protegidos del uso o mal uso. El papel, los cartuchos de tinta, los medios magnéticos y los

sellos son los más utilizados. Una persona no puede utilizar un sello oficial, así como el papel y el cartucho no pueden utilizarse con la ausencia de un control.

- **Personal**: Las cuentas de los usuarios y/o clientes deben tener uno o varios responsables que se encargan de administrar dicha información. Cada usuario estará habilitado para ver solamente su perfil, y cada cliente debe estar seguro que sus datos no se encuentran a la vista.

Asegurándose de identificar todos los recursos o bienes que la empresa dispone, es posible clasificarlos en categorías, por ejemplo, los sistemas de información de una Organización deberán estar clasificados de la siguiente manera:

- **Clave**: Directamente orientado con el deber fiscalizador de la Organización.

- **Apoyo**: apoyarán a estos procesos claves contribuyendo a su mejor funcionamiento.

- **Estratégico**: Necesarios para el mantenimiento y progreso de la organización.

Por otro lado, también es necesario clasificar los datos que llegan, los que se manipulan y los que se generan en las salidas de los Sistemas:

- **Datos públicos**: Su conocimiento por el público no afecta el funcionamiento de la organización dueña de los datos.

- **Datos sensibles**: Requiere de un nivel más elevado que los datos públicos. Se debe tener especial cuidado de una pérdida de confidencialidad o integridad por alteraciones no autorizadas.

- **Datos privados**: Sólo debe ser conocido por la organización. Su divulgación puede afectar de alguna manera el funcionamiento de la organización.

- **Datos confidenciales**: Sólo puede ser conocida por la organización y que afecta considerablemente a ésta. Típicamente, si se comete infidencia, las sanciones legales son aplicadas a partir de esta categoría. Por ejemplo podemos mencionar el caso de las multas, fusiones, Oficios reservados, etc.

3.9.4 Identificar los riesgos

Los riesgos a los cuales está expuesta la Organización, pueden obtenerse imaginando que sucedería si alguno de los activos de información se dañaran, perdieran, modificasen sin autorización, etc.. Estos tipos de interrogantes fueron necesarios para determinar e identificar los riesgos a los que estamos expuestos:

RIESGO	CAUSA	NIVEL
Copia de datos y/o información	Maliciosa	Alto
Robo de Hardware	Maliciosa	Alto
Modificación de datos	Maliciosa	Alto
Claves por defecto	Ignorancia	Medio
Versiones vulnerables	Desconocimiento	Medio
Borrado de datos	Maliciosa/descuido	Medio
Borrado de respaldos	Maliciosa/descuido	Muy Alto
Virus	Maliciosa	Medio
Eventos Naturales	Imprevisto	Muy bajo
Bloqueo de usuarios	Intentos fallidos	Bajo

3.9.5 Amenazas

A los profesionales de seguridad informática, les atañe un tema difícil de abordar a la hora de hablar de amenazas, ya que es un tema abstracto y en continuo crecimiento. La mejor manera de visualizar las amenazas, es imaginarse que nuestros activos de información fuesen como un ser humano, y la ropa como dispositivos de seguridad: De nada sirve comprarse un vestón si sólo tenemos pantalones cortos, así como de nada sirve comprar un firewall si no tenemos asegurada nuestra red interna. Es muy importante enunciar esto, ya que hablar de amenazas no implica distinguirlas sino saber prevenirlas en su conjunto.

En la ilustración siguiente se proporciona un modelo teórico que se utiliza para determinar las distintas amenazas, motivos y objetivos, métodos, puntos débiles y vulnerabilidades que podrían emplearse en contra de la organización en un ataque.

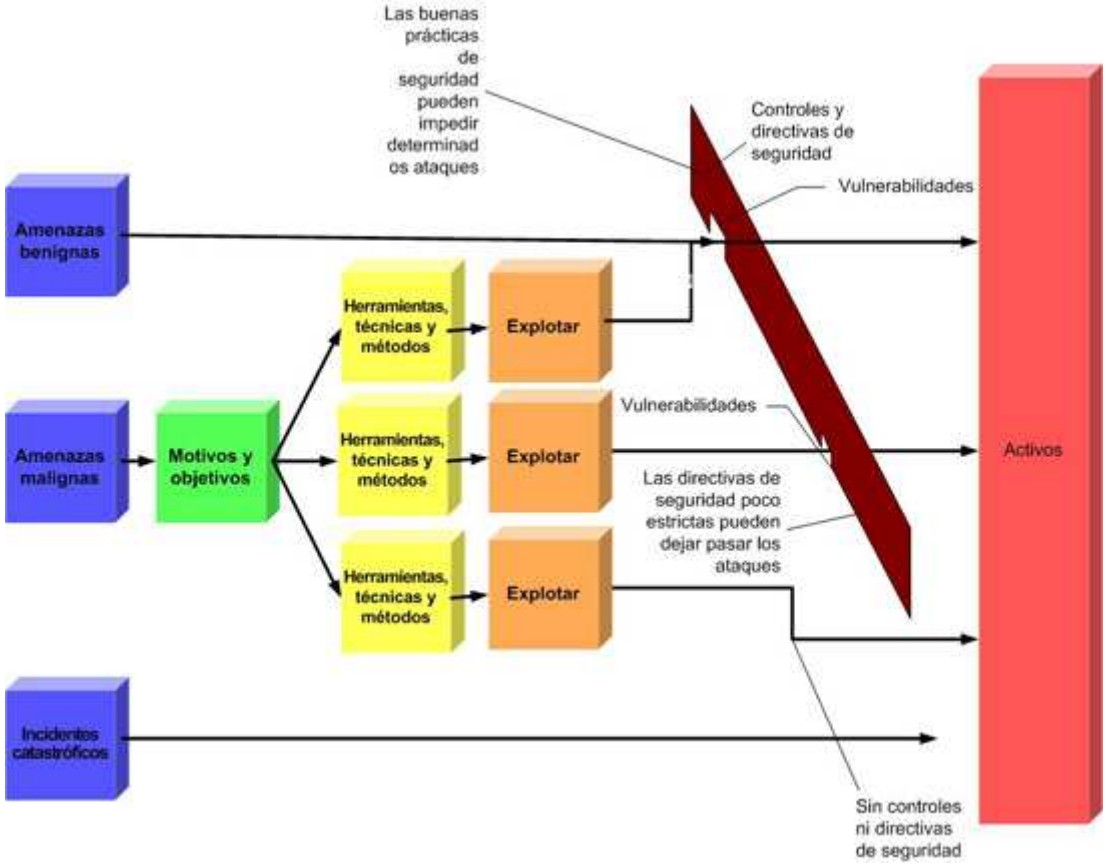


Figura 3.1 - Esquema de las amenazas en los activos

3.9.6 Ataques Internos

Este tipo de amenaza se fundamenta en que la gran mayoría de los ataques, a los activos de información en general, provienen desde dentro de la organización y cada vez es mayor la brecha entre los ataques externos y los internos.
La información de una empresa siempre es confidencial hasta que esté explícito lo contrario. Si bien hay recursos que tal vez no parezcan, lo son: un instructivo de cómo instalar un certificado digital, un Excel antiguo, un documento en Word que habla sobre posibles fiscalizaciones, un manual de un sistema clave, etc.. Dentro del grupo de amenazas internas, hay dos que no son intencionales:

- **Ignorancia**: Un empleado que no tiene noción de la política de seguridad o bien de computación, no entiende el riesgo que implica divulgar información de seguridad.
- **Descuido**: a diferencia de la ignorancia, los empleados que entran en este ítem son los que están conscientes de los peligros de divulgar información pero que, por determinados motivos, la divulgan sin intención. Los motivos pueden ser cansancio, estrés, etc.

Luego están las dos amenazas intencionales, que son:

- **Maldad**: intencionalmente, un empleado con información confidencial quiere causar daño ya sea destruyendo, divulgando o haciendo uso indebido de la información
- **Indiferencia**: un empleado que conoce las políticas de seguridad decide no hacer caso a las mismas y toma acciones en contra con propósitos personales. Dejar anotada la clave en un papel, pedir ayuda a un compañero permitiendo que éste vea la información, son ejemplos de amenazas de gente que es indiferente a la política de seguridad por diversos motivos.

3.9.6.1 Métodos de prevención

Obviamente que hay métodos para prevenir estas amenazas, ya que no sería útil sólo nombrarlas:

- Cuando una persona se va de la empresa, inmediatamente su cuenta debe ser dada de baja para que no pueda transmitir ni dañar la confidencialidad
- Los empleados que no están contratados oficialmente por la empresa (honorarios, reemplazo, en práctica), deben manejar las herramientas y sistemas que no son ni estratégicos ni claves de la organización.
- Las cuentas de los usuarios son de carácter individual, en consecuencia, no pueden utilizarse varias a la vez.
- Revisar periódicamente los sectores en busca de irregularidades, tanto físico (papeles, cajones, etc.), como personal con actitudes sospechosas.
- Protectores de pantalla con clave.
- Capacitar a los empleados basándose en la política de seguridad y demostrando cuales son los riesgos de violarla.
- Dejar en claro que los sistemas están siendo monitoreados constantemente.

3.9.7 Ataques Externos

Los ataques externos se producen de dos formas principales: ataques perpetrados por personas y los efectuados por aplicaciones malintencionadas. Ambos tipos tienen diferentes características y perfiles de amenaza. Los atacantes humanos pueden aprender detalles sobre la red de destino y modificar el ataque como sea pertinente, mientras que las aplicaciones malintencionadas pueden afectar a varios equipos y dejar puertas traseras para que las utilicen los atacantes.

Las aplicaciones malintencionadas incluyen varias amenazas posibles, como virus, gusanos y troyanos. Aunque estas aplicaciones pueden ser problemáticas y causar trastornos considerables, estos ataques son más sencillos de evitar que los perpetrados por personas.

3.9.7.1 Problemas empresariales

Ahora analizaremos los problemas empresariales que surgen debido a ataques externos que intentan penetrar la red y que son detectables en el nivel de presentación o de aplicación. La supervisión de la seguridad no resulta especialmente útil para identificar un ataque de denegación de servicio distribuida (DDoS), aunque otros mecanismos, como los registros de Servicios de Internet Information Server (IIS), pueden identificar la duración, el tipo de paquete, la dirección IP aparente (probablemente falsa) y otros detalles del ataque DDoS.

La identificación de aplicaciones malintencionadas es de importancia considerable para las organizaciones de todos los sectores, aunque sobre todo para aquéllas que funcionan en el sector financiero o que deben cumplir normativas. Por ejemplo, ese tipo de organizaciones sienten más preocupación hacia la presencia de aplicaciones espía. Las aplicaciones espía pueden residir en un servidor o estación de trabajo y transmitir información confidencial a terceros externos.
Un problema empresarial importante con las aplicaciones malintencionadas es la inseguridad de que existan en una red. Un ejemplo especialmente inquietante es cuando el componente de software malintencionado es un programa que toma el control absoluto de un equipo y, a continuación, enmascara el hecho de que a partir de ese momento un atacante lo controla. Es difícil tener la certeza de que los equipos no ejecutan tales aplicaciones malintencionadas, ya que puede que el rootkit tenga más destreza en ocultarse que la empresa en detectarlo.

3.9.7.2 Problemas técnicos

El aumento en la cantidad de ataques a las organizaciones es consecuencia de las acciones de atacantes sin experiencia que utilizan secuencias de comandos configuradas previamente para explotar vulnerabilidades. Mucho más peligro revisten los miembros del pequeño y dedicado conjunto de atacantes muy experimentados y

capacitados (que también cooperan entre sí), que puede utilizar un conjunto de ataques diferentes para intentar penetrar una red.
Un atacante es una persona que realiza un ataque deliberado; un virus, gusano o troyano que actúa por sí solo no es un atacante.
La principal forma de identificar aplicaciones malintencionadas es realizar el seguimiento de procesos. Al hacerlo, se identifica cada programa que se inicia o se detiene en una estación de trabajo o servidor. La desventaja que presenta es que genera una gran cantidad de sucesos, la mayoría de los cuales carecen de interés.

El análisis de procesos de los que se ha realizado un seguimiento puede ser difícil en las dos zonas siguientes:

- Servidores Web que utilizan CGI (Common Gateway Interface). Cada visita a la página crea un proceso.
- Estaciones de trabajo de desarrollo. Las compilaciones de las aplicaciones crean numerosos procesos en un breve período de tiempo.

Estos factores pueden causar elevadas cantidades de sucesos en poco tiempo o crear muchos sucesos continuamente. En cualquier caso, se necesitan filtros eficaces que extraigan los sucesos de ataques diferenciándolos de los legítimos.

3.9.7.3 Problemas de seguridad

Los problemas de seguridad que causan los ataques externos son considerables, ya que los atacantes disponen de gran flexibilidad para elegir el método de intrusión en la red. Los atacantes externos pueden penetrar las redes a través de los siguientes mecanismos:

- Intento de conseguir contraseñas
- Cambio o restablecimiento de contraseñas

- Explotación de vulnerabilidades
- Engaño a un usuario para que ejecute una aplicación malintencionada
- Uso de la elevación de privilegios para comprometer a equipos adicionales (lo que en inglés se denomina island hopping, saltos a otros sistemas)
- Instalación de un rootkit o troyano
- Uso de una estación de trabajo no autorizada
- Uso de un ataque phishing, en el cual una dirección de correo electrónico fraudulenta dirige a un sitio Web malintencionado

El principal método para detectar atacantes y aplicaciones malintencionadas consiste en realizar un seguimiento de los procesos. Se necesita aplicar este método con mucha atención e integrarlo con directivas de restricción de software en Directiva de grupo. Tenga en cuenta que se deben definir directivas estrictas que estipulen qué programas se pueden ejecutar en los equipos dentro de las redes perimetrales.

3.9.7.4 Requisitos de la solución

Los requisitos de la solución para identificar a atacantes externos coinciden en parte con los necesarios para identificar amenazas internas. Entre estos requisitos, se incluyen:

- Un método de defensa en profundidad para implementar la seguridad.
- Registros de auditoría de seguridad eficaces.
- Recopilación centralizada confiable de los registros de seguridad.
- Análisis automatizados de los registros de seguridad para identificar firmas de ataques.

Los requisitos de la solución para detectar aplicaciones malintencionadas comparten algunos de los necesarios para identificar amenazas internas. Entre estos requisitos, se incluyen:

- Procedimientos eficaces para auditar todo software no autorizado en la red.
- Registros de auditoría de seguridad configurados correctamente.
- Recopilación centralizada confiable y filtros de registros de seguridad.
- Análisis automatizados de los registros de seguridad para identificar comportamiento sospechoso, con el uso de programas de terceros si es necesario.

3.9.7.5 Amenazas humanas

La ingeniería social es el arte de aprovecharse de la ingenuidad o de la buena fe de las personas. Aprovecha debilidades psicológicas que son muy complejas de aprender y muy fácil de realizar. Es una debilidad universal, ya que cada computador es manejado por una persona, y esa persona no es un robot sino que tiene sentimientos, y es aquí donde el atacante quiere llegar, al sentimiento de la persona. Todo usuario ha tirado papeles importantes al tacho de la basura, ha respondido a consultas sin saber quien era el emisor de la interrogante, ha escrito su clave en algún lado. Todo lo que los usuarios hacen a menudo, hace que las personas sean uno de los riesgos más importantes que tiene la empresa.

3.10 Vulnerabilidades

3.10.1 ¿Qué es una vulnerabilidad?

La mejor palabra que podríamos usar para definir una vulnerabilidad es debilidad. Sin duda, una vulnerabilidad hace que la seguridad se vea disminuida o, en algunos casos, que se vea nula. Es por ello que es correcto afirmar el concepto de debilidad.
Según la academia de la lengua española, la vulnerabilidad es "*que puede ser herido o recibir lesión física o moral*", para nuestro caso, sería necesario agregar "*virtualmente*".

3.10.2 Tipos de vulnerabilidades

Antes de definir los tipos de vulnerabilidades, es necesario dejar en claro que todas las aplicaciones han sido escritas en un lenguaje de programación. Por tal motivo, la mayoría de los servicios en Internet son vulnerables ya que los lenguajes de programación son vulnerables. Las vulnerabilidades se clasifican en tres tipos:

- Vulnerabilidades que permiten escalar privilegios
- Vulnerabilidades de Denegación de Servicio–DoS (Denial of Service)
- Vulnerabilidades que otorgan privilegios de Administrador o Root.

Pueden originarse en la plataforma del Sistema Operativo o en el Software instalado. La manera tradicional de explotar vulnerabilidades es a través de Exploits (falla o agujero de seguridad), los mismos pueden ser locales, remotos o códigos desarrollados por programadores, generalmente en lenguaje C.

En la lista siguiente se detallan posibles tipos vulnerabilidades, que representan sólo unas pocas de las tantas existentes e incluyen ejemplos de las áreas de seguridad física, de información y de red.

Vulnerabilidades	Ejemplos
Físicas	Puertas sin cerrojo
Naturales	Edificio corporativo construido sobre una línea de error
Hardware y software	Software antivirus y revisiones de sistemas operativos desactualizados
Medios	Interferencia eléctrica
Comunicaciones	Protocolos no cifrados
Humanas	Procedimientos mal definidos y aplicaciones escritas de manera inadecuada

La relación entre amenazas, vulnerabilidades y riesgos puede ser un concepto difícil de entender al principio. Cada amenaza y vulnerabilidad que se identifique dentro de la organización debe ser calificada y clasificada de acuerdo a un estándar, como baja, media o alta. La clasificación varía entre las distintas organizaciones y a veces también dentro de la misma organización. Por ejemplo, la amenaza de un terremoto es significativamente mayor para las oficinas que se encuentran cerca de una línea de error importante que para cualquier otro lugar. De forma similar, la vulnerabilidad del daño físico a equipos será muy alta para una organización que se dedique a la producción de equipos de electrónica extremadamente sensibles y frágiles, pero la misma vulnerabilidad será más baja para una compañía constructora.

La matriz de administración de riesgo ayuda a evaluar las amenazas y su impacto en la organización. El nivel de riesgo en su organización se incrementa con el nivel de amenaza y vulnerabilidad, como se indica en la ilustración siguiente.

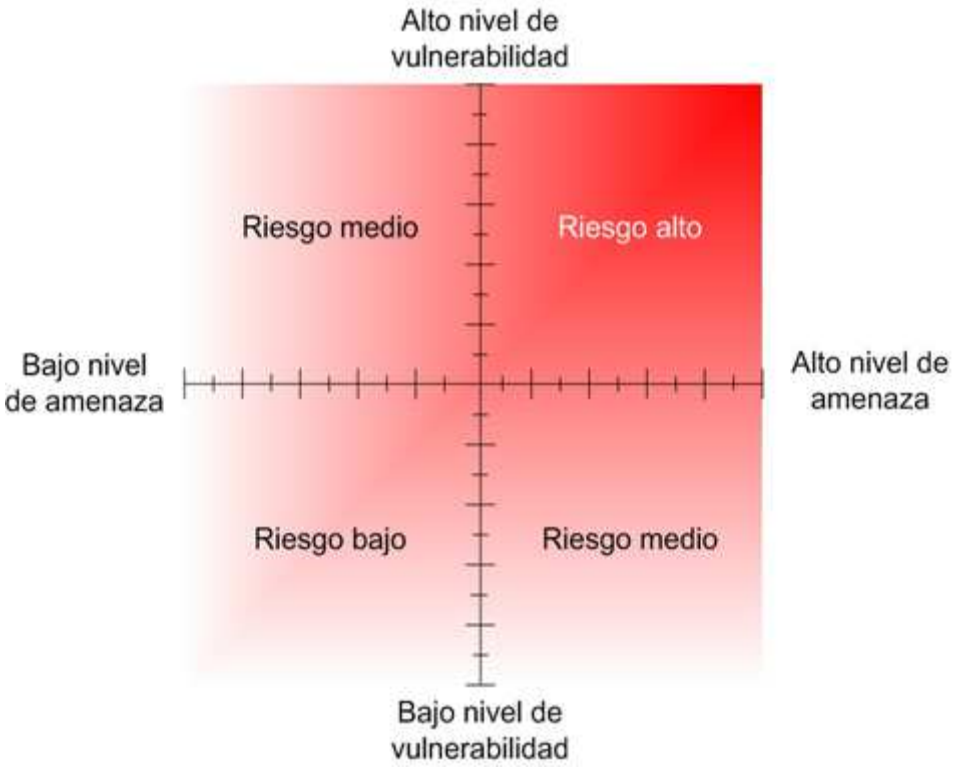


Imagen 3.2 - Matriz de administración de riesgo

3.10.2.1 Seguridad Física

Para hacer un trabajo de seguridad, no podría faltar todo lo referente a seguridad física, que es tan importante como la seguridad que se tiene con la información con respecto a posibles intrusiones. En este punto definiremos los temas más importantes y necesarios para poder lograrla.

Cuando hablamos de seguridad en términos físicos, no estamos hablando solamente del hardware, sino que estamos hablando sobre el entorno, que es tan importante como los equipos mismos.

3.10.2.2 Los Accesos

Lo mejor para hacer un buen diagrama de seguridad es tener el plano del edificio a fin de poder enumerar los posibles accesos de los atacantes. No obstante, si no hay posibilidad de tener el plano, nos conformaremos con revisar y constatar por nuestra propia cuenta las posibles filtraciones que pueda haber.
Lo primeo es enumerar los accesos visibles, como las puertas principales y las ventanas próximas al público, y luego, los otros accesos que no son conocidos o visibles. Los empleados deben tener un medio para ser identificados para acceder a los lugares definidos como estratégicos dentro del edificio.

3.10.2.3 Datacenter

El datacenter, o centro de cómputo, debe tener muchísima más seguridad que cualquier otra sección. No hace falta mencionar las redundancias que hay en todo sentido, desde el aire acondicionado hasta la electricidad, pasando por todos los niveles de comunicación que tiene la empresa con el centro de cómputos. Lo óptimo es tener una máquina dedicada a monitorear los estados de la arquitectura y del entorno (cómo está la temperatura, si hay un posible incendio, si los sistemas de enfriamiento funcionan correctamente, si los accesos están íntegros, etc.), esta opción sería óptima siempre y cuando se tomen en cuenta los registros que informan, ya que como en muchas ocasiones, dichos registros no son vistos por nadie, como por ejemplo, los “logs” de algunas bases de datos.

3.10.2.4 Desastres naturales

Los desastres naturales pueden traer en forma directa, o indirecta, diversas complicaciones para el normal cumplimiento dentro de la organización, es por ello que se debe realizar un plan que contemple cada uno de los posibles acontecimientos que puedan afectarnos:

3.10.2.5 Electricidad

Éste es un tema muy importante dentro de todo lo concerniente a la seguridad física, ya que es lo que hace funcionar a nuestros equipos, y en caso que lo haga mal, puede afectarnos de diferentes formas: desde el mal o nulo funcionamiento del hardware hasta importantes pérdidas derivadas de la incapacidad de procesar los datos que se encuentren almacenados dentro del equipo. Hay varias fallas que pueden surgir con respecto a la electricidad, que van desde altas y bajas de tensión hasta un rayo, o directamente, un corte de suministro de energía por un tiempo limitado.

3.10.2.6 Incendios

Los sistemas para prevenir incendios son, sin duda, indispensables en cualquier centro de cómputo. Dichos sistemas son capaces de alertarnos cuando se está originando un incendio o algunos pueden detectar esto antes que suceda (en teoría, ya que se basan en el grado de temperatura y demás factores como presión, voltajes, etc.). Es obvio mencionar que los sistemas de prevención de incendios no pueden funcionar con agua, por la sencilla razón de que dañarían al hardware. Por tal motivo, deben basarse en CO2 (dióxido de carbono), o en espuma. En cuanto a los extintores, se debe confeccionar una planilla en donde se informe la cantidad, ubicación, vencimiento de la carga, estado unidades faltantes, identificación y señalización de los mismos.

3.10.2.7 Temperatura

Los sistemas de refrigeración (equipos de aire acondicionado), deben estar en una posición estratégica para hacer circular el aire a todos los equipos, por consiguiente, no debe haber nada que obstruya el circuito. Es importante mencionar que todos los sistemas de refrigeración deben estar conectados a un sistema de alimentación continuo o UPS.

3.10.2.8 Backups

La pérdida de los datos sin tener un backup puede ser fatal, pero la pérdida de los backups no sólo puede ser peligrosa porque perdimos información guardada, sino que esa pérdida se puede deber a una acción maliciosa, como por ejemplo, el hurto. Es decir que es fundamental que haya una extrema seguridad para almacenar las copias de seguridad.

3.10.2.9 Redundancia

La localización física ya dejo de ser un problema, por ahora es posible tener en otro sitio físico un computador, o servidor, de auxilio o redundancia en caso de que sufra algún problema un computador, o servidor, crítico. Si bien es cierto que a nivel de hardware resulta costoso implementar este tipo de redundancia distribuida, también es cierto que este tipo de mecanismos se está haciendo más común dentro de las organizaciones que "*no pueden parar de funcionar*" ante cualquier evento o problema en un computador, o servidor crítico.

3.10.2.10 Acceso físico al hardware

El acceso físico al hardware debe ser autorizado teniendo en cuenta el nivel y el sector que tiene cada personal de la empresa. No todos los equipos son iguales, por lo tanto los niveles de accesos a ellos no van a ser los mismos. Entonces, todos los dispositivos importantes deben estar ubicados en un sector donde la seguridad sea equivalente a la criticidad que hay en los equipos. Es importante que el registro de seguridad se realice sobre las personas que deban tener un contacto físico con el hardware, quedando registradas las modificaciones que se realizaron y el responsable de tales modificaciones.

3.10.2.11 Cámaras de seguridad

Las cámaras de seguridad son un elemento imprescindible si tenemos a nuestro cargo sistemas realmente críticos o sistemas especialmente atractivos para los supuestos intrusos o hackers. Esto incluye todos los sistemas que alberguen datos personales de nuestros usuarios. Si tenemos centros de datos que almacenan datos de este tipo o cualquier tipo de datos críticos para el funcionamiento de la empresa o secretos debemos tener personal de vigilancia contratado. Este personal deberá contar con cámaras de seguridad que les permita monitorizar el edificio ante la posibilidad de intrusos o de actuaciones sospechosas del personal. Lo ideal es tener personal de vigilancia presencial en el centro de datos para el control de acceso y luego personal de vigilancia encargado de la monitorización de las cámaras de vigilancia.
Debemos tener en cuenta las cuestiones relativas a la privacidad de nuestro personal cuando instalemos o aconsejemos instalar cámaras de vigilancia. Normalmente debemos poner en conocimiento de los empleados la existencia de estas cámaras, su localización y su función de vigilancia.

3.10.2.12 Ventanas

Uno de los errores en seguridad física más comunes que se suelen observar en entornos reales es la visibilidad desde el exterior de los monitores y teclados de los usuarios que están trabajando dentro del edificio. Esto es un fallo de seguridad física muy importante, pues un intruso malintencionado puede observar desde una ventana o desde el exterior del edificio como el personal teclea sus claves personales o datos secretos o críticos para la empresa. Este es un caso muy común en las oficinas de los bancos, que suelen estar situadas en las primeras plantas de los edificios y tienen normalmente grandes fachadas de cristal que permiten la visibilidad al interior por parte de cualquier intruso.

La solución es muy sencilla. Basta con elegir la localización de los monitores y teclados fuera del alcance de un supuesto observador exterior. No se aconseja en principio la instalación de cortinillas o sistemas similares si no es imprescindible, porque casi siempre con una reubicación de los escritorios de los empleados o de sus sistemas informáticos basta para proporcionar una seguridad física suficiente en este caso.

3.10.2.13 Bocas de red

Las bocas de red suponen un peligro inmediato de seguridad física, pues cualquier intruso con un portátil puede conectarse a cualquiera de ellas y probablemente obtendrá una conexión a la red interna de la empresa. Debemos estudiar por tanto las bocas de red que no estén ocupadas (y las que estén ocupadas y puedan ser desconectadas y usadas) y los concentradores que tengan conexiones libres. Para el caso de los concentradores el cuidado es el mismo de siempre, deben estar en armarios o racks cerrados donde solo los administradores de red tengan acceso a ellos. Para las bocas de red es más complicado. Si tenemos una red fija y no tenemos perspectivas de tener que instalar nuevas máquinas a menudo lo más aconsejable es desconectar todas las bocas de red que no estén siendo usadas para que nadie pueda conectarse a ellas. Si tenemos que instalar una nueva máquina o necesitamos otra boca de red vamos al rack

y conectamos el cable que da conectividad a la boca de red en cuestión. Tener todas las bocas de red conectadas es tener accesos libres a la red repartidos por toda la empresa que cualquiera puede usar, incluido un supuesto intruso.
Para las bocas de red que están siendo usadas por los usuarios deberemos monitorizar e identificar de alguna forma las máquinas que deben estar en cada red, o asignarlas las direcciones IPs y la conectividad por medio de las direcciones MAC de las tarjetas, esto nos avisará o prevendrá el que un supuesto intruso desconecte una máquina y conecte un portátil o un dispositivo de mano y acceda a la red. Es trabajoso mantener en el servidor DHCP o en los concentradores todas las direcciones MAC de las tarjetas de red en las máquinas de usuario, pero esto nos asegurará que sólo las máquinas que nosotros deseamos tendrán acceso a nuestra red.

3.10.2.14 Dispositivos de almacenamiento externo

Los dispositivos de almacenamiento externo, como discos externos, pendrive, etc., son un problema para los administradores de sistemas y los encargados de la seguridad del sistema. Para empezar tenemos lo que puede venir en ellos: virus, software pirateado, todo tipo de software o datos poco recomendables para un lugar de trabajo, juegos, etc. Luego tenemos todo lo que se puede llevar en ellos: datos de la empresa, software cuya licencia ha sido adquirido por la empresa, software bajado de internet, etc.
Si lo que más nos preocupa es que el usuario pueda replicar datos y sacarlos de al empresa solo podemos hacer dos cosas, la primera y la que siempre recomendamos es mantener los datos lejos del usuario, la segunda es inhabilitar los puertos USB y los sistemas serie o paralelo, ya sea mediante métodos de software o hardware.
Los puertos serie y paralelo no suponen un gran peligro, puesto que los dispositivos de almacenamiento que normalmente se conectan a ellos suelen necesitar en el sistema operativo Windows de drivers especiales, que podemos controlar que no se puedan instalar de diversas formas, sobre todo mediante software de control de instalación de software. Los dispositivos USB son un problema mayor, como veremos.

Si estamos hablando de Software Libre como Linux o FreeBSD no hay mucho problema. El soporte USB de almacenamiento viene como módulos del kernel que pueden quitarse del sistema con lo que no se podrá usar dongles USB ni dispositivos de almacenamiento USB. Lo mismo para los dispositivos serie y paralelo. Este sistema es muy simple y es ideal para evitar este tipo de comportamientos.

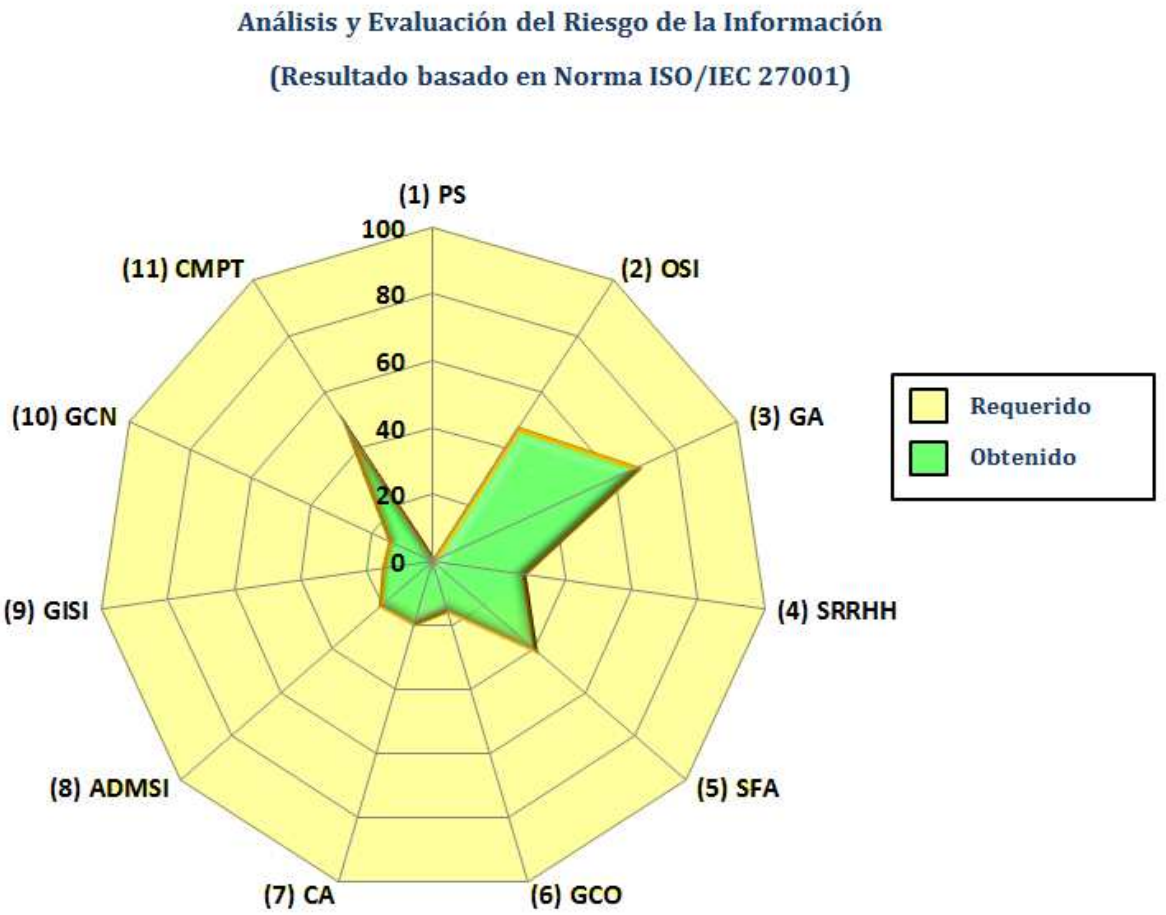
Pero si hablamos de Windows el caso es diferente. Aquí es más complicado quitar los drivers de almacenamiento externo USB, sobre todo en Windows 7 u 8, que incorporan una serie de drivers para todo este tipo de dispositivos. Si es posible se deben quitar del sistema los drivers para este tipo de dispositivos o se inhabilitará mediante software la instalación de nuevo hardware en el sistema (lo cual es un problema si tenemos impresoras o mouse y teclados USB que deben autodetectarse).

La solución más radical (y no por ello la más recomendable) es quitar el cableado de los puertos USB frontales que conectan a la placa base y a puertos. Podemos incluso sellar o desconectar los puertos USB integrados en la placa base. Si no queremos realizar semejante cambio del hardware, podemos intentar desactivar estos puertos mediante switches o puentes en la placa base, pero esto no es siempre posible. Si queremos aislar de verdad el sistema siempre podemos comprar cajas de metacrilato cerradas que solo permiten la ventilación del sistema y no el acceso a este, pero estamos hablando ya de soluciones realmente radicales para un simple Pen Drive.

4.0 RESULTADOS

Una vez que se ha medido cada una de las once áreas o dominios definidos por la ISO 27001, es necesario agruparlas para así poder mostrar los resultados en un gráfico que represente el resultado global del análisis y evaluación de la seguridad de la información. De esta forma la gerencias de las Organizaciones pueden ver claramente qué áreas son las más vulnerables o con mayores deficiencias en materia de seguridad, a fin de poder emprender un plan de seguridad que abarque las áreas con mayor riesgo, y de esta forma, minimizarlos, todo lo anterior, de acuerdo con los objetivos de la Organización y dentro del marco Legal.

A continuación se presenta un gráfico polar o tipo “radar”, que muestra el resultado global de Seguridad de la Información en la Organización.



(1) PS: Política de Seguridad
(2) OSI: Organización de la Seguridad de la Información
(3) GA: Gestión de Activos
(4) SRRHH: Seguridad de los Recursos Humanos
(5) SFA: Seguridad Física y Ambiental
(6) GCO: Gestión de las Comunicaciones y Operaciones
(7) CA: Control de Acceso
(8) ADMSI: Adquisición, Desarrollo y Mantenimiento de los SI
(9) GISI: Gestión de Incidentes de Seguridad de la Información
(10) GCN: Gestión de la Continuidad del Negocio
(11) CMPT: Cumplimiento

4.1 Presentación de resultados

A continuación se presenta el resultado del análisis y evaluación de seguridad de la información separada por cada una de las 11 áreas consideradas en el presente trabajo.

4.1.1 Políticas de Seguridad

El objetivo que persigue revisar y descubrir esta área es el siguiente:

- Proporcionar la dirección y ayuda de la administración a la seguridad de la información

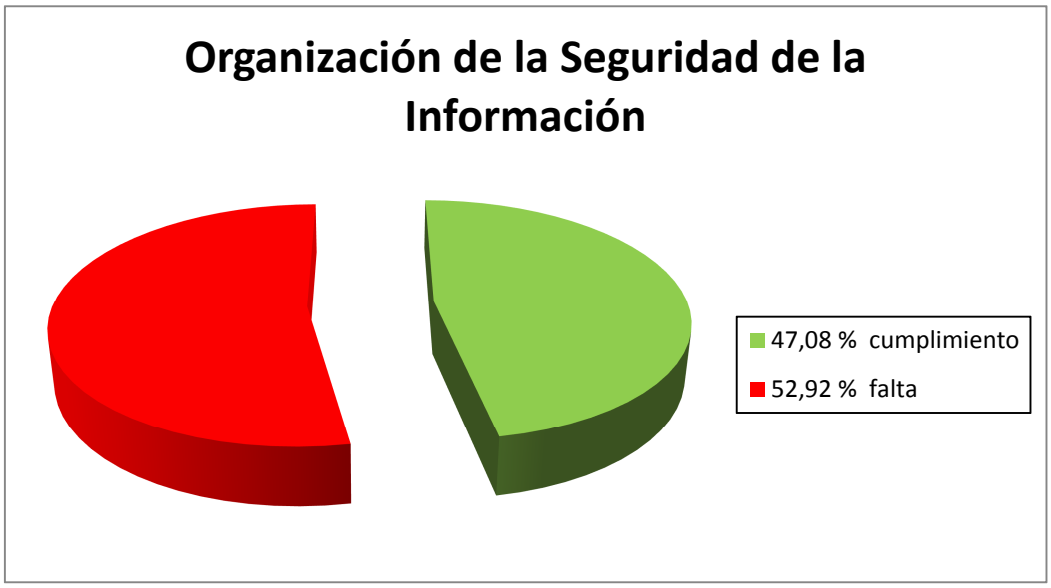
El resultado obtenido en ésta área es el siguiente:

4.1.2 Organización de la Seguridad de la Información

Dentro de ésta área, los objetivos que persigue descubrir y revisar son los siguientes:

- Administrar la seguridad de la información dentro de la Organización.
- Mantener la seguridad de las instalaciones de procesamiento y activos de información accedidos, procesados, comunicados o administrados por colaboradores externos.

Los resultados obtenidos en ésta área son los siguientes:

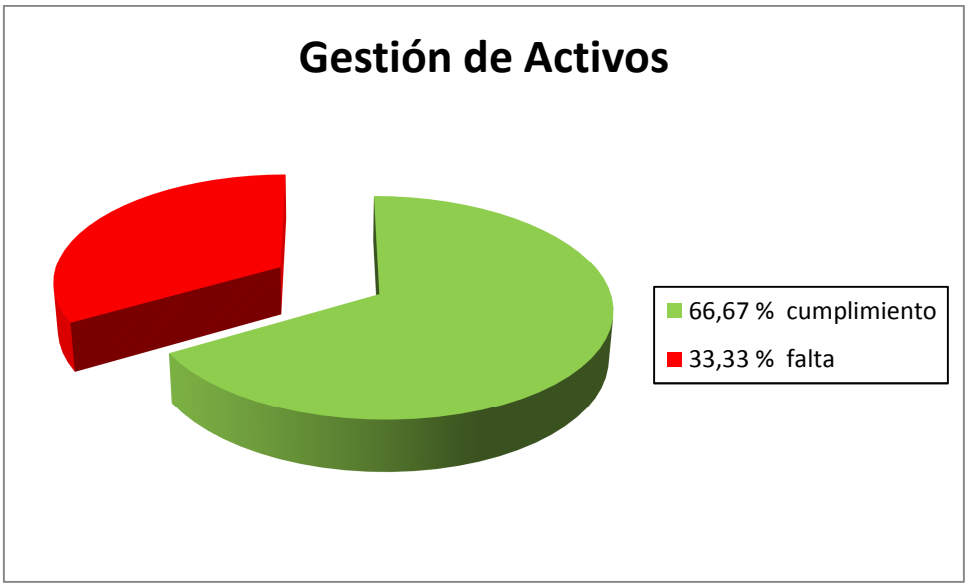


4.1.3 Gestión de Activos

Ésta área pretende revisar y descubrir los siguientes objetivos:

- Asegurar y mantener la protección apropiada de los activos de la Organización.
- Asegurar que la información recibe un nivel apropiado de protección.

El siguiente gráfico muestra los resultados obtenidos en ésta área:

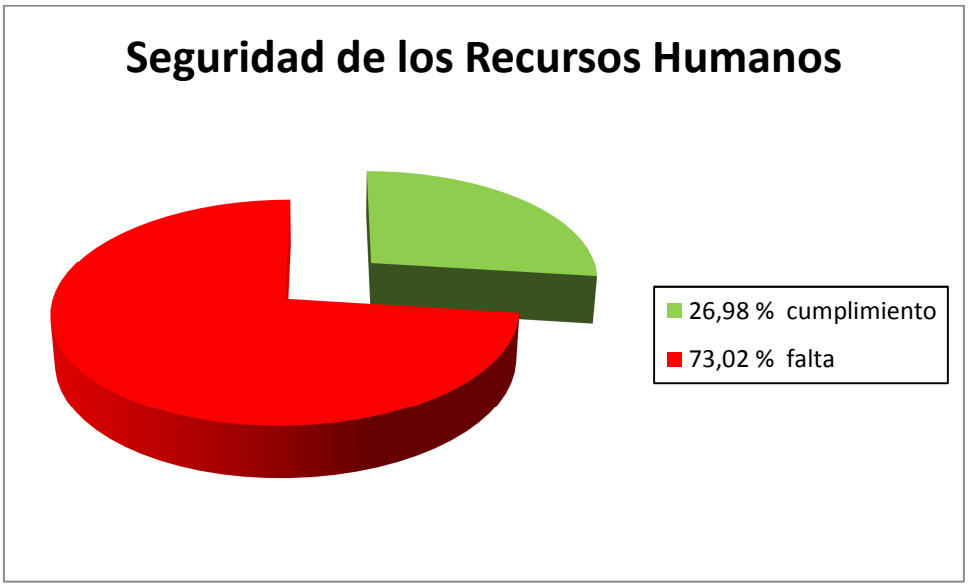


4.1.4 Seguridad de los Recursos Humanos

Los objetivos que persigue revisar y descubrir esta área son los siguientes:

- Asegurar que los empleados, contratistas y colaboradores externos comprendan sus responsabilidades y sean idóneos para los roles en los que han sido considerados, para prevenir robos, fraudes, o mal uso de las instalaciones.
- Asegurar que los usuarios estén conscientes de las amenazas a la seguridad de la información y sus graves consecuencias.
- Asegurar que los usuarios estén preparados para apoyar la política de seguridad de la Organización durante su trabajo.
- Asegurar que cuando un empleado, contratista o colaborador externo deja de tener una relación contractual con la Organización, éste abandona los nexos en forma controlada y reglamentada.

El resultado obtenido en ésta área es el siguiente:

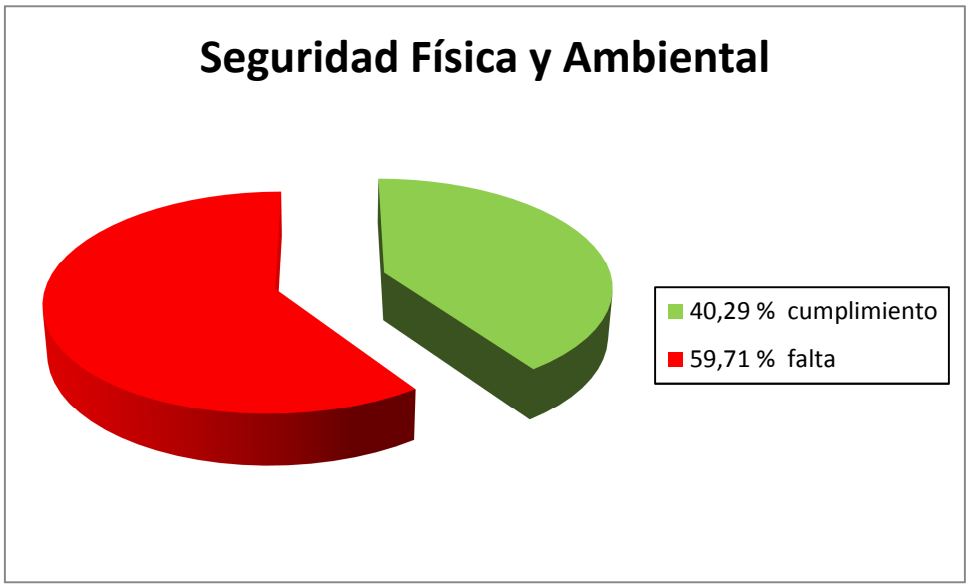


4.1.5 Seguridad Física y Ambiental

Dentro de ésta área, los objetivos que persigue descubrir y revisar son los siguientes:

- Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones e información de la Organización.
- Prevenir pérdida, daño o compromiso de activos o interpretación de las actividades organizacionales.

Los resultados obtenidos en ésta área son los siguientes:



4.1.6 Gestión de las Comunicaciones y Operaciones

Ésta área pretende revisar y descubrir los siguientes objetivos:

- Asegurar la correcta y segura operación de las instalaciones de procesamiento de la información.
- Implementar y mantener el nivel apropiado de seguridad de la información y de entrega de servicios externos alineados con los acuerdos.
- Minimizar el riesgo de falla de sistemas.
- Proteger la integridad del software y la información.
- Mantener la integridad y la disponibilidad de la información y las instalaciones de procesamiento.
- Asegurar la protección de la información en redes y la protección de la infraestructura de apoyo.
- Prevenir la divulgación, modificación, remoción o destrucción no autorizada de activos y la interrupción de las actividades del negocio.
- Mantener la seguridad de la información y el software intercambiado dentro de la organización y con cualquier entidad externa.
- Asegurar la seguridad de los servicios de comercio electrónico y su seguridad.
- Detectar actividades de procesamiento de información no autorizada.

El siguiente gráfico muestra los resultados obtenidos en ésta área:

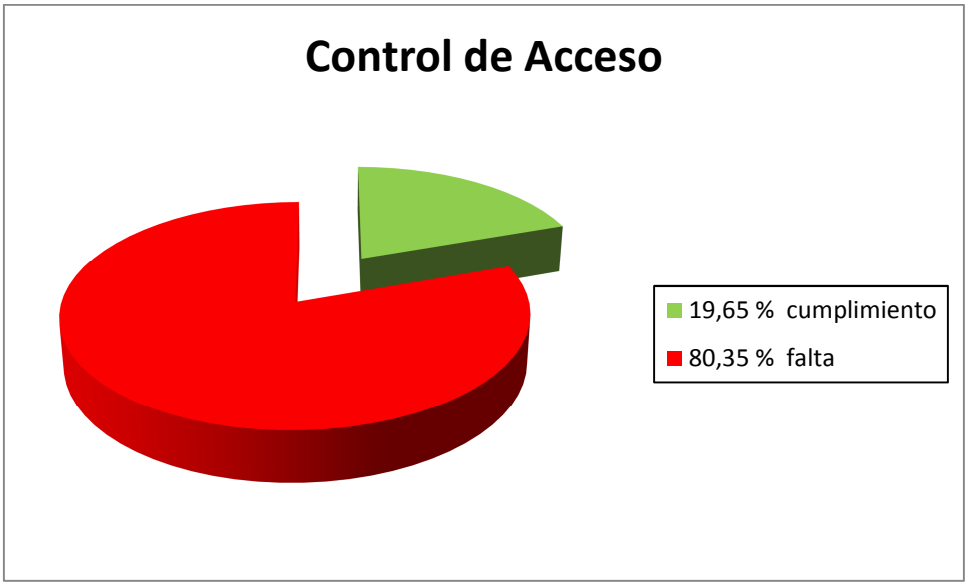
4.1.7 Control de Acceso

Dentro de ésta área, los objetivos que persigue descubrir y revisar son los siguientes:

- Controlar el acceso a la información.
- Asegurar que los privilegios de acceso a los Sistemas de Información estén apropiadamente autorizados, asignados y mantenidos.
- Asegurar que los usuarios autorizados tienen acceso y prevenir accesos no autorizados.
- Proteger los servicios de trabajo en red.
- Prevenir el acceso no autorizado a los Sistemas Operativos.
- Prevenir acceso no autorizado a la información utilizada por los Sistemas de Información.

- Asegurar la seguridad de la información y comunicación, cuando se utiliza computación móvil o tele-trabajo.

El siguiente gráfico muestra los resultados obtenidos en ésta área:



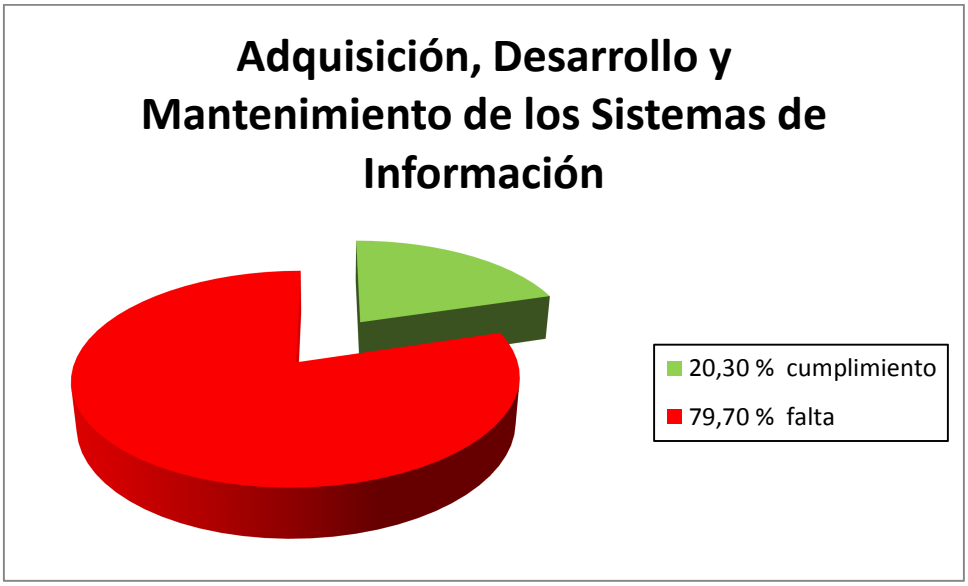
4.1.8 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Ésta área pretende revisar y descubrir los siguientes objetivos:

- Asegurar que la seguridad es parte integral de los sistemas de información.
- Prevenir errores, pérdida, modificaciones no autorizadas o mal uso de la información en las aplicaciones.
- Proteger la confidencialidad, autenticidad o integridad de la información.
- Asegurar seguridad en los sistemas de archivos.
- Mantener la seguridad del software de aplicación del sistema y de la información.

- Reducir el riesgo resultante de la explotación de las vulnerabilidades técnicas públicas.

Los resultados obtenidos para ésta área se muestran en el siguiente gráfico:

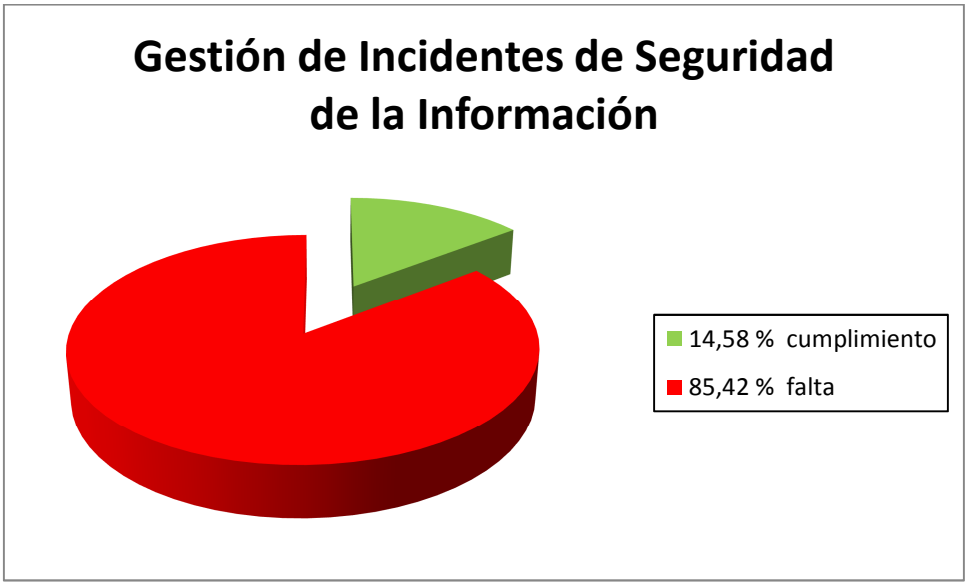


4.1.9 Gestión de Incidentes de Seguridad de la Información

Los objetivos que persigue descubrir y revisar esta área son los siguientes:

- Asegurar que los eventos de seguridad y debilidades asociadas a sistemas de información, sean comunicadas de modo que permitan tomar acciones correctivas.
- Asegurar que se aplica una aproximación consistente y efectiva a la gestión de incidentes de seguridad de la información.

El siguiente gráfico muestra los resultados obtenidos en ésta área:

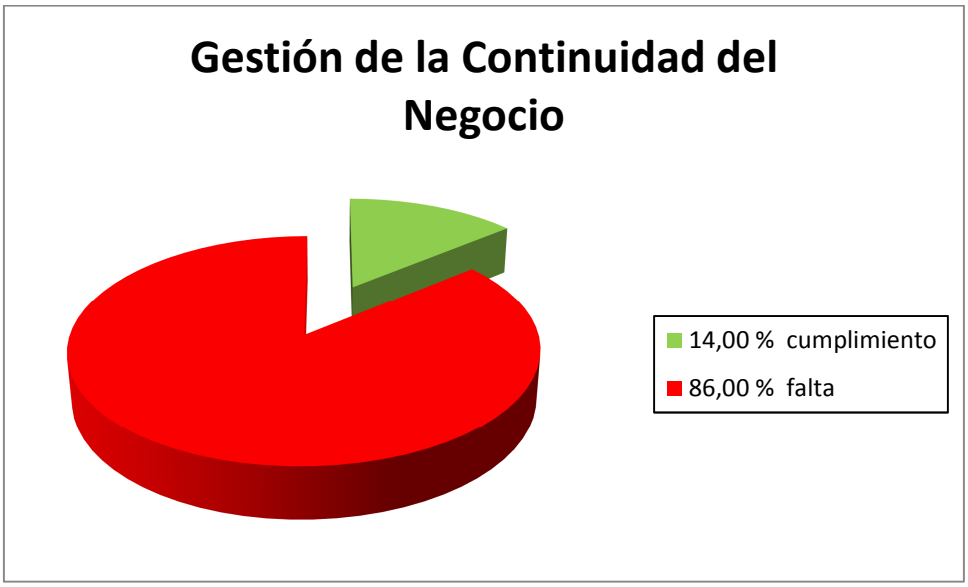


4.1.10 Gestión de la Continuidad del Negocio

Ésta área pretende revisar y descubrir el siguiente objetivo:

- Mitigar interrupciones a las actividades de negocio y proteger los procesos críticos del negocio, de los efectos de fallas mayores o desastres.

Los resultados obtenidos para ésta área se muestran en el siguiente gráfico:



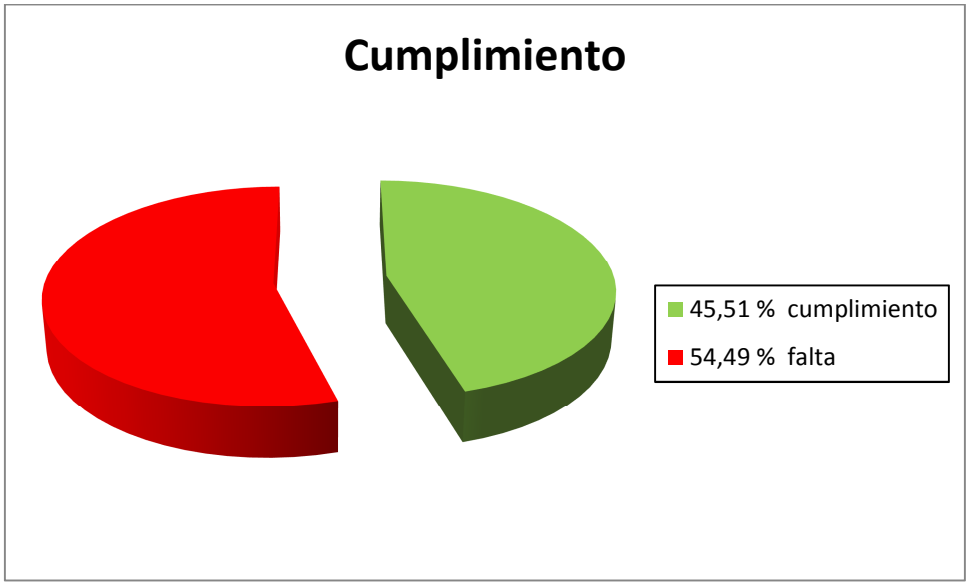
4.1.11 Cumplimiento

Ésta área pretende revisar y descubrir los siguientes objetivos:

- Evitar violaciones a cualquier ley, estatuto u obligación contractual o regulatoria y a cualquier requisito de seguridad.

- Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad de la organización.
- Maximizar la efectividad y minimizar la interferencia a, o desde, los procesos de auditoría.

El siguiente gráfico muestra los resultados obtenidos en ésta área:



5.0 CONCLUSIONES

La mayoría de las empresas, sobre todo las pequeñas y medianas, no toman muy en cuenta la vital importancia de mantener sus activos de información resguardados. En la presente tesis se aplicó la normativa ISO 27001, para lograr demostrar el enorme grado de vulnerabilidad que la empresa presenta, en las diferentes áreas analizadas.

Durante el proceso de aplicación de esta normativa, quedó de manifiesto que es muy robusta para aplicarla a una empresa pequeña o mediana, no es muy clara al momento de definir que se va a medir, debido a que sus enunciados son demasiado genéricos, conceptuales, ambiguos, y no representan una guía práctica para aplicarla en cada uno de los dominios que abarca.

Para aplicar la normativa primero se tuvo que entender a cabalidad cada enunciado, y transformarlo en una guía práctica que sirviera de modelo aplicable en cada una de las áreas de la empresa.

El resultado obtenido, resumido en una gráfica de tipo radar, permitió a la gerencia primero, darse cuenta del alto grado de vulnerabilidad, y segundo, tomar conciencia de la importancia de elevar el nivel de seguridad, sobre todo en al área de gestión de continuidad del negocio, tomando a futuro un compromiso de tomar medidas necesarias para mitigar los riesgos, desde acciones tan simples, y que no representan un gasto oneroso, como por ejemplo, poner contraseñas a los equipos, etc.

Podemos decir que el objetivo de la tesis se cumplió, ya que la empresa no solo tomó conciencia de elevar el nivel de seguridad, sino que también mostro un nivel de maduración frente al tema aplicado en la presente tesis

6.0 GLOSARIO

Activo: Cualquier cosa que tenga valor para la organización.

Amenaza: Una amenaza es cualquier cosa que puede suceder y que cuando ocurre, tiene consecuencias negativas sobre el valor de nuestros activos.

Análisis de Riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.

Autenticidad: Comprobación de que la fuente de datos recibidos es la alegada.

Confidencialidad: La propiedad que ésta información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Control: medio para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales (administrativas, técnicas, de gestión o de naturaleza legal). También es sinónimo de salvaguarda o contramedida.

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Evaluación del riesgo: Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evento de seguridad de la información: ocurrencia, identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión de riesgos: Selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.
NOTA. La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

Impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

Incidente de seguridad de la información: un evento o una serie de eventos "inesperados" de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.

Lineamiento: una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información: Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Riesgo residual: Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

Rootkit: Es un programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras

aplicaciones. El término proviene de una concatenación de la palabra inglesa root, que significa 'raíz' (nombre tradicional de la cuenta privilegiada en los sistemas operativos Unix) y de la palabra inglesa kit, que significa 'conjunto de herramientas' (en referencia a los componentes de software que implementan este programa). El término rootkit tiene connotaciones peyorativas ya que se lo asocia al malware.
En otras palabras, usualmente se lo asocia con malware, que se esconde a sí mismo y a otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a una amplia variedad de sistemas operativos como pueden ser GNU/Linux, Solaris o Microsoft Windows para remotamente comandar acciones o extraer información sensible.

Típicamente, un atacante instala un rootkit en una computadora después de primero haber obtenido un acceso al nivel raíz, ya sea por haberse aprovechado de una vulnerabilidad conocida o por haber obtenido una contraseña (ya sea por crackeo de la encriptación o por ingeniería social). Una vez que el rootkit ha sido instalado, permite que el atacante disfrace la siguiente intrusión y mantenga el acceso privilegiado a la computadora por medio de rodeos a los mecanismos normales de autenticación y autorización. Pese a que los rootktis pueden servir con muchos fines, han ganado notoriedad fundamentalmente como malware, escondiendo programas que se apropian de los recursos de las computadoras o que roban contraseñas sin el conocimiento de los administradores y de los usuarios de los sistemas afectados. Los rootkits pueden estar dirigidos al firmware, al hipervisor, al núcleo, ó, más comúnmente, a los programas del usuario.

La detección del rootkit es dificultosa pues es capaz de corromper al programa que debería detectarlo. Los métodos de detección incluyen utilizar un sistema operativo alternativo confiable; métodos de base conductual; controles de firma, controles de diferencias y análisis de volcado de memoria. La eliminación del rootkit puede ser complicada o prácticamente imposible, especialmente en los casos en que el rootkit reside en el núcleo; siendo a veces la reinstalación del sistema operativo el único método posible que hay para solucionar el problema.

Salvaguarda: Protección referente a las amenazas para los activos.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo y qué acción realizó.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

7.0 BIBLIOGRAFÍA

Referencias Bibliográficas:

- Internacional Standard. ISO/IEC 27001:2005. Information technology – Security tecniques – Information security management systems – Requierement.
- Internacional Standard. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management.
- Callio Technologies 2006 (http://www.calio.com/).
- Global Solution. Gestión de Riesgos. Implementación del SGSI Norma ISO/IEC 17799-BS7799.
- Global Solution. Gestión de Riesgos de la Información. Modelo BS7799
- Microsoft Tech-Net. Guía de Administración de riesgos de seguridad (http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx).
- Libro Electrónico de Seguridad Informática y Criptografía (http://www.criptored.upm.es/guiateoria/gt_m001a.htm)
- Libro “SEGURIDAD DE LA INFORMACIÓN”, Vicente Aceituno Canal (Creaciones Copyright)
- http://www.it360.es/trazabilidad-iso27001-seguridad-es-gran-olvidado.php

8.0 ANEXOS

			Resultados		Checklist	
			Área	Objetivo de Control	Realizados	Considerados
Área: Política de Seguridad			0,00			
1.1	5.1	Política de seguridad de la información		0,00	7	7
Área: Organización de la Seguridad de la Información			47,08			
2.1	6.1	Organización interna		27,50	8	8
2.2	6.2	Entidades externas		66,66	3	3
Área: Gestión de Activos			66,67			
3.1	7.1	Responsabilidad de activos		83,33	3	3
3.2	7.2	Clasificación de la información		50,00	2	2
Área: Seguridad de los recursos humanos			26,98			
4.1	8.1	Antes del empleo		14,29	7	7
4.2	8.2	Durante el empleo		33,33	3	3
4.3	8.3	Término del empleo		33,33	3	3
Área: Seguridad física y ambiental			40,29			
5.1	9.1	Áreas seguras		38,57	7	7
5.2	9.2	Seguridad de equipamiento		42,00	15	15
Área: Gestión de las comunicaciones y Operaciones			15,26			
6.1	10.1	Procedimientos de operaciones y responsabilidades		20,00	5	5
6.2	10.2	Administración de servicios de terceras partes (Outsourcing)		0,00	4	4
6.3	10.3	Planificación y aceptación de sistemas		16,66	3	3
6.4	10.4	Protección contra código malicioso o móvil		12,50	4	4
6.5	10.5	Respaldos		65,00	2	2
6.6	10.6	Administración de redes		5,00	4	4
6.7	10.7	Manipulación de medios		0,00	6	6
6.8	10.8	Intercambio de información		0,00	7	7
6.9	10.9	Servicio de comercio electrónico		0,00	5	5
6.10	10.10	Monitoreo		18,18	11	11
Área: Control de acceso			19,65			

7.1	11.1	Requerimientos de la empresa para el control de acceso		0,00	3	3
7.2	11.2	Administración de accesos de usuarios		26,00	5	5
7.3	11.3	Responsabilidad de los usuarios		6,66	3	3
7.4	11.4	Control de acceso a redes		9,09	11	11
7.5	11.5	Control de accesos a Sistemas Operativos		4,13	8	8
7.6	11.6	Control de accesos a la aplicaciones e información		75,00	2	2
7.7	11.7	Computación móvil o tele-trabajo		16,66	3	3
Área: Adquisición, desarrollo y mantenimiento de los sistemas de información			20,30			
8.1	12.1	Requerimientos de seguridad para los Sistemas de Información		0,00	3	3
8.2	12.2	Procesamiento correcto de las aplicaciones		85,71	7	7
8.3	12.3	Controles criptográficos		0,00	8	8
8.4	12.4	Seguridad de los archivos del sistema		25,00	4	4
8.5	12.5	Seguridad de los procesos de desarrollo y soporte		11,11	9	9
8.6	12.6	Gestión de vulnerabilidades técnicas		0,00	1	1
Área: Gestión de incidentes de seguridad de la información			14,58			
9.1	13.1	Reportando eventos y debilidades en la seguridad de la información		16,66	3	3
9.2	13.2	Gestión de incidentes y mejoras en la seguridad de la información		12,50	8	8
Área: Gestión de la continuidad del negocio			14,00			
10.1	14.1	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio		14,00	10	10
Área: Cumplimiento			45,51			
11.1	15.1	Cumplimiento con requerimientos legales		61,53	13	13
11.2	15.2	Cumplimiento con políticas y estándares de seguridad y cumplimento técnico		62,50	4	4
11.3	15.3	Consideraciones de auditoría de sistemas de información		12,50	4	4

Área: Política de Seguridad					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
1.1	5.1	**Política de seguridad de la información**			
1.1.1	5.1.1	**Documentación de la política de seguridad de la información**	Hay Información de política de seguridad la que esté aprobada por la administración, publicada y comunicada adecuadamente a todos los empleados	No	0
			La política indica el compromiso de la administración e intenta un enfoque de la organización en el manejo de la seguridad de información. (La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes.)	No	0
1.1.2	5.1.2	**Revisión y evaluación de la política de seguridad de la información**	Si la Política Informativa de Seguridad es revisada a intervalos planificados, o si se dan cambios significativos para asegurar su continuidad conveniente, adecuada y efectiva.	No	0
			La Política Informativa de Seguridad tiene un propietario que tenga responsabilidad administrativa aprobada para el desarrollo, revisión y evaluación de la seguridad	No	0
			Existen algunos procedimientos definidos de revisión de Política de Seguridad de Información y si ellos incluyen requisitos para la revisión de la administración.	No	0
			Los resultados de la revisión administrativa son tomados en cuenta.	No	0
			Se obtiene la aprobación administrativa para la política revisada.	No	0

			(La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.)		

Área: Organización de la Seguridad de la Información					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
2.1	6.1	**Organización Interna**			
2.1.1	6.1.1	**Participación de la gerencia en la seguridad de la información**	La administración demuestra un apoyo activo para las medidas de seguridad dentro la organización. Esto puede ser realizado vía dirección clara compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información. (Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización.)	Si	100
2.1.2	6.1.2	**Coordinación de la seguridad de la información**	La seguridad de información vigentes están coordinadas por representantes de diversas áreas de la organización con roles y responsabilidad pertinentes. (Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.)	Medianamente	30
2.1.3	6.1.3	**Asignación de responsabilidades de seguridad de la información**	Hay responsabilidades para la protección de los bienes particulares y el llevar a cabo los procesos específicos, fueron claramente identificados y definidos. (Se deberían definir claramente todas las responsabilidades para la seguridad de la	No	0

			información.)		
2.1.4	6.1.4	**Proceso de autorización para las instalaciones de procesamiento de seguridad de la información**	Existe un mecanismo de autorización administrativa definido e implementado para el fácil procesamiento de alguna aplicación nueva dentro de la organización. (Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información.)	No	0
2.1.5	6.1.5	**Acuerdos de confidencialidad**	Hay la necesidad de la organización para la Confidencialidad o Acuerdo de No Revelación (Información Reservada), para la protección de información y está claramente definida y revisadas regularmente.	No	0
			Cumple la organización con el requisito para proteger la información confidencial usando términos legales aplicables. (Se deberían identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización.)	Si	100
2.1.6	6.1.6	**Contacto con autoridades**	Existe un procedimiento que describa, cuando y a quien: autoridades relevantes tales como la Carabineros, bomberos, etc., deberían ser contactados, y como el incidente debería ser reportado. (Se deberían mantener los contactos apropiados con las autoridades pertinentes.)	No	0
2.1.7	6.1.7	**Contacto con grupos de interés especial**	Se mantienen contactos apropiados con grupo de especial interés o con foros de otros especialistas en seguridad o asociaciones profesionales.	Medianamente	40

			(Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.)		
2.1.8	6.1.8	**Revisiones independientes de seguridad de la información**	El enfoque de la organización a manejar la seguridad de información y su implementación, es revisada independientemente en intervalos planeados o cuando cambios mayores a la implementación de seguridad se dan. (Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.)	No	0
2.2	6.2	**Entidades externas**			
2.2.1	6.2.1	**Identificación de riesgo derivados del acceso de terceros**	¿Hay riesgos a la información de la organización y su fácil procesamiento, derivados de procesos externos? ¿Están identificadas e implementadas las medidas de control, previa entrega del acceso? (Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.)	Medianamente	50
2.2.2	6.2.2	**Directriz de seguridad en el trato con clientes**	Hay requisitos de seguridad que se cumplen antes de otorgar a los clientes acceso a la información propia de la organización.	Si	100

			(Se deberían anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.)		
2.2.3	6.2.3	**Directriz de seguridad en el acuerdo con terceras partes**	Hay acuerdos con terceros que involucran acceso, procesamiento, comunicación o administración de la información de la organización, o facilidad de procesamiento de información, o la introducción de productos o servicios para el procesamiento de información. Obedecen todos los requisitos adecuados de seguridad. (Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.)	Medianamente	50

Área: Gestión de Activos					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
3.1	7.1	**Responsabilidad de activos**			
3.1.1	7.1.1	**Inventario de activos**	Todos los activos están identificados, hay un inventario y si se mantiene un registro con todos los activos importantes. (Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.)	Si	100
3.1.2	7.1.2	**Propiedad de activos**	Si cada activo tiene identificado tiene un dueño, o más, definido, y la clasificación de la seguridad y restricciones de acceso que son revisadas periódicamente (Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.)	Medianamente	50
3.1.3	7.1.3	**Uso aceptable de activos**	Hay regulaciones para el uso de la información privilegiada, asociados con una facilidad de procesamiento (software) que están identificados, documentados e implementados. (Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.)	Si	100
3.2	7.2	**Clasificación de la información**			
3.2.1	7.2.1	**Guías para clasificación**	Hay información que está clasificada en términos de su valor, requisitos legales, sensibilidad y críticas para la organización. (La información debería clasificarse en	Si	100

			relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.)		
3.2.2	7.2.2	**Manejo de etiquetado de la información**	Si se ha definido un set de procedimientos para el etiquetado y manejo de la información, de acuerdo con la clasificación del esquema adoptado por la organización. (Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización.)	No	0

Área: Seguridad de los recursos humanos					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
4.1	8.1	**Antes del empleo**			
4.1.1	8.1.1	**Roles y responsabilidades**	Los roles y responsabilidades de los empleados de seguridad, contratistas, y terceros fueron definidos y documentados de acuerdo con la política de seguridad de información de la organización. (Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.)	No	0
			Fueron los roles y responsabilidades definidos y comunicados claramente a los postulantes al trabajo durante el proceso de postulación.	Si	100
4.1.2	8.1.2	**Investigación de antecedentes**	Hay comprobación del origen de todos los candidatos para el empleo, contratistas y terceros, y el proceso fue llevado a cabo de acuerdo a las regulaciones pertinentes.	No	0
			Hay chequeo que incluye las referencias, confirmación de antecedentes académicos, profesionales y verificación de la identidad. (Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.)	No	0
4.1.3	8.1.3	**Términos y condiciones del empleo**	Si a empleados, contratistas y terceros se	No	0

			les solicito firmar confidencialmente un acuerdo de privacidad, como parte de los términos y condiciones del contrato de empleo.		
			El acuerdo cubre las responsabilidades de seguridad de información de la organización con el empleado, usuarios o contratistas. (Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.)	No	0
4.1.4	8.1.4	**Términos y condiciones del empleo**	Si los términos y condiciones del empleo cubren la responsabilidad de seguridad de información. Se considera apropiado que estas responsabilidades continuaran por un periodo de tiempo definidos después del término del trabajo.	No	0
4.2	8.2	**Durante el empleo**			
4.2.1	8.2.1	**Responsabilidades administrativas**	La administración requiere empleados, contratistas y terceros para aplicar la seguridad de acuerdo con las políticas establecidas y procedimientos de la organización. (La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes PARA aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.)	Si	100
4.2.2	8.2.2	**Capacitación, educación y entrenamiento en seguridad de información**	Todos los empleados en la organización, contratistas y terceros reciben capacitación, relacionadas con las labores de su trabajo.	No	0

			(Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.)		
4.2.3	8.2.3	**Proceso disciplinario**	Si hay un proceso disciplinario formal para los empleados que han cometido una infracción de la seguridad. (Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.)	No	0
4.3	8.3	**Término del empleo**			
4.3.1	8.3.1	**Responsabilidades de término de contrato**	Las responsabilidades para realizar la finalización del empleo, o cambio, están claramente definidas (Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas.)	No	0
4.3.2	8.3.2	**Reintegro de activos**	Existe un proceso que asegure que los bienes prestados a los empleados, contratistas y terceros de toda la organización, sean devueltos al término de sus empleos, contratos o acuerdo. (Todos los empleados, contratistas y terceros deberían devolver todos los activos de la organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo.) (El proceso de finalización debería estar formalizado para incluir el retorno previo de los software, documentos corporativos y	No	0

			equipos. Otros activos de la organización como dispositivos móviles de computo, tarjetas de crédito, tarjetas de acceso, manuales, software e información guardada en medios electrónicos, también necesitan ser devueltos. En casos donde el empleado, contratista o tercero compra el equipo de la organización o usa su propio equipo, se debería seguir procedimientos para asegurar que toda la información relevante es transferida a la organización y borrado con seguridad del equipo (consultar 10.7.1). En casos donde un empleado, contratista o tercero tiene conocimiento que es importante para las operaciones en curso, esa información debe ser documentada y transferida a la organización.)		
4.3.3	8.3.3	**Remoción de derechos de acceso**	Los derechos de acceso de todos los empleados, contratistas y terceros, a la información y facilidades de procesamiento de información, son eliminados cuando terminan sus empleos, contrato o acuerdo, o son reasignados a su reemplazante.	Si	100

Área: Seguridad física y ambiental					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
5.1	9.1	**Áreas seguras**			
5.1.1	9.1.1	**Perímetro de seguridad física**	Ha sido implementada una capa física de seguridad para proteger el servicio de procesamiento de información. (Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.)	Medianamente	70
5.1.2	9.1.2	**Controles de acceso físico**	Existen áreas de la organización con controles de entrada para permitir solo el ingreso de personal autorizado. (Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.)	No	0
5.1.3	9.1.3	**Seguridad de las oficinas, salas e instalaciones**	Los lugares en los cuales existe un servicio de procesamiento de información están cerrados o cuentan con cerrojos que se puedan cerrar en forma segura. (Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.)	No	0
5.1.4	9.1.4	**Protección contra amenazas externas y ambientales**	Están diseñadas las protecciones físicas contra los daños del fuego, inundaciones, terremotos, explosiones, disturbios civiles, otras formas naturales o desastres provocados por el hombre.	Medianamente	50
			Si existe alguna amenaza potencial de parte de vecinos altamente riesgosos. Están tomadas las medidas de seguridad	Medianamente	50

			necesarias para mitigarla. (Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.)		
5.1.5	9.1.5	**Trabajando en áreas seguras**	Están diseñadas e implementadas las protecciones físicas y directrices para trabajar en áreas seguras. (Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras.)	Medianamente	50
5.1.6	9.1.6	**Área de acceso público, carga y descarga**	Los centros de cómputos se aíslan del acceso del personal de despacho, cargas y otras áreas donde hay personas no autorizadas en la organización (Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.)	Medianamente	50
5.2	9.2	**Seguridad de equipamiento**			
5.2.1	9.2.1	**Ubicación y protección de equipos**	Los equipos están protegidos para reducir los riesgos de amenazas del medio ambiente u otros peligros y la posibilidad de acceso a personas no autorizadas. (El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.)	Medianamente	70
5.2.2	9.2.2	**Herramientas de apoyo**	Los equipos están protegidos con utilitarios para fallas del suministro eléctrico y otras	Medianamente	70

			interrupciones		
			El abastecimiento de respaldo energía, tales como, múltiples y generador de respaldo, están siendo usados. (Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.)	Medianamente	70
5.2.3	9.2.3	**Seguridad del cableado**	Los cables de comunicación, que transmite la información o servicios de apoyo de información, están protegidos de interferencias o daños.	Si	100
			Hay algunos controles de seguridad adicionales para la información delicada o crítica. (Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.)	No	0
5.2.4	9.2.4	**Mantenimiento de equipos**	Los equipos están correctamente mantenidos para asegurar su continua disponibilidad e integridad.	Medianamente	50
			Los equipos reciben mantención periódica, tal como lo recomiendan los suministradores y especificaciones. (Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.)	Medianamente	50
			La mantención es llevada a cabo sólo por personal autorizado.	Si	100
			Los registros de mantención se guardan	No	0

			con todas las correcciones, defectos reales y medidas preventivas.		
			Si los controles apropiados están implementados al realizar la mantención dentro de la organización.	Medianamente	50
			Están los equipos cubiertos por el seguro y los requisitos del seguro satisfacen.	No	0
5.2.5	9.2.5	**Seguridad de equipos fuera de las instalaciones**	Si los riesgos se valoraron con respecto a cualquier uso del equipo fuera de la organización local y controles de mitigación implementaron.	No	0
			El uso de la facilidad del proceso de la información afuera de la organización ha sido autorizado por la administración. (Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.)	No	0
5.2.6	9.2.6	**Seguridad en el reciclaje y deshecho de equipos**	Todo el equipamiento, contenido de medios de almacenamiento, esta revisado para asegurar que la información delicada o software licenciado sea físicamente destruido, o reescrito, antes de ser eliminado o devuelto. (Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.)	No	0
5.2.7	9.2.7	Retirada de materiales propiedad de la empresa. (Traslado de activos)	Hay controles que son en los equipos, en la información y el software, para que no sean tomados fuera sin la autorización respectiva.	Medianamente	70

			(No deberían sacarse equipos, información o software fuera del local sin una autorización.)		

Área: Gestión de las comunicaciones y Operaciones					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
6.1	10.1	**Procedimientos de operaciones y responsabilidades**			
6.1.1	10.1.1	**Documentación de los procedimientos operativos**	Los procedimientos de operación están documentados, mantenidos y disponibles para todos los usuarios que lo necesiten.	No	0
			Tales procedimientos están considerados como documentos formales, que en caso de cualquier cambio, necesiten la autorización de la administración. (Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.)	No	0
6.1.2	10.1.2	**Control de cambios operacionales**	Todos los cambios en los procesos de información y sistemas están controlados. (Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.)	No	0
6.1.3	10.1.3	**Segregación de tareas**	Las tareas y áreas de responsabilidades están separadas, reduciendo de esta forma las oportunidades para modificaciones no autorizadas o uso indebido de información o servicios. (Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.)	Si	100

6.1.4	10.1.4	**Separación de instalaciones de desarrollo de pruebas**	El desarrollo y prueba de sistemas están aislados del área de producción (La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.)	No	0
6.2	10.2	**Administración de servicios de terceras partes (Outsourcing)**			
6.2.1	10.2.1	**Prestación de servicios**	Hay medidas incluidas en el contrato de entrega de servicios de terceros, que se toman para los controles de seguridad, definiciones de servicio y niveles de entrega, que estén implementados, operados y mantenidos por los terceros. (Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.)	No	0
6.2.2	10.2.2	**Monitoreo y revisión de os servicios prestados por terceros**	Todos los servicios, informes y registros proporcionados por los terceros, son monitoreados y revisados regularmente.	No	0
			Hay auditorías realizadas en intervalos regulares a los servicios de terceros, las que generan informes y registros. (Los servicios, informes y registros suministrados por terceros deberían ser monitoreados y revisados regularmente, y las auditorías se deberían realizar a intervalos regulares.)	No	0
6.2.3	10.2.3	**Administración de cambios de los**	Existe una gestión realizada a los cambios	No	0

		servicios prestados por terceros	en la entrega de servicios, los que incluyen el perfeccionamiento de las políticas de seguridad existentes, procedimientos y controles. (Se deberían gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes, en los procedimientos y los controles teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.)		
6.3	10.3	**Planificación y aceptación de sistemas**			
6.3.1	10.3.1	**Verificación de capacidades**	Las capacidades de los recursos de los servidores son monitoreadas y proyectadas, de manera tal de anticiparse a problemas futuros (Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.)	No	0
6.3.2	10.3.2	**Aceptación de sistemas**	Los criterios de aceptación del sistema tienen establecidos mecanismos para las nuevas configuraciones, actualizaciones y versiones.	Medianamente	50
			Las pruebas pertinentes fueron llevadas a cabo con antelación a la aceptación. (Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.)	No	0
6.4	10.4	**Protección contra código malicioso o móvil**			

6.4.1	10.4.1	**Controles contra código malicioso**	Los procedimientos, para protegerse de códigos malicioso, fueron desarrollados e implementados para la detección, prevención y controles de recuperación. (Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.)	No	0
6.4.2	10.4.2	**Controles a código móvil**	Solamente los códigos móviles identificados tienen acceso	No	0
			La configuración asegura que el código móvil autorizado opera de acuerdo a la política de seguridad.	No	0
			La ejecución de un código móvil no autorizado es impedida. (Cuando se autoriza la utilización de código móvil, la configuración debería asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos móviles no autorizados.)	Medianamente	50
6.5	10.5	**Respaldos**			
6.5.1	10.5.1	**Respaldo de información**	Los respaldos de información y software son hechos y probados, regularmente, en concordancia con la política de respaldo.	Medianamente	50
			La información esencial y software pueden ser recuperados después de un desastre o falla. (Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con	Medianamente	80

			la política acordada de recuperación.)		
6.6	10.6	**Administración de redes**			
6.6.1	10.6.1	**Controles de redes**	La red es administrada y monitoreada adecuadamente, para protegerla de amenazas y para mantener la seguridad de los sistemas y aplicaciones que la utilizan, incluyendo la información en tránsito.	Medianamente	20
			Los controles fueron implementados para asegurar la seguridad de información en las redes y la protección de los servicios conectados, en contra de las amenazas, tales como accesos no autorizados. (Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.)	No	0
6.6.2	10.6.2	**Seguridad de los servicios de red**	Las características de seguridad, niveles de servicio y requisitos administrativos, de todos los servicios de redes, están instalados en todos los servicios de todas las redes de la organización. (Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.)	No	0
			La habilidad de los proveedores de servicios de red, para administrar los servicios de una forma segura, es	No	0

			determinada y monitoreada regularmente, y el derecho de auditoria está acordado.		
6.7	10.7	**Manipulación de medios**			
6.7.1	10.7.1	**Administración de medios removibles**	Existen los procedimientos para la administración de medios removibles, tales como pen-drives, cintas, diskettes, tarjetas de memoria e informes.	No	0
			Los procedimientos y niveles de autorización están informados, definidos claramente y documentados. (Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.)	No	0
6.7.2	10.7.2	**Eliminación de soportes**	Son eliminados los medios de almacenamiento masivo, si no son utilizados (utilización de herramientas de borrado seguro de soportes) (Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales)	No	0
6.7.3	10.7.3	**Procedimientos de manejo de información**	Existe un procedimiento para el manejo de almacenamiento de información.	No	0
			Apunta este procedimiento a la protección de la información, de la revelación no autorizada o uso indebido. (Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados)	No	0
6.7.4	10.7.4	**Seguridad de la documentación de**	El sistema de documentación está	No	0

		sistemas	protegido de los accesos no autorizados. (Se debería proteger la documentación de los sistemas contra accesos no autorizados)		
6.8	10.8	**Intercambio de información**			
6.8.1	10.8.1	**Procedimientos y políticas de intercambio de información**	Existe un procedimiento de intercambio formal de políticas de control, para asegurar la protección de información.	No	0
			Los procedimientos y controles sobre el uso de las comunicaciones, cubren el intercambio de información. (Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.)	No	0
6.8.2	10.8.2	**Acuerdos de intercambio**	Los acuerdos están establecidos en relación al intercambio de información y software, entre la organización y externos a ella.	No	0
			El contenido del acuerdo de seguridad refleja la sensibilidad de la información involucrada. (Se deberían establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.)	No	0
6.8.3	10.8.3	**Medios físicos en tránsito**	La información dentro los medios está protegida de los accesos no autorizados, usos indebidos o corrupción durante el transporte más allá de la frontera física de la organización. Por ejemplo uso de aplicativos que crean particiones ocultas y con cifrado en cualquier unidad USB Flash, accesible solo	No	0

			con contraseña. (ROHOS) (Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.)		
6.8.4	10.8.4	**Mensajería electrónica**	La información inserta en la mensajería electrónica está bien protegida. Por ejemplo aplicativos que cifran los adjuntos en los e-mail enviados. (Se debería proteger adecuadamente la información contenida en la mensajería electrónica.)	No	0
6.8.5	10.8.5	**Sistemas de información del negocio**	Las políticas y procedimientos están desarrollados y se hacen cumplir para proteger la información asociada con la interconexión de los sistemas de información del negocio. (Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información del negocio.)	No	0
6.9	10.9	**Servicio de comercio electrónico**			
6.9.1	10.9.1	**Comercio electrónico**	La información involucrada con el comercio electrónico, que pasa a través de redes públicas, está protegida de la actividad fraudulenta, conflictos de contrato, algún acceso no autorizado o modificación.	No	0
			El control de Seguridad, tal como la aplicación de controles de cifrados, ha sido tomado en cuenta.	No	0

			Los acuerdos del comercio electrónico entre socios comerciales incluye un contrato documentado, el cual compromete a ambas partes a cumplir los términos del negocio, incluyendo detalles de seguridad. (Se debería proteger la información involucrada en el comercio electrónico que pasa por redes públicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.)	No	0
6.9.2	10.9.2	**Transacciones en línea**	Si la información involucrada en la transacción en línea está protegida para prevenir una transmisión incompleta, pérdida de la comunicación, alteración del mensaje, revelación no autorizada, duplicación de mensaje, no autorización o repetición. (Se debería proteger la información involucrada en el comercio electrónico que pasa por redes públicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.)	No	0
6.9.3	10.9.3	**Información disponible al público**	La integridad de la información publicada y disponible, está protegida de cualquier modificación no autorizada. (Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas.)	No	0
6.10	10.10	**Monitoreo**			
6.10.1	10.10.1	**Registro de auditoría**	La auditoría apunta a los registros de las actividades de los usuarios, excepciones e información de eventos de seguridad que	No	0

			se producen, y se mantienen, durante un periodo acordado, para ayuda de futuras investigaciones y monitoreo de control de acceso.		
			Las medidas adecuadas de protección de Privacidad son consideradas en la mantención del registro de Auditoria. (Se deberían producir y mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.)	No	0
6.10.2	10.10.2	**Uso de sistemas de monitoreo**	Los procedimientos de monitoreo de procesamiento de información están desarrollados y se hace cumplir su funcionamiento	No	0
			El resultado de la actividad de monitoreo es revisada regularmente.	No	0
			El nivel de monitoreo requerido para el procesamiento de información individual, está determinado por una evaluación de riesgo. Por ejemplo uso de aplicativos para la recolección, análisis, informes y archivo de logs de eventos permite habilitar un completo sistema de monitorización y gestión. Otro ejemplo, herramientas de monitoreo de servidores, aplicaciones, y redes. (Se deberían establecer procedimientos	No	0

			para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo.)		
6.10.3	10.10.3	**Protección de la información de los registros**	El registro de información está bien protegido de la manipulación y accesos no autorizados. (Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.)	No	0
6.10.4	10.10.4	**Registro de operación del administrador y operador**	Son registrados los procesos del administrador y operador de sistemas	No	0
			Los registros de actividades son revisados regularmente (Se deberían registrar las actividades del administrador y de los operadores del sistema.)	No	0
6.10.5	10.10.5	**Registros de fallas**	Las fallas registradas son analizadas y se toman las medidas apropiadas.	Medianamente	50
			El nivel del registro de falla, requerido para un sistema individual, está determinado por una evaluación, tomando en consideración la degradación del rendimiento del sistema. (Se deberían registrar, analizar y tomar acciones apropiadas de las averías.)	Medianamente	50
6.10.6	10.10.6	**Sincronización de relojes**	Si el sistema de relojes de todo el sistema de procesamiento de información, dentro de la organización o dominio de seguridad,	Si	100

			esta cuidadosamente sincronizado. (Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.)		

Área: Control de acceso					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
7.1	11.1	**Requerimientos de la empresa para el control de acceso**			
7.1.1	11.1.1	**Política de control de acceso**	Si hay una política de control de acceso desarrollada y revisada en base al negocio y requisitos de seguridad.	No	0
			Se considera la parte lógica como el control de acceso físico en la política.	No	0
			Se les entregó a los usuarios y proveedores una visión clara del requisito del negocio (Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.)	No	0
7.2	11.2	**Administración de accesos de usuarios**			
7.2.1	11.2.1	**Registro de usuarios**	Existe un procedimiento de registro de ingreso y salida, que garantice el acceso de todos los sistemas de información y servicios. (Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.)	No	0
7.2.2	11.2.2	**Administración de privilegios**	La asignación al uso de algunos privilegios, en el ambiente de sistema de información, está restringido y controlado, es decir, hay privilegios en base a la necesidad de uso, y estos privilegios están asignados después de una proceso de autorización formal.	Medianamente	80

			(Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.)		
7.2.3	11.2.3	**Administración de contraseñas de usuarios**	La asignación y reasignación de contraseña es controlada a través de un proceso de administración formal.	Medianamente	50
			Se les solicito a los usuarios firmar un compromiso de confidencialidad de contraseña. (Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal.)	No	0
7.2.4	11.2.4	**Revisión de derecho de acceso de usuarios**	Existe un proceso de revisión, a intervalos regulares, de los derechos de acceso de los usuarios. Ejemplo: revisión de privilegio especial cada 3 meses, privilegios normales cada 6 meses. (El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.)	No	0
7.3	11.3	**Responsabilidad de los usuarios**			
7.3.1	11.3.1	**Uso de contraseñas**	Existe una práctica segura para guiar a los usuarios a seleccionar y mantener contraseñas seguras. (Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.)	No	0
7.3.2	11.3.2	**Equipos informático de usuario**	Los usuarios y contratistas están	Medianamente	20

		desatendido por el usuario	conscientes de los requisitos de seguridad y procedimientos para proteger el equipo desatendido. Ejemplo establecer Logoff cuando la sesión se acaba, terminar la sesión cuando termina, etc. (Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.)		
7.3.3	11.3.3	**Política de escritorio y pantallas limpios**	Los usuarios están informados de la seguridad y orden que deben tener dentro de sus computadores personales (Se debiera adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información)	No	0
7.4	11.4	**Control de acceso a redes**			
7.4.1	11.4.1	**Políticas de uso de servicios de red**	Los usuarios tienen acceso solamente a los servicios que han sido específicamente autorizados a usar.	No	0
			Existe una política que involucre las direcciones IP de una red y los servicios de la red. (Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.)	No	0
7.4.2.	11.4.2	**Autenticación de usuarios para conexiones externas**	Se usa un mecanismo apropiado de autenticación para controlar el acceso de usuarios remotos. (Se debieran utilizar métodos de autenticación apropiados para controlar el acceso de usuarios	Si	100

			Remotos)		
7.4.3	11.4.3	**Identificación de los equipos en la red**	La identificación automática del equipo está considerada como un medio de autenticar las conexiones, desde una localización o equipo especifico. (Se debería considerar la identificación automática de los equipos como un medio de autenticación de conexiones procedentes de lugares y equipos específicos.)	No	0
7.4.4	11.4.4	**Protección de puertos de configuración y diagnóstico remoto**	El diagnóstico de los acceso físico y lógico a los puertos se controla en forma segura, es decir, si está protegida por un mecanismo de seguridad. (Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.)	No	0
7.4.5	11.4.5	**Segregación de redes**	Los grupos de servicios de información, usuarios y sistemas de información están segregados en las redes.	No	0
			Si la red (que es utilizada por organizaciones relacionadas y/o terceros que necesitan el acceso al sistema de información), es segregada usando mecanismos de perímetro de seguridad tales como los cortafuego.	No	0
			Se considera en la segregación las redes inalámbricas, las redes internas y privadas, (Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes.)	No	0
7.4.6	11.4.6	**Control de conexión a la red**	Existe una política de control de acceso, que establezca el control de la conexión de	No	0

			la red, para redes compartidas, en especial para aquellas extendidas fuera de los límites de la organización. (En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio.)		
7.4.7	11.4.7	**Control de rutas de redes**	La política de control de acceso, establece que los controles de rutas deben ser implementados para las redes.	No	0
			El control de rutas está basado en mecanismos de identificación de destinatarios. (Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio.)	No	0
7.5	11.5	**Control de accesos a Sistemas Operativos**			
7.5.1	11.5.1	**Control de accesos a Sistemas Operativos**	El acceso al Sistema Operativo está controlado por un procedimiento seguro de Log-on. (Debería controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión.)	No	0
7.5.2	11.5.2	**Identificación y autenticación de usuario**	El identificado único (ID usuario) se proporciona a cada usuario tales como operadores, administradores de sistemas y	No	0

			otro personal que incluyen técnicos y mantenedores.		
			La técnica de la autenticación conveniente es elegida en base a la identidad del usuario.	No	0
			Se proporcionan cuentas genéricas, sólo en caso de circunstancias excepcionales donde hay un beneficio comercial claro. Se hacen necesario controles adicionales para mantener la responsabilidad. (Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.)	No	0
7.5.3	11.5.3	**Sistema de administración de contraseñas**	Existe un sistema de administración de contraseña que haga cumplir varios controles de contraseña, tales como: contraseña individual por responsabilidad, hacer cumplir los cambios de contraseñas, almacenar contraseñas de forma encriptada, no mostrar las contraseñas en la pantalla, etc. (Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas.)	No	0
7.5.4	11.5.4	**Uso de herramientas del sistema**	Los programas utilitarios son capaces de administrar el sistema y restringen con hermetismo su seguridad Por ejemplo, Herramientas para detectar los servicios habilitados mediante el chequeo del registro del sistema, los puertos locales abiertos y los servicios en ejecución. (**WINDOWS WORMS DOORS**	No	0

			CLEANER) (Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones.)		
7.5.5	11.5.5	**Time-out de sesiones**	Una sesión inactiva es cerrada después de un período definido de inactividad. (Se deberían desconectar las sesiones tras un determinado periodo de inactividad.)	Medianamente	33
7.5.6	11.5.6	**Limitaciones de tiempo de conexión**	Existe restricción en tiempo de conexión para aplicaciones de alto riesgo. Esto debería ser considerado para aplicaciones delicadas para los cual los terminales se instalan en locaciones de alto riesgo. Por ejemplo, si un usuario no autorizado ingresa fuera de horario con una cuenta plagiada, este no podrá hacer login en el pc, porque la cuenta plagiada esta deshabilitada fuera de horario. Si un colaborador requiere trabajar fuera de horario, la jefatura debe solicitar formalmente la ampliación del horario para esa cuenta. (Se deberían utilizar limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo.)	No	0
7.6	11.6	**Control de accesos a la aplicaciones e información**			
7.6.1	11.6.1	**Restricción del acceso a la información**	El acceso a la información y a las funciones del sistema de aplicación esta restringido para los usuarios y personal de apoyo, de acuerdo a la política de control	Si	100

			definida. (Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.)		
7.6.2	11.6.2	**Aislamiento de sistemas sensibles o críticos**	Los sistemas sensibles están provistos (aislados), en un medio ambiente especializado para informática, adecuado para el funcionamiento de un computador especializado, para compartir recursos sólo con sistema de aplicación confiable, etc. (Los sistemas sensibles deberían disponer de un entorno informático dedicado (propio).)	Medianamente	50
7.7	11.7	**Computación móvil o tele-trabajo**			
7.7.1	11.7.1	**Ordenadores portátiles y comunicaciones móviles.**	Hay una política formal, y están adoptadas las medidas de seguridad para protegerse de los riesgos del uso de la informática móvil. (Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.)	Medianamente	50
7.7.2	11.7.2	**Tele-trabajo**	La política, plan operacional y procedimientos están desarrollados e implementados para las actividades del teleworking.	No	0
			La política de Tele-trabajo está autorizada y controlada por la administración.	No	0

			(Se debería desarrollar e implantar una política, planes operacionales y procedimientos para las actividades de teletrabajo.)		

Área: Adquisición, desarrollo y mantenimiento de los sistemas de información					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
8.1	12.1	**Requerimientos de seguridad para los Sistemas de Información**			
8.1.1	12.1.1	**Especificación y análisis para de requerimientos de seguridad**	Los requisitos de seguridad para los nuevos sistemas de información y las mejoras a los sistemas de información existente, especifican los requisitos para los controles de seguridad.	No	0
			Los requisitos de seguridad y controles identificados, reflejan el valor comercial de recursos involucrados y las consecuencias de un fracaso en Seguridad.	No	0
			Los requisitos del sistema para la seguridad de información y procesos para implementación de la seguridad, están integrados en las fases preliminares de proyectos de sistemas de información. (Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad.)	No	0
8.2	12.2	**Procesamiento correcto de las aplicaciones**			
8.2.1	12.2.1	**Validación de los datos de entrada**	La entrada de datos, a sistema de aplicación, esta validada para asegurar que es correcto y apropiado.	Si	100
			Están considerados los controles tales como: diferentes tipos de entradas para chequear los mensajes de error, procedimientos para responder a la validación de errores, definición de responsabilidades de todo el personal	Si	100

			involucrado en el proceso de entrada de datos, etc.. (Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados.)		
8.2.2	12.2.2	**Control de procesamiento interno**	La validación de chequeos está incorporada en la aplicaciones, para detectar cualquier corrupción de información a través del procesamiento de errores o actos deliberados.	Si	100
			El diseño e implementación de las aplicaciones aseguran que los riesgos de procesar con errores, que conllevan a una pérdida de integridad, se disminuyen. (Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas.)	Si	100
8.2.3	12.2.3	**Integridad de los mensajes**	Los requisitos para asegurar y proteger la integridad del mensaje en las aplicaciones están identificados, y los controles apropiados identificados e implementados.	Si	100
			La evaluación de un riesgo de seguridad se lleva a cabo para determinar si la integridad del mensaje se requiere, e identificar el método más apropiado de implementación. (Se deberían identificar los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, e identificar e implantar	No	0

			los controles apropiados.)		
8.2.4	12.2.4	**Validación de datos de salida**	Los datos de salida son validados para asegurar que el proceso de almacenamiento de información emitida o generada, esté correcto (Se deberían validar los datos de salida de las aplicaciones para garantizar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.)	Si	100
8.3	12.3	**Controles criptográficos**			
8.3.1	12.3.1	**Políticas de uso de controles criptográficos**	La organización está usando una política de controles criptográficos para la protección de la información.	No	0
			La política está exitosamente implementada.	No	0
			La política criptográfica considera el acercamiento de la administración hacia el uso de controles criptográficos, el riesgo de valoración de resultados para identificar niveles requeridos de protección, métodos de administración claves y varias normas para una implementación efectiva. (Se debiera desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información)	No	0
8.3.2	12.3.2	**Administración de claves.**	Hay una administración llaves para apoyar a la organización en el uso de las técnicas criptográficas.	No	0
			Las claves criptográficas están protegidas de la modificación, pérdida y destrucción.	No	0
			Las llaves secretas y privadas están protegidas de la revelación no autorizada.	No	0
			Los equipos usados para generar,	No	0

			almacenar llaves están físicamente protegidos.		
			El sistema de administración de llaves está basado en un conjunto de normas, procedimientos y métodos seguros. (Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la Organización.)	No	0
8.4	12.4	**Seguridad de los archivos del sistema**			
8.4.1	12.4.1	**Control de software operacional**	Hay algunos procedimientos para controlar la instalación del software en los sistemas operativos. (Esto minimiza el riesgo de corrupción de los sistemas operativos). (Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos.)	No	0
8.4.2	12.4.2	**Protección de datos de prueba de sistemas**	El sistema de prueba está protegido y controlado.	Si	100
			El uso de información personal o cualquier información sensible, para probar, es rechazada. (Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.)	No	0
8.4.3	12.4.3	**Control de acceso al código fuente de los sistemas**	Existen controles estrictos para restringir el acceso a librería de programas fuentes. (Se debería restringir el acceso al código fuente de los programas.)	No	0
8.5	12.5	**Seguridad de los procesos de desarrollo y soporte**			
8.5.1	12.5.1	**Procedimientos de control de cambios**	Hay un procedimiento de estricto para la implementación de cambios del sistema de	No	0

			información. (Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.)		
			Este procedimiento se orienta a la reducción del riesgo y análisis de impactos de cambios.	No	0
8.5.2	12.5.2	**Revisión técnica de aplicaciones después de cambios al sistema operativo**	Hay un proceso para revisar y testear aplicaciones críticas del negocio, impidiendo el impacto adverso en las operaciones o seguridad organizacional después del cambio de Sistemas Operativos. (Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización)	No	0
8.5.3	12.5.3	**Restricción en los cambios de paquetes de software**	Si las modificaciones con paquetes de software se realizan necesariamente para funcionamiento y seguridad.	Medianamente	50
			Los cambios están controlados estrictamente. (Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.)	Medianamente	50
8.5.4	12.5.4	**Fuga de información**	Están los controles para prevenir la fuga de información	No	0
			Son considerados los controles, tales	No	0

			como, escanear los medios de respaldo, monitoreo regular del personal y actividades del sistema, permitidas bajo la legislación local (Se debería prevenir las posibilidades de fuga de información.)		
8.5.5	12.5.5	**Desarrollo de software externalizado**	El desarrollo de software externalizado está supervisado y monitoreado por la organización.	No	0
			Están considerados los puntos como: acuerdo de licencia, acuerdos de custodia, requisitos contractuales para el seguro de calidad, prueba antes de la instalación para detectar el código Trojan, etc. (Se debería supervisar y monitorizar el desarrollo del software subcontratado por la Organización.)	No	0
8.6	12.6	**Gestión de vulnerabilidades técnicas**			
8.6.1	12.6.1	**Control de vulnerabilidades técnicas**	La información oportuna acerca de las vulnerabilidades técnicas, de sistemas de información en uso, se están obteniendo.	No	0
			La exposición de la organización a tales evaluación de vulnerabilidades y medidas apropiadas tomadas, se hacen para mitigar el riesgo asociado. (Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados.)		

Área: Gestión de incidentes de seguridad de la información					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
9.1	13.1	**Reportando eventos y debilidades en la seguridad de la información**			
9.1.1	13.1.1	**Reportar eventos de seguridad de información**	Los eventos de seguridad de información son reportados a través de un canal de administración apropiado, tan rápido como sea posible	Medianamente	50
			El procedimiento formal de reporte de información de eventos de seguridad, la respuesta del incidente e intensificación del procedimiento está desarrollado e implementado. (Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados.)	No	0
9.1.2	13.1.2	**Reportar vulnerabilidades técnicas**	Existe un procedimiento que asegure a todos los usuarios de sistemas de información y servicios, sean requeridos para reportar cualquier observación o sospecha de debilidad de la seguridad en el sistema o servicios. (Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.)	No	0
9.2	13.2	**Gestión de incidentes y mejoras en la seguridad de la información**			
9.2.1	13.2.1	**Responsabilidades y procedimientos**	Las responsabilidades y procedimientos de administración fueron establecidos para	Medianamente	50

			asegurar una rápida, efectiva y ordenada respuesta a la información de los incidentes de seguridad.		
			Se monitorea los sistemas, las alerta y las vulnerabilidades son usadas para detectar incidentes de seguridad de información.	No	0
			El objetivo de la administración de la seguridad de información de incidentes esta en concordancia con los planes de la organización. (Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.)	Medianamente	50
9.2.2	13.2.2	**Aprendizaje de incidentes de seguridad de la información**	Hay un mecanismo para identificar y cuantificar el tipo, volumen y costos de incidentes se seguridad de información.	No	0
			La información obtenida de la última evaluación realizada sobre incidentes de seguridad de información, está siendo usada para identificar incidentes similares y/o de alto impacto. (Debería existir un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información.)	No	0
9.2.3	13.2.3	**Recolección de evidencias**	La acción de seguimiento a una persona u organización, después de un incidente de seguridad de información, involucra acción legal (civil o criminal).	No	0
			Las evidencias relativas al incidente son reunidas, retenidas y presentadas para conformar las evidencias a presentar de acuerdo a las reglas en la jurisdicción	No	0

			pertinente.		
			Los procedimientos internos son desarrollados y seguidos cuando se reúnen y presentan las evidencias, con el propósito de una tomar una acción disciplinaria dentro de la organización. (Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada conforme a las reglas para la evidencia establecidas en la jurisdicción relevante.)	No	0

Área: Gestión de la continuidad del negocio					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Área auditada, objetivo y pregunta**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
10.1	14.1	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**			
10.1.1	14.1.1	**Incluyendo la seguridad de la información en el proceso de continuidad del negocio**	Hay un proceso administrado que apunta a los requisitos de información de seguridad para el desarrollo y mantención de la continuidad del negocio dentro la organización.	Medianamente	20
			Este proceso entiende los riesgos que la organización enfrenta, identifica los recursos críticos del negocio, identifica los incidentes graves, considera la implementación de controles preventivos adicionales y la documentación de planes de continuidad del negocio, apuntando a los requisitos de la seguridad. (Se debería desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del negocio.)	Medianamente	20
10.1.2	14.1.2	**Continuidad del negocio y evaluación de riesgos.**	Los eventos que causan la interrupción, al proceso del negocio, son identificados con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de información. (Se deberían identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.)	Medianamente	20

			Los planes fueron desarrollados para mantener y restaurar operaciones comerciales, asegurar disponibilidad de información dentro del nivel requerido, en el marco de tiempo requerido, después de una interrupción o falla de procesos comerciales.	Medianamente	40
10.1.3	14.1.3	**Diseño e implementación de planes de continuidad del negocio**	Los planes consideran la identificación y responsabilidades, identificación de una perdida aceptable, implementación de recuperación y procedimiento de restauración, documentación de procedimiento y prueba regular. (Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requeridos, tras la interrupción o fallo de los procesos críticos de negocio.)	Medianamente	40
10.1.4	14.1.4	**Marco de trabajo para planificación de continuidad del negocio**	Hay solo una estructura de plan de continuidad del negocio.	No	0
			La estructura se mantiene para asegurar que todos los planes sean consistentes e identifiquen prioridades para pruebas y mantención.	No	0
			El plan de continuidad del negocio apunta a identificar al requisito de seguridad de información. (Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.)	No	0
10.1.5	14.1.5	**Prueba, mantenimiento y reevaluación de planes de**	Los planes de continuidad del negocio son probados regularmente para asegurar que	No	0

		continuidad del negocio	estén actualizados y efectivos.		
			Las pruebas del plan de continuidad del negocio aseguran que todos los miembros del equipo de recuperación y otros grupos relevantes, estén conscientes de los planes y de sus responsabilidades para la continuidad del negocio y seguridad de información, y sepan sus roles cuando el plan se sea evocado. (Se deberían probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia.)	No	0

Área: Cumplimiento					
Referencia		**Área auditada, objetivo y pregunta**		**Resultado**	
Lista	**Standard ISO/IEC 27001:2005**	**Sección**	**Pregunta de control**	**Se encuentra**	**Cumplimiento**
11.1	15.1	**Cumplimiento con requerimientos legales**			
11.1.1	15.1.1	**Identificación de la legislación aplicable**	Todos los requisitos relevantes estatutarios, regulatorios, contractuales y acercamiento organizacional para satisfacer los requisitos fueron explícitamente definidos y documentados para cada sistema de información y organización.	Si	100
			Los controles específicos y responsabilidades individuales, para suplir estos requisitos, fueron definidos y documentados. (Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Organización para cumplir con estos requisitos, deberían ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización.)	Si	100
11.1.2	15.1.2	**Derechos de propiedad intelectual**	Estos procedimientos aseguran el cumplimiento de requisitos legislativos, regulatorios y contractuales en el uso de material respecto de los cuales pueden ser de derechos de propiedad intelectual y sobre el uso de productos software patentados.	Si	100
			Los procedimientos están bien implementados.	Si	100
			Son considerados los controles como: publicación de la política de cumplimiento de derechos de propiedad intelectual,	Si	100

			procedimientos para la adquisición de software, conciencia de la política, mantención de pruebas de propiedad, cumplimiento con los términos y condiciones del software. (Se debieran implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado)		
11.1.3	15.1.3	**Protección de los registros de la organización**	Los registros importantes de la organización están protegidos de perdidas, destrucción y falsificación, de acuerdo con lo estatutario, regulatorio, contractual y requisitos comerciales.	Si	100
			Se considera la posibilidad de deterioración de medios usados para el almacenamiento de archivos.	No	0
			Los sistemas de almacenamiento fueron escogidos de tal manera que la información sea recuperada en una marco de tiempo apropiado y formato adecuado, dependiendo de los requisitos a cumplir. (Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio.)	No	0
11.1.4	15.1.4	**Protección de datos y privacidad de la información personal**	La protección y privacidad de la información está asegurada de acuerdo a la legislación pertinente, regulación y, si es aplicable, según las causas contractuales. (Se debería garantizar la protección y	Si	100

			privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales.)		
11.1.5	15.1.5	**Prevención del mal uso de instalaciones de procesamiento de información**	El uso de la información obtenida con propósitos no comerciales, ni autorizados, sin la aprobación administrativa, es tratado como uso impropio dentro de la organización	No	0
			Se presenta un mensaje de advertencia en la pantalla antes de Log-on. El usuario tiene que reconocer la advertencia y reaccionar apropiadamente al mensaje continuando con el proceso de log-on.	Si	100
			El consejo legal se considera antes de implementar cualquier procedimiento de monitoreo. (Se debería disuadir a los usuarios del uso de los recursos dedicados al tratamiento de la información para propósitos no autorizados.)	No	0
11.1.6	15.1.6	**Regulación de controles criptográficos**	Los controles criptográficos están usados cumpliendo todos los acuerdos, leyes y regulaciones. (Se deberían utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes.)	No	0
11.2	15.2	**Cumplimiento con políticas y estándares de seguridad y cumplimento técnico**			
11.2.1	15.2.1	**Conformidad con políticas y estándares de seguridad**	Los administradores aseguran que todos los procedimientos de seguridad, dentro de sus áreas de responsabilidad, sean llevados a cabo correctamente, para lograr el cumplimiento de las políticas de seguridad y normas.	Medianamente	50
			Los administradores revisan regularmente	No	0

			el cumplimiento del proceso de información, dentro de sus áreas de responsabilidad, para el cumplimiento de la política y procedimientos pertinente. (Los directivos se deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad.)		
11.2.2	15.2.2	**Verificación de conformidad técnica**	Los sistemas de información están regularmente chequeados para el cumplimiento de la implementación de seguridad y normas.	Si	100
			El chequeo de cumplimiento técnico es llevado a cabo bajo la supervisión de personal competente y autorizado (Se debería comprobar regularmente la conformidad de los sistemas de información con los estándares de implantación de la seguridad.)	Si	100
11.3	15.3	**Consideraciones de auditoría de sistemas de información**			
11.3.1	15.3.1	**Controles para auditoría de sistemas de información**	Los requisitos de auditoria y las actividades que involucran el chequeo de los sistemas de operacionales, deberían ser cuidadosamente planeados y acordados para minimizar el riesgo de alteración al proceso comercial.	Medianamente	50
			Los requisitos de auditoria y su alcance están dentro de la administración. (Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio.)	No	0
11.3.2	15.3.2	**Protección de herramientas de**	El acceso a las herramientas de auditoria	No	0

		auditoría de sistemas	del sistema de información, tales como software o archivos de datos, están protegidos para prevenir cualquier mal uso o peligro.		
			Las herramientas de auditoria del sistema de información están separadas del desarrollo y sistemas operacionales, al menos que se les dé un nivel apropiado de protección adicional. (Se deberían proteger los accesos a las herramientas de auditoría de los sistemas de información con objeto de prevenir cualquier posible mal uso o compromiso.)	No	0