UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM VALLE DE MÉXICO

PROPUESTA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE MESAS DE SERVICIO DE LA EMPRESA SONDA MÉXICO S.A DE C.V.

REPORTE DE APLICACIÓN DE CONOCIMIENTOS

Que para obtener el Título de

LICENCIADO EN INFORMATICA ADMINISTRATIVA

P r e s e n t a

C. Delfino Vázquez García

Asesor: M.T.I Mónica C. Fuentes González

Atizapán de Zaragoza, Edo. de Méx. Mayo 2017

Centro Universitario UAEM Valle de México

RESUMEN

La propuesta está basada en la seguridad de la información de la norma de ISO/IEC 27001:2013, se implementaran políticas y controles en la unidad de negocio del Services Desk de la empresa SONDA, se realizará un análisis de riesgo el cual nos ayudara a identificar los riesgos de seguridad, amenazas, vulnerabilidades, probabilidad e impacto, con la finalidad de resguardar, proteger y preservar la confidencialidad, integridad y disponibilidad de la seguridad de la información. Todo activo identificado como riesgo se clasificara por activo de apoyo como software, hardware, recursos humanos, información, sistemas y/o infraestructura.

Todos los riesgos identificados deben de tener un tratamiento, existen cuatro formas para el tratamiento, uno aceptar el riesgo, dos eludir o evitar el riesgo, tres trasferir el riesgo, cuatro mitigar el riesgo, el tratamiento es uno de los puntos más importantes para reducir un riesgo, se debe saber cómo clasificar el riesgo ya que dependiendo del resultado que tenemos podemos tratar el riesgo, para llevar a cabo el tratamiento se deberá de llenar un formato de control de riesgos.

Hoy en día están muy de moda los virus como Phishing y Ransomware. Los virus son las amenazas externas que puede acabar con los equipos que no tienen instalado o actualizado el antivirus, es importante tener protegida la información, es por ello que la seguridad de la información es muy importante para las empresas que se dedican a la tecnología de la información.

Cada dos meses deberá haber una reunión del comité de seguridad, donde se muestren los avances de los riesgos identificados, las métricas, hallazgos e informes, toda información que se ve en el comité de seguridad se debe presentar en la siguiente reunión, los encargados de cada unidad de negoción son responsables de monitorear y dar seguimiento a sus hallazgos y riesgos de seguridad.

SUMMARY

The proposal is based on the information security of the ISO / IEC 27001: 2013 standard, policies and controls will be implemented in the Business Unit of the Services Desk of the company SONDA, a risk analysis will be carried out which will help us Identify security risks, threats, vulnerabilities, probability and impact, in order to safeguard, protect and preserve the confidentiality, integrity and availability of information security. Any asset identified as risk would be classified by supporting asset such as software, hardware, human resources, information, systems and / or infrastructure.

All identified risks must have a treatment, there are four ways to treat, one to accept the risk, two to avoid or avoid risk, three to transfer risk, four to mitigate risk, treatment is one of the most important points to reduce A risk, you must know how to classify the risk since depending on the result that we can treat the risk, to carry out the treatment must be filled out a format of risk control.

Nowadays viruses like Phishing and Ransomware are very fashionable. Viruses are the external threats that can end with computers that do not have installed or updated the antivirus, it is important to have protected information, that is why information security is very important for companies engaged in the technology of information.

Every two months there should be a meeting of the security committee, showing the progress of identified risks, metrics, findings and reports, all information seen in the security committee should be presented at the next meeting, Each business unit is responsible for monitoring and tracking its findings and security risks.

Índice de Contenido.

Contenido

Índice de Figuras.

Índice de Tablas.

1. Planteamiento del problema

1.1 Antecedentes

SONDA es uno de los principales integradores y proveedores de servicios de Tecnologías de la Información (TI) en América Latina, tiene representación en 10 países y más de 1,000 ciudades bajo cobertura, con una organización de más de 10,000 profesionales y técnicos al servicio de sus clientes. Su misión es agregar valor a sus clientes, mediante el mejor uso de las tecnologías de información, a través de la provisión de servicios y soluciones de calidad que apoyen su gestión productiva y empresarial.

Proporcionan un amplio abanico de soluciones y servicios de TI que agregan valor a los negocios de sus clientes, diseñan e implementan soluciones que permiten cubrir integralmente las necesidades de TI de una organización.

Considerando las necesidades particulares, se enfocan hasta en los más mínimos detalles, pero siempre asegurando una visión integral que permita al cliente resolver su problema y/o atender sus necesidades de negocio según su propia estrategia y sin distraerse en los aspectos técnicos. Los proyectos que desarrollan pueden llegar a ser de gran complejidad o tamaño, requerir de vastos conocimientos y recursos, así como experiencia en múltiples geografías e industrias.

Entre las diferentes divisiones de la empresa que prestan servicios se pueden mencionar las siguientes, Service Desk, Field Services y Software Specialist Support. La problemática presentada en el reporte está relacionada con la división Service Desk.

Planteamiento del problema

En el Service Desk se propone aplicar la norma ISO/IEC 27001:2013 para proporcionar mayores niveles de seguridad de la información, asegurando la Confidencialidad, Integridad y Disponibilidad, de esta forma se validará el cumplimiento de controles operativos tales como:

- Política de acceso de internet para todos los usuarios.
- Bloqueo de todas las entradas de dispositivos para evitar cualquier tipo de dispositivo que inserten a sus computadoras y provocar con ello que la información manejada pueda ser alterada o hacer mal uso de ella.
- Para que se le pueda permitir a una persona ingresar al área de Mesas de Servicio se le pedirá como requisito que porte el gafete.
- Controles de cumplimiento de la política de escritorio limpio y bloqueo de pantalla.
- Control de acceso físico, donde además de solicitar una identificación oficial a personas ajenas a la empresa, se revisarán mochilas y número de serie de equipos de cómputo que entran y salen en el corporativo.

Con esta propuesta se pretende hacer una comparación dentro de la Unidad de Negocio, principalmente en Mesas de Servicio y verificar si se está cumpliendo con estos lineamientos.

Muchas de las solicitudes que se realizan en el ámbito laboral son repetitivas, es decir, pueden suceder muchas veces, por lo que se recomienda tener una bitácora o seguimiento de las incidencias. Por otro lado, parte del personal que labora en la empresa, debe conocer las políticas y parámetros, para mantener la seguridad de la información, todos los equipos de cómputo se tienen que controlar, porque son la principal herramienta para desarrollar su trabajo.

1.2 Descripción

La Mesa de Servicio (Service Desk) opera como punto único de contacto (al que se puede acceder por distintos canales: telefónicamente, e-mail, chat y acceso web) que resuelve en forma oportuna los requerimientos que puedan tener los distintos tipos de usuarios de la empresa ante incidentes, consultas y peticiones de servicios de TI. Esto permite mejorar continuidad operativa y tener una mayor visibilidad de las TI de la empresa.

Las mesas de servicio, actúan como punto de contacto para canalizar todas las solicitudes de servicios de los clientes, así como desde que se levanta un ticket, se registran los datos del cliente en una herramienta de gestión que utiliza la empresa (Remedy y Moebius), se da el seguimiento del estatus que se encuentra, se realiza una escalación de cada uno de los tickets registrados.

El servicio está disponible hacia los clientes con base en lo escrito ya sea en contrato o propuesta del servicio, así también satisfaciendo las necesidades del usuario. Este servicio está disponible 24x7 y los 365 días del año.

La unidad de negocio se define como mesas de servicio y se divide en tres: Mesa de Servicio “**MS**”; **MS Nivel Dispatch, MS Primer Nivel y MS Servicios Especializados**: en este servicio el ingeniero solo se encarga de recibir la llamada, correo, chat y web, debe documentar el ticket de lo que está solicitando el usuario, el agente tiene la responsabilidad de brindarle el ticket al grupo correspondiente que está a cargo de esa área, el ingeniero tiene que mencionarle el número de ticket ejemplo: “DVG_901037”, el agente está monitoreando el ticket en qué estatus está, se deja de monitorear el ticket hasta que esté solucionado, al final se genera el reporte del cierre o la solución que se le dio al usuario.

Mesa de Servicio: **Nivel Dispatch**

Punto único de contacto para gestionar un alto volumen de llamadas y redirigir a los usuarios, a otras instancias de soporte y/o comerciales, excepto en los casos más sencillos.

Funciones:

- Administrar la herramienta de Gestión de tickets, si así lo define el contrato.
- Administrar al personal que ejecutará las siguientes tareas:
    - Tomar llamada, correo o ticket web.
    - Documentar ticket.
    - Asignar ticket a grupo de soporte correspondiente.
    - Informar al usuario el número de ticket.
    - Realizar seguimiento de atención de reporte.
    - Generar reportes acordados con clientes.

Mesa de Servicio: **Primer Nivel**

Punto único de contacto para ofrecer una primera línea de soporte técnico que permita resolver en el menor tiempo las interrupciones del servicio o requerimientos.

Funciones:

- Administrar la herramienta de Gestión de tickets, si así lo define el contrato.
- Administrar al personal que ejecutará las siguientes tareas:
    - Tomar llamada, correo o ticket web.
    - Documentar ticket.
    - Resolver fallas o requerimientos dentro de su alcance.
    - Asignar ticket a grupo de soporte correspondiente en los casos donde no pueda realizar la solución.
    - Informar al usuario el número de ticket para su servicio.

- Realizar seguimiento de atención de reporte.
- Generar reportes acordados con clientes.

Mesa de servicio: **Servicio Especializado**

Punto de contacto para ofrecer un primera línea de soporte técnico que permite resolver en el menor tiempo las interrupciones del servicio o requerimientos así como los tickets referentes a tecnologías especializadas, algunas actividades del servicio especializado son: por ejemplo SAP, plataforma Microsoft, VMwar.

- Soporte Especializado.
- Administrar la herramienta de Gestión de tickets, si así lo define el contrato.
- Administrar al personal que ejecutará las siguientes tareas:
  - Tomar llamada, correo o ticket web.
  - Documentar ticket.
  - Resolver fallas o requerimientos dentro de su alcance.
  - Asignar ticket a grupo de soporte correspondiente en los casos donde no pueda realizar la solución.
  - Informar al usuario número de ticket.
  - Realizar seguimiento de atención de reporte.
  - Generar reportes acordados con clientes.

Actualmente la empresa SONDA cuenta con políticas, procesos, procedimientos e instructivos de seguridad de la información, (es recomendable realizar la implementación de un Sistema de Gestión de Seguridad de la Información dentro de esta área para garantizar el cumplimiento y seguimiento de dichos controles operativos), garantizando que su información es confiable y está debidamente protegida de acceso no autorizado, asegurar la consulta de información que requiere el cliente cuando lo solicite, atender fallas de operación de servicio de cómputo,

como por ejemplo bloqueo de contraseñas, instalación de software, solicitar refacciones para equipo de cómputo, asignación de claves de acceso para personal de nuevo ingreso, atención de incidentes de seguridad como por ejemplo SPAM, Contaminación por virus, Phishing.

Debido a lo anterior del planteamiento del problema, surge la necesidad de desarrollar una propuesta de gestión de seguridad de la información de Mesas de Servicio que proporcione las medidas preventivas y correctivas de sus activos de información.

Un activo de información es aquél que tiene valor dentro de una organización y como tal debe ser adecuadamente protegido; la seguridad de la información está conformada por tres principios básicos los cuales son: confidencialidad, integridad y disponibilidad, que protegen el recurso de la información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño, maximizar las oportunidades de mejora para la unidad de negocio y el crecimiento de la empresa.

1.3 Delimitación

Se pretende que la propuesta sea aplicada en las Unidades de Negocio (UUNN) de las Mesas de Servicio de la empresa en un plazo no máximo a 6 meses, con la finalidad de mantener la confidencialidad e integridad de la información que maneja la empresa. Para la propuesta, el reporte se basará en algunas normas internacionales de seguridad como son:

ISO: es Organización de Estándares Internacionales, es una federación de alcance mundial integrada por cuerpos de estandarización internacionales.

ISO/IEC 27001:2013 es una norma internacional emitida por la International Organization for Standardization (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

ISO27002 La ISO/IEC 27002:2013 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

ISO 31000:2009 Esta norma internacional está destinada a satisfacer las necesidades de una amplia gama, para realizar las evaluaciones, la eficacia y tratamientos de los riesgos empresariales.
http://www.iso.org/iso/catalogue_detail?csnumber=43170

ITIL: Information Technology Infrastructure Library, (Biblioteca de Infraestructura de Tecnologías de Información) es un modelo de operación para el manejo de servicios de tecnologías de TI, ha ido evolucionando con la adición de las mejores prácticas de la industria de servicios de tecnologías tanto públicas y privadas, es una referencia de cómo sería mejor la administración de infraestructura de servicios de tecnología de información.

1.4 Beneficios

A corto plazo, al aplicar la propuesta de este reporte, se podrá implementar la norma ISO/IEC 27001:2013, lo cual permitirá brindar a los clientes un mejor nivel de servicio, la información estará clasificada y protegida. Todo el personal involucrado con el manejo de la información deberá cumplir con las políticas y normas de gestión de seguridad de la información de la empresa. A largo plazo, se pretende que la Unidad de Negocio esté certificada bajo la norma ISO/IEC 27001:2013.

2 Objetivos

2.1 General

Definir las principales actividades que se deben realizar para gestionar la seguridad de la información en la entrega de los servicios de TI, estas actividades se deben cumplir como lo indican las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

2.2 Específicos

- **Comunicar** las políticas de seguridad de la información a todos los proveedores, clientes y empleados.
- **Definir** el enfoque del sistema de gestión de seguridad de la información y los criterios para asumir los riesgos.
- **Implementar** controles de seguridad.
- **Reducir** los riesgos que están afectando la unidad de negocio de las mesas de servicio.

3 Justificación

La información que se maneja en la división Mesas de Servicio es de vital importancia para la empresa y para sus clientes, por eso es necesario contar con medidas y controles de seguridad que la protejan y también a los activos que la transmiten y almacenan, con la finalidad de proteger su confidencialidad, Integridad y Disponibilidad, así mismo, se busca cumplir con la legislación de protección de datos personales y compromisos contractuales que establecen requerimientos en materia de seguridad de la información.

Por lo anterior se busca con esta propuesta de proyecto implementar buenas prácticas de la industria, en este caso la norma ISO/IEC 27001:2013 “Sistema de Gestión de Seguridad de la Información”.
Con esto también se obtendrá ventaja competitiva en el mercado al obtener la certificación bajo esta norma.

Siendo egresado de la carrera de Informática Administrativa y estando certificado en ITIL, cuento con una cultura empresarial adquirida en base a experiencia de trabajo, la adquisición, desarrollo de competencias y habilidades específicas.

4 Marco teórico

Estado del Arte.

Los sistemas de información han crecido a pasos agigantados y la vulnerabilidad de la información que se maneja en ellos también, motivo por el cual la Seguridad de la Información se ha considerado una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer confidencialidad, integridad y disponibilidad, buen uso de la información que reside en un sistema de información (Andres, 2015).

Debido a lo anterior ha surgido una Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) que es una colección de documentos públicos, que basados en procesos y en un marco de buenas prácticas de la industria, permite la Gestión de Servicios de TI con calidad. (Tim Malone (Author), 2009).

Por otra parte, la norma ISO/EIC 27001:2013, es una norma internacional emitida por la International Organization for Standardization (ISO) y describe cómo gestionar la seguridad de la información en una empresa. El Sistema de Gestión de Seguridad de la Información (SGSI) nos puede guiar en mejorar procesos de mesas de servicio, como crear una política de clasificación de datos, capacitación a los agentes, tener reunión con el área de TI para tener un plan de actualización de las herramientas, habilitar los puertos de las máquinas de los agentes si así lo requiere el cliente, no enviar correos personales, pruebas de disponibilidad para verificar que estén al 100% las herramientas de gestión, las normas son también guías para definir una política de cualquier riesgo, amenaza o incidente mayor, (Ejemplo de un riesgo puede ser la caída de un servicio, como la herramienta de gestión de Moebius que es una base de datos de todos los ticket registrados, esto puede afectar la operación), una política son reglamentos de qué es lo que se puede y que no se debería de hacer. (final draft ISO/IEC FDIS 27001:2005, Voting begins on: 2005).

La norma ISO/IEC 27001:2013 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2013 por International Organization for Standardization y por la comisión International Electrotechnical Commission. (Kenneth, 1997).

El Diagrama de Edwards Deming es un modelo que se encarga de la ejecución de una mejora continua en la empresa, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). Fue Inventado por Walter Andrew Shewhart y popularizado por William Edwards Deming, conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), como se muestra en la Figura 1, (ISO 27001: Ciclo de Deming, 2015).

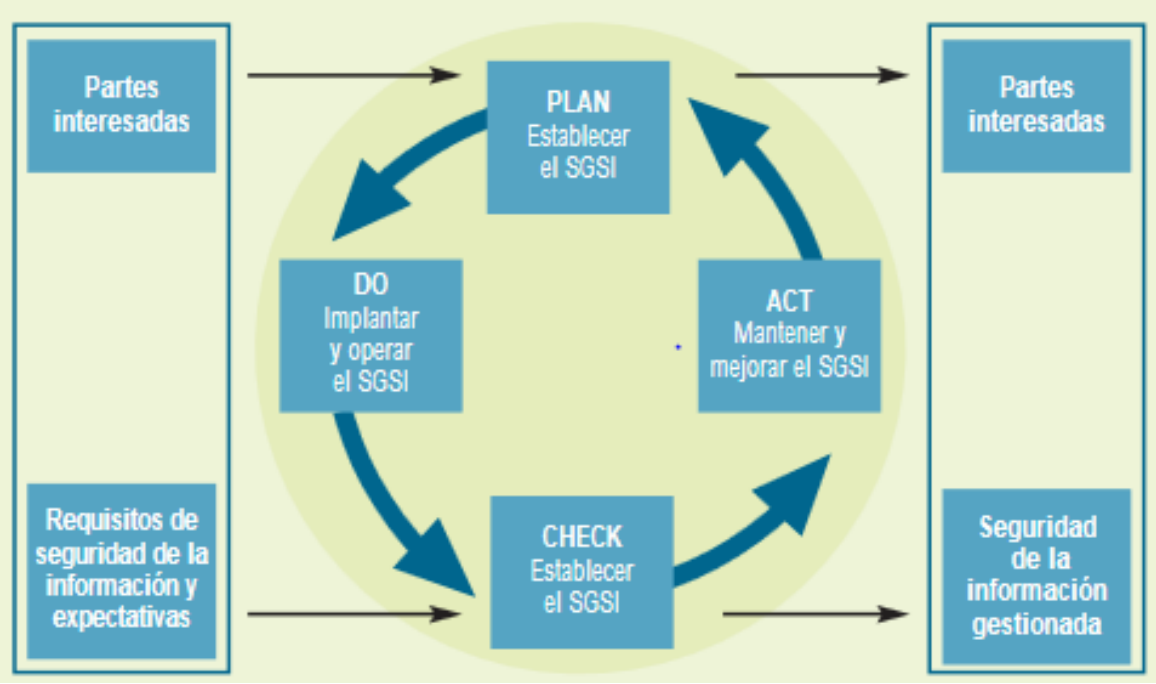


Figura 1 Ciclo de Deming

FUENTE: http://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

5 Fundamentación teórica

El uso de tecnologías de la información y comunicaciones (TIC) supone beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

El conocimiento de los riesgos otorga la confianza en que los sistemas desempeñarán su función correctamente. La confianza es la esperanza que se tiene que algo responderá a lo imprevisto, así se puede pensar que los sistemas de información ayudarán a cumplir los objetivos y se puede dejar a un lado la inquietud por la inseguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo se encuentra protegido el sistema.

5.1 Seguridad

Cuando se utiliza esta palabra en una locución adjetival ('de seguridad') significa que un dispositivo o mecanismo está diseñado para evitar riesgos o garantizar el buen funcionamiento, resguardar toda información y proteger cualquier activo de la mesa de servicio. Por ejemplo: 'Control de acceso lógicos'.
(http://www.significados.com/seguridad/)

5.2 Información

Información es un activo que pertenece a la organización, existen varios tipos de información dentro de la unidad de negocio de las mesas de servicio, la información es lo más importante, la información se encuentra clasificada en:

- Archivos de administración en papel.
- Archivos de administración en medios electrónicos.
- En pantallas de computadoras.
- Audiovisual.

5.3 Seguridad de la información

Es el conjunto de medidas preventivas y correctivas de un activo, la seguridad de la información está conformada por tres pilares que son: confidencialidad, integridad y disponibilidad, que protegen el recurso de la información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio como se muestra en la Figura 2, minimizar el daño y maximizar las oportunidades de mejora para la unidad de negocio y el crecimiento de la empresa. (Jule Hintzbergen,Kees Hintzbergen,André Smulders,Hans Baars, Mayo 2010)

Figura 2 Pilares de la seguridad de la información
Fuente: Autoría propia

5.3.1 Confidencialidad

Intenta impedir la divulgación intencional o no intencional del contenido de un mensaje. La pérdida de la confidencialidad puede ocurrir de muchas maneras, tales como a través de la liberación intencional de información privada o de empresa a través de una aplicación incorrecta de los derechos de la red, (Jule Hintzbergen,Kees Hintzbergen,André Smulders,Hans Baars, Mayo 2010), a todo el personal se le debe hacer conciencia de que no pueden divulgar la información entre compañeros o amigos externos que no laboren dentro de la empresa, todo el personal tiene que firmar una política de confidencialidad en donde se compromete a no divulgar la información, no vender bases de datos, no proporcionar direcciones de los clientes, no robar información, no acceder al sistema sin autorización, para toda aquella persona que viole los parámetros de la empresa se tendrá que levantar un acta administrativa dependiendo el tipo de incidente si es menor o mayor.

El tipo de incidente se comprobará monitoreándolo, verificando las cámaras de video de seguridad, en el momento en que se tengan las pruebas de la falta de información se decidirá si el empleado permanecerá dentro de la empresa o se dará de baja.

El personal debe de contar con un acceso restringido, solo se dará acceso únicamente a aquellas personas que cuenten con la debida autorización para manipular la información.

5.3.2 Integridad

La integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados , (Jule Hintzbergen,Kees Hintzbergen,André Smulders,Hans Baars, Mayo 2010), la integridad es uno de los pilares o principios básicos para la seguridad de la información que protegen los datos o procesos de la unidad de negocio, al día de hoy nos enfrentamos con personas que tienen más habilidad o experiencia para poder violar las políticas de seguridad, por lo cual se tienen que implementar controles de seguridad dependiendo de la amenaza y vulnerabilidad que afecte a los activos de la unidad de negocio.

La integridad se puede definir como la imposibilidad de que alguien modifique datos sin ser autorizado, todo el personal tendrá un usuario y password para que pueda acceder a las instalaciones, salas de computo, sistemas de red, este password se le asignará dependiendo el perfil o rol que tenga para poder realizar sus funciones. Algunos ataques que pueden afectar la integridad son: recuperación de datos, realizar copias de datos, borrados o eliminados, modificados y destrucción de datos.

5.3.3 Disponibilidad

Disponibilidad asegura el acceso confiable y oportuno a los datos o recursos de computación por parte del personal apropiado. En otras palabras, la disponibilidad garantiza que los sistemas estén en funcionamiento cuando sea necesario, (Jule Hintzbergen,Kees Hintzbergen,André Smulders,Hans Baars, Mayo 2010). La disponibilidad es el acceso a la información y a los sistemas por personas que están autorizadas o que tengan los accesos para poder visualizar la información en el momento que se requiera.

La disponibilidad es muy importante para la empresa, los empleados firman un contrato donde el servicio debe estar disponible los 365 días del año, en caso de que un cliente requiera visualizar información, levantar un incidente, solicite asesoría o un requerimiento, el ingeniero debe estar al pendiente en caso de que soliciten apoyo, ya que si no se cumplen con esas métricas se penalizará a la empresa por no cumplir como lo mencionó en el contrato. Además, en las carpetas de red o en la nube se están monitoreando las actividades por si algún cliente solicita información y no puede acceder a ella, en esos casos, debe haber una persona que apoye al cliente para poder entrar al sistema en caso de que lo requiera el usuario.

6 Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI es la abreviatura que se utiliza para referirse a un Sistema de Gestión de Seguridad de la información (SGSI), ISMS es el mismo concepto de SGSI pero en el idioma inglés Information Security Management System (ISMS). (http://www.iso27000.es/download/doc_sgsi_all.pdf).

Es un sistema que garantiza la coherencia de la seguridad de la información en la organización. En contexto es un conjunto de información y datos de la organización, son todos los datos que tienen valor para la empresa como: personas, los procesos, tecnologías, información en papel, correo electrónico, datos en la nube, manuales, instructivos, repositorio (carpetas en la red), fax, esta información aplica para personal interno, externo y clientes.

El SGSI garantiza la Seguridad de la Información mediante una estructura de buenas prácticas, definidas como:

- Gestión de Riesgos.
- Políticas.
- Procesos.
- Controles.

- Revisiones.
- Mejoras.

6.1 Amenazas

Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento que pueda afectar la operación, causando grandes daños para la unidad de negocio, la amenaza puede afectar los recursos, sistemas o aplicaciones, información, hardware, comunicaciones o infraestructura. (http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html). Un ejemplo de una amenaza, es que las maquinas tengan virus y la vulnerabilidad es que no tengan antivirus instalados, el riesgo es que se pierda información la cual es un activo valioso de la empresa.

Es necesario identificar la mayor cantidad de amenazas que puede sufrir la información para disponer de las alternativas de solución y prevención de las mismas con el objetivo de preservar la seguridad, integridad y disponibilidad de la información de la empresa. Se considera que el activo más importante de cualquier empresa es la información ya que ésta proporcionará las bases para la toma de decisiones, de ahí la importancia de su seguridad. Además si ésta se llega a perder o la roban, puede servir como arma para que otras empresas compitan suciamente en el mercado.

6.2 Tipos de Amenazas para la Seguridad de la Información

Algunas de las amenazas que puede afectar la información de la empresa como se muestran en la Figura 3:

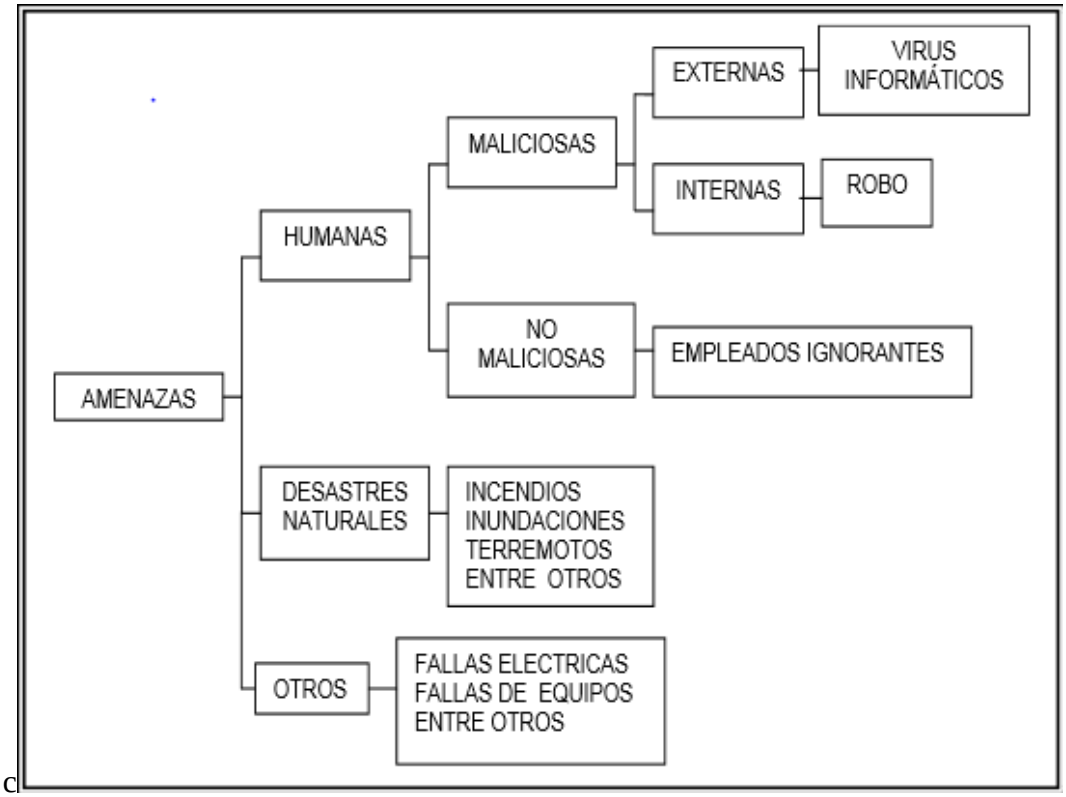


Figura 3 Tipos de Amenazas
Fuente: http://core.ac.uk/download/pdf/12401004.pdf

6.3 Vulnerabilidad

La vulnerabilidad es una debilidad de un sistema, recursos, información, todo tipo de activo, que puede ser explotada por una o varias amenazas. (http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#01). Algunos ejemplos podrían ser que los equipos sean obsoletos, a la planta de luz no se le da mantenimiento. Lo anterior puede provocar riesgos, pérdida de dinero, de información e interrupción en el servicio a los clientes.

6.4 Impacto negativo

Es la consecuencia de que una amenaza explote una vulnerabilidad, debido a la falta o falla de seguridad, esto provoca que no se esté cumpliendo con la Confidencialidad, la Integridad, y Disponibilidad de los datos, lo cual afecta al cliente porque no se está respetando con lo que se le prometió y el cliente tiene una mala apreciación de la calidad en el servicio que la empresa presta.

6.5 Probabilidad

Es la posibilidad de que un evento ocurra o no, entre mayor sea el evento hay más probabilidad de que corra en riesgo la operación, es decir que si hay una falla se tiene que resolver en ese momento para evitar una debilidad para la empresa.

7 Análisis de Riesgo de Seguridad

Es una aproximación metódica para determinar el riesgo. Existen diferentes metodologías que se pueden aplicar para poder determinar cuáles son los riesgos que se van a tratar. La metodología que se va utilizar para el análisis de riesgos tecnológicos es MAGERIT, existen muchas metodologías de riesgos, como EBIOS, FRAP, CRAMM, OCTAVE, ISO27005, AS/NZS 4360, asimismo existe una metodología para riesgos empresariales, la cual se le conoce como ISO/31000:2009.

8 Metodología MAGERIT

Historia

En la actualidad se encuentra en la versión 3.0, pero el tiempo ha pasado desde la primera publicación de Magerit en 1997, y su segunda publicación en 2005, donde el análisis de riesgos se ha venido consolidando como eje central para la gestión de la seguridad.

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

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.
Implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de la tecnología de la información. (Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas, 2012)

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

La metodología Magerit persigue los siguientes objetivos:

a. Directos:
   I. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

II. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
III. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

b. Indirectos:

I. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Magerit se basa en cuatro actividades principales que dependen unas de otras.

1- Método de análisis de riesgos.
2- Proceso de gestión de riesgos.
3- Proyecto de análisis de riesgos.
4- Plan de seguridad.

Magerit se enfoca en estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. Propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados que permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Para obtener la información se tiene que realizar un cuadro de matriz de riesgos, se requiere de la participación de diferentes áreas de responsabilidad dentro de la empresa, para poder obtener una lluvia de ideas y poder identificar más fácil la amenaza, vulnerabilidad, impacto, probabilidad en un corto tiempo.
(Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas, 2012).

8.1 Riesgos de Seguridad de la Información

La información, en sus más variadas formas, es uno de los activos más valiosos y estratégicos de cualquier empresa, de ahí la importancia de mantener la información segura. Un riesgo de seguridad es la probabilidad de que una amenaza explote una vulnerabilidad para un activo o activos, esto hace que cause un gran impacto para la operación con una gran pérdida de recursos, (ISO copyright office, 2009).

La seguridad de la información, como se mencionó anteriormente está basada en pilares básicos: confidencialidad, integridad y disponibilidad.

9 ISO

ISO significa Organización Internacional de Estándares, es una federación de alcance mundial integrada por cuerpos de estandarización nacionales más de 160 países, uno en cada país, la ISO es una organización no gubernamental establecida en 1947, ISO proviene de la palabra griego “isos” que significa “igual”, el cual es la raíz del prefijo “ISO”.

El principal objetivo de la norma es incrementar la satisfacción del cliente, mediante procesos de mejora continua. Está pensada para que las organizaciones que la apliquen, puedan garantizar su capacidad de ofrecer productos y servicios, que cumplen con las exigencias de sus clientes, gracias a una certificación internacional que les brinde prestigio y garantías de calidad, algunas de las mejoras que se realizó en la mesa de servicio fue en los KPI´s, se agregaron las gráficas de los porcentajes de KPI´s

10 Propuesta de Gestión de Seguridad de la Información de Mesas de Servicio de la Empresa Sonda México S.A de C.V.

Es establecer un proceso de gestión de riesgos basado en la norma de 27001, de acuerdo al siguiente diagrama de flujo como lo muestra en la tabla 1.

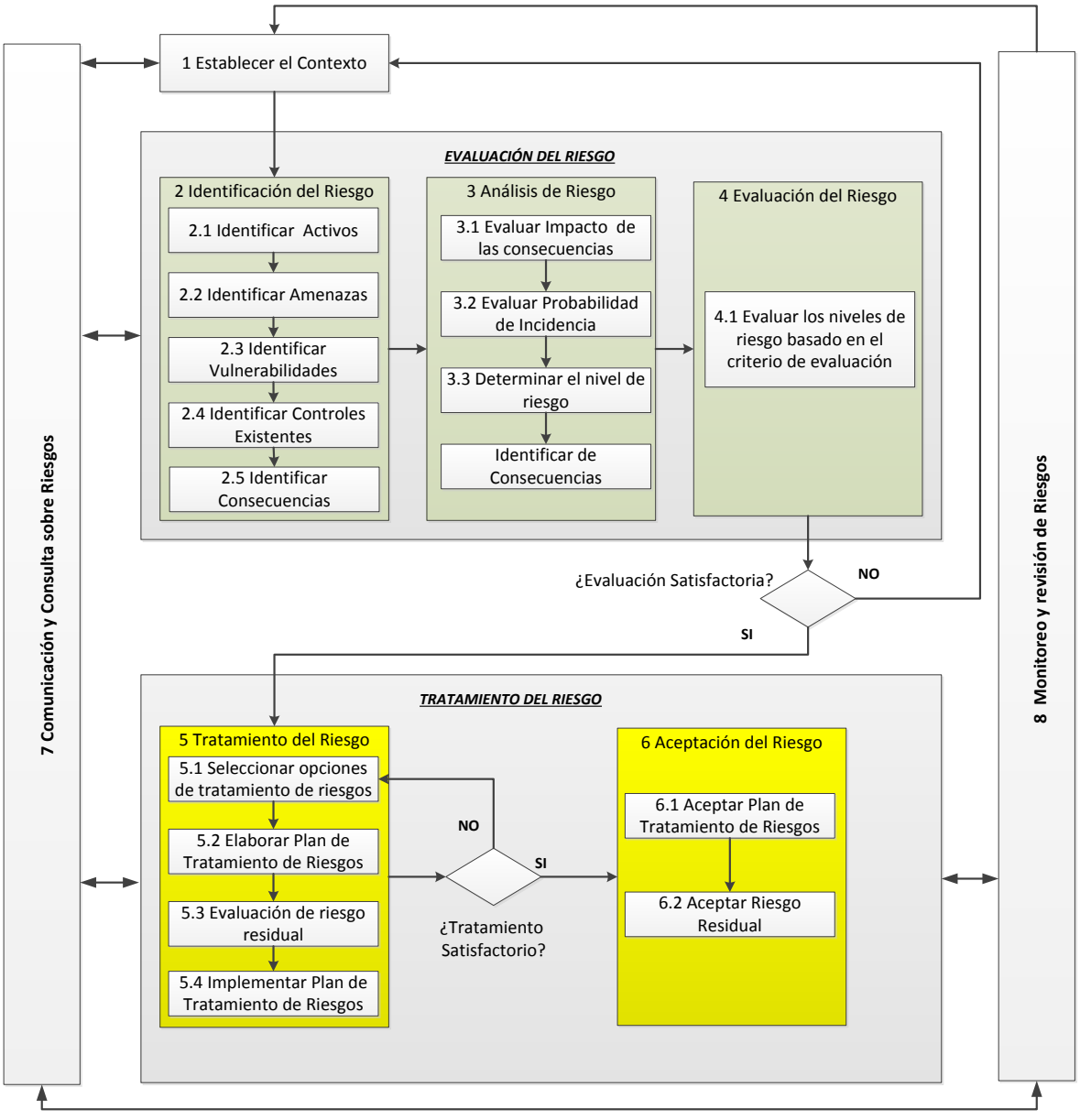


Tabla 1 Procedimiento de Gestión de Riesgos

Fuente: Autoría propia/CISO

Para llevar a cabo la propuesta se tiene que aplicar los siguientes pasos como:

1. **Establecer Contexto**
2. **Identificación del riesgo**
3. **Análisis de riesgo**
4. **Evaluación del riesgo**
5. **Tratamiento del riesgo**
6. **Aceptación del riesgo**
7. **Comunicación y consulta sobre riesgos.**
8. **Monitoreo y revisión de los riesgos.**

La propuesta de gestión de riesgo está relacionado con el plan de trabajo, este se tuvo que elaborar para tener un control y orden de las actividades que se tiene que realizar día a día, contiene los ocho pasos del diagrama más concientización, Auditorias, Mejora continua, Informes; como se muestra en la tabla 2.

PLAN DE TRABAJO.

Nos permite administrar los tiempos, aprovechar los tiempos muertos, así mismo alcanzar la meta que se requiere, para poder entregar las actividades en tiempo y formar, ser más eficientes y eficaz.

CRONOGRAMA DE ACTIVIDADES

ISO/IEC 27001:2013				Años	2016								2017			
ISO/IEC 31000	No.	Pasos de procedimiento de gestion	Periodos	Meses	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril
	1	Establecer Contexto														
Evaluacion de riesgo	2	Identificación del riesgo														
	3	Análisis de riesgo	Cada año													
	4	Evaluación del riesgo														
Tratamiento del riesgo	5	Tratamiento del riesgo														
	6	Aceptación del riesgo														
	7	Comunicación y consulta sobre riesgos	Cada vez que hay un riesgo													
	8	Monitoreo y revisión de los riesgos	Cada mes													
		Concientización de seguridad de la información	cada vez que hay un nuevo ingreso													
		Auditorias Internas o/e Externas	Tres veces al año		Externa 20001				Interno 27001		Interno 20001					
		Mejora Continua	Cada año													
		Informe de Seguridad de la Información	Cada mes													

Fecha estimada de entrega de evidencia:

Tabla 2 Cronograma de actividades

Fuente: Autoría propia

10.1 Establecer Contexto

Establecer un sistema de gestión de riesgos en el Service Desk para reducir el mínimo de vulnerabilidad, lo que se pretende es mejorar la seguridad.

- Activos de información relevantes.
- Estrategia, objetivos y políticas aplicables.
- Los procesos de negocio involucrados.
- Funciones y estructura operativa (esto ayuda a definir el personal que participara en la evaluación del riesgo).
- Requisitos legales, regulatorios y contractuales aplicables.
- La política de seguridad de la información de la organización.
- El enfoque general de la organización para la gestión de riesgos.
- Ubicaciones y características geográficas.
- Restricciones que afectan a la organización.
- Expectativas de las partes interesadas.
- Entorno socio-cultural.
- Los criterios básicos para el enfoque de gestión, la evaluación, el impacto y la aceptación del riesgo, están definidos en cada una de las actividades correspondientes dentro de este procedimiento.

Roles, Funciones y estructura operativa (esto ayuda a definir el personal que participara en la evaluación del riesgo).

En los siguientes párrafos identificamos cuáles son sus funciones y roles de cada encargado o responsable de los procesos.

Roles: un grupo de responsabilidades, actividades, que son asignadas a un proceso y esto puede ser asignado a una persona o equipo.

Una persona o equipo pueden tener varios roles por ejemplo, gestión de seguridad de la información, gestión de incidentes, gestión de coordinador de diseño.

Los roles también se pueden ver como puestos, que son papeles específicos a una función, como lo muestra la figura 4.

- Gerentes.
- Coordinadores.
- Analistas.
- Agentes.

Figura 4 Rol

Fuente: http://www.churchleaders.com/wp-content/uploads/files/article_images/1_23_Sr._Pastors_Roles_Change_as_Church_Grows_715561077.jpg

Funciones: es un equipo o grupo de personas que realizan uno o varios procesos y actividades, las funciones crean su propio cuerpo de conocimientos a través de la experiencia que va adquiriendo, como lo muestra la figura 5.

La función también se puede ver como un área específica dentro de una organización de TI.

- **Mesas de Servicio**, Opera como punto único de contacto (al que se puede acceder por distintos canales: telefónicamente, e-mail, chat y acceso web).
- **NOC** "Network Operation Center", se encarga de monitorear las redes en tiempo real, ejemplos, VOZ, DATOS, VIDEO.
- **SOC** "Security Operation Center", se encarga de monitorear la seguridad física. Es un área que se encarga de proteger de cualquier amenaza y vulnerabilidad, con un horario de 24 x 7 de monitoreo, algunos ejemplos: monitoreo de "Antivirus".

Figura 5 Función

Fuente: https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTSQpiLSqi5c4M0WrHHXL6-oTaDsMuMsGM_IM-pkNqUsUZ3NIOv

Estructura Organizacional

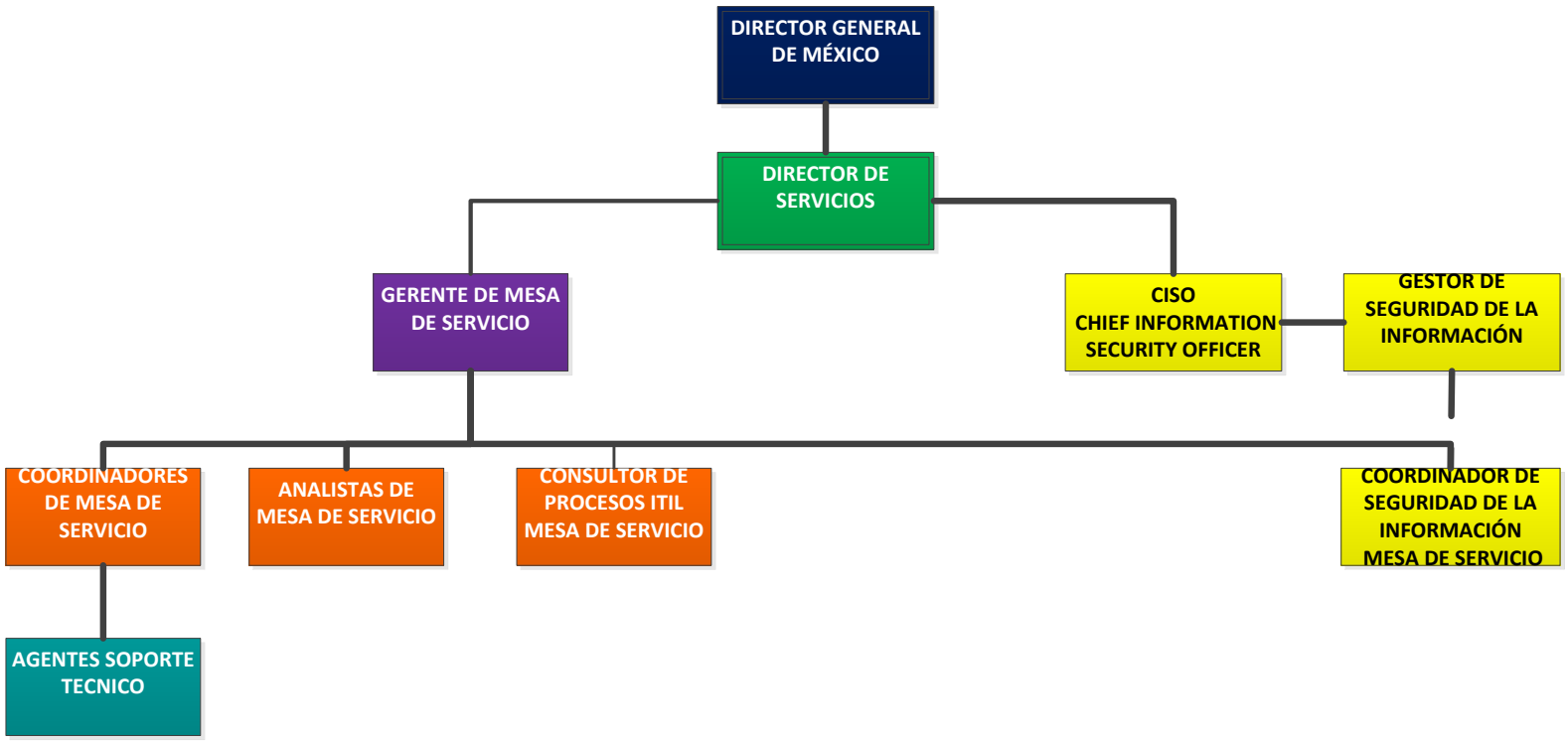


Tabla 3 Organigrama General Empresa Sonda

Fuente: Autoría propia

Estructura Organizacional.

Menciono de cómo está conformado el organigrama de la empresa, se define lo siguiente (perfiles, roles y funciones), que tiene cada colaborador desde el Director General hasta el Agente.

Descripción de actividades.

La estructura organizacional de la empresa se puede observar en el organigrama anterior, tabla 3. Enseguida se explicarán las funciones de algunos puestos.

Director general de México.

Es el que tiene a su cargo la representación total de la empresa u organización. Revisa los temas comerciales por cada apertura de negocio, visita a los clientes, tiene actividades externas “corporativo de Chile”, revisa la operación, Recursos Humanos, servicios, Presupuestos, Ventas, Toda la Administración de Sucursales y Corporativo de México.

Director de Servicios.

Es el que tiene a su cargo todas la áreas de servicio, con los gerentes de diferentes áreas de unidad de negocio, es el responsable de autorizar los presupuestos para cada UUNN de cuánto es lo que se tiene que gastar al año, el sueldo de la gente, desde agentes hasta gerentes, tiene mucho contacto con los clientes para el cumplimiento de los lineamientos del contrato, está enterado de las sucursales y corporativo de México de lo que está pasando, tiene reuniones con los clientes, también es responsable de autorizar y comunicar las políticas, toma decisiones de los controles de seguridad de la información, si se mitiga o acepta el riesgo.

Gerente de Mesa de Servicio.

Es la persona que se encarga de revisar las herramientas de gestión, sueldos de los agentes, analistas, coordinadores, cada cliente que visita las instalaciones de la empresa, el gerente tiene la responsabilidad de mencionar cómo funcionan las MS, supervisa todo el personal que está a su cargo, asiste a las juntas del comité de seguridad, toma las decisiones de los controles que se implementan dentro de su UUNN.

Coordinador de Mesa de Servicio.

Son las personas que se encargan de supervisar las mesas de servicio, de brindarle cualquier apoyo que requieran los agentes, cumplir cualquier requerimiento del cliente que se encuentren dentro del alcance de los servicios contratados.

Órganos de Gobierno "CISO".

Son las personas que tienen la responsabilidad de CISO (Chief Information Security Officer) oficial de seguridad de la información, son aquellas personas que presiden el comité de seguridad de la información, definen e implementan controles, elaboran políticas de SI, identifican riesgos y dan seguimiento a Incidentes de seguridad de la información, definen procesos, proporcionan capacitación de seguridad de la información, concientización de SI, hacen auditorias, implementan SGSI.

Gestor de Seguridad de la Información.

Son los responsables de asesorar al coordinador de seguridad de la información de sus actividades, supervisa que los análisis de riesgos estén bien desarrollados y dar el Vo.Bo. Monitorear el Antivirus que funcione adecuadamente, clasificar la información, hacer políticas, procesos, manuales.

Dirección ejecutiva "Coordinador de SI".

Son los responsables que toman las decisiones que concretan de cómo alcanzar un objetivo de negocio marcado por los órganos de gobierno.

El responsable de dirección ejecutiva, en este caso será el coordinador de seguridad de la información de la unidad de negocio quien es el responsable de verificar que se implemente una política, un control, cerrar los hallazgos que se obtienen en una auditoria interna o externa etc., y que se ejecuten todos los acuerdos que se definen en el comité de SGSI.

Dirección operacional "Agentes".

Son todas las personas que están en la mesas de servicio, los agentes que brindan el apoyo de dar soporte por vía telefónica, chat, correo y vía remota, solucionando cualquier requerimiento o incidente que reporta el cliente o ingeniero, en caso de que no pueda solucionarlo el agente, se encargará de escalar el ticket con un ingeniero para que lo apoye y se le dará seguimiento hasta su cierre.

10.2 Identificación del riesgo

10.2.1 Identificar Activos

Activo es todo aquel elemento que tiene valor dentro de una organización.

Para la identificación las amenazas, riesgos, vulnerables, impacto y consecuencia se definen de dos tipos de activos:

Los activos primarios:

- Procesos y actividades empresariales.
- Información.

Los activos de apoyo:

(Son utilizados por los activos principales).

- Recursos Humanos.
- Información.
- Sistemas.

- Software.
- Hardware (TI y comunicaciones).
- Infraestructura.

Recursos Humanos.

- R.H. incluye todo el personal de diferentes tipos de perfiles o puestos que forman parte de la UUNN del Service Desk.
- Agentes: Son los que se encargan de generar los tickets y solucionar los incidentes o requerimientos.
- Analistas: Son los que se encargan de hacer métricas e informes, encuestas, indicadores, monitoreo y otras actividades.
- Soporte especializado: Son los que se encargan de generar los tickets y solucionar los incidentes o requerimientos, en aplicación de diferentes clientes.
- Coordinador (Supervisor): Es el encargado de las mesas de servicio.
- Gerencia: Persona que se encarga de dirigir o administrar una sociedad, en este caso en la Unidad de Negocio del Service Desk “Mesas de Servicio”.

Información.

- Documentación operativa: Datos que materializan la información.
- Archivos de administración en papel, certificados, constancias, actas administrativas, formatos de asistencia de capacitación.
- Archivos de administración en medios electrónicos, manuales, instructivos, informes, métricas, métricas de agentes, presentaciones, políticas, protocolos.
- En pantallas de computadoras, monitoreo de red, aplicación de soporte vía remoto (TeamViewer).
- Audiovisual: Hace la referencia conjuntamente al oído y a la vista ejemplo WebEx solo para reuniones en línea como si fuera presencial.

Sistema y Software.

- Software: Una aplicación es un tipo de programa informático que se instala en las máquinas de los usuarios para poder realizar sus actividades, hay algunas aplicaciones que no se pueden nombrar las que se tienen en la empresa, ya que es confidencial.
- Sistema: Consiste en un software que sirve para interactuar con el sistema operativo, algunos de ellos se utilizan en la empresa como: sistema de grabación de llamadas “NICE”, Sistema de Telefonía “Avaya”.
- NICE: Permite la grabación de forma ordenada el ingreso y salida de todas las llamadas, los usuarios, agentes, proveedores.
- Avaya: El servicio de telefonía es de fundamental importancia para poder establecer el contacto con nuestros clientes y poder ofrecerles los servicios correspondientes.

Hardware (TI y comunicaciones).

- PC. Computadora personal de escritorio.
- Laptops. Computadora personal portátil.
- UPS. Unidad de alimentación ininterrumpida.
- Planta de Energía: Sistema de emergencia la luz comercial cuya operación consta de un motor de diésel y siempre lo hace a través de un switch de transferencia.
- Access Point: Punto de Acceso inalámbrico, es un dispositivo que interconecta a varios otros vía red inalámbrica, estos son algunos de los dispositivos que se pueden conectar como: Laptops, Impresoras, Teléfonos inteligentes “smartphones”.
- Cámaras de Seguridad: Es cámara de videovigilancia en tiempo real.

Infraestructura.

- Oficinas: espacios de trabajo e instalaciones, como el caso de las mesas de servicio que se encuentran en el primer nivel.

10.2.2 Identificar Amenazas

Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento y pueda afectar la operación, causando grandes daños para la unidad de negocio, la amenaza puede afectar como recursos, sistemas o aplicaciones, información, hardware, comunicaciones, infraestructura. Un ejemplo de una amenaza, un ERP no cuenta con una seguridad de control de acceso lógico, la vulnerabilidad es que todos tienen acceso de lectura y escritura afectando la integridad, el riesgo es el robo de identidad de los clientes registrados en el la herramienta de gestión ERP.

Tipos de amenazas para la seguridad de la información.

Existen muchos tipos de amenazas que pueden afectar la operación de una Mesa de Servicio, en la figura 6 se muestran algunos ejemplos.

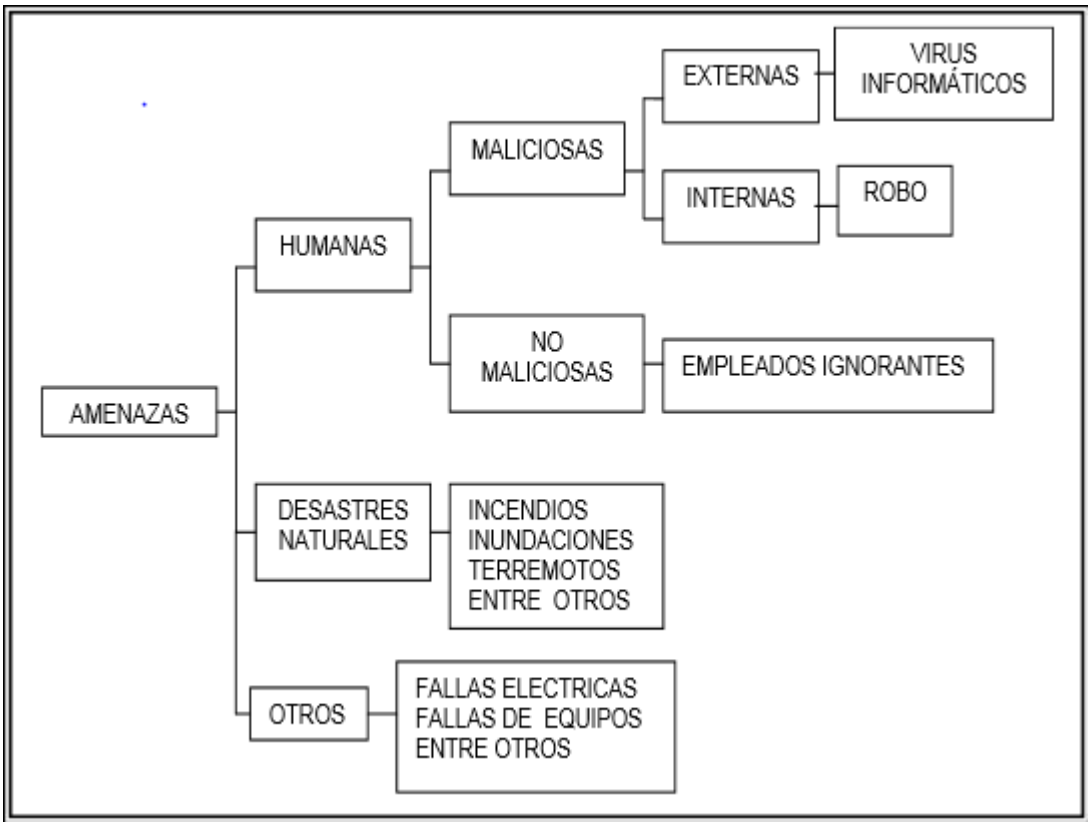


Figura 6 Tipos de Amenazas
Fuente: http://core.ac.uk/download/pdf/12401004.pdf

Amenazas Humanas

Está conformada por dos partes: maliciosas y no maliciosas.

Maliciosos externas

Son todos los tipos de virus que existen, hay infinidad de virus pero solo los más comunes, se mencionarán los que pueden afectar gravemente la Mesa de Servicio.

Virus informáticos

Son todos los virus que pueden infectar máquinas, existen infinidad de virus pero solo se mencionarán los más comunes y peligrosos que pueden eliminar un archivo hasta hackear un sistema.

¿Cómo funcionan los virus? Se puede decir que es un código que está basado en un lenguaje de programación que permite trabajar directamente sobre el hardware, a veces no necesita pasar por un sistema operativo.

En la figura 7 podemos observar una representación gráfica en la que se muestra cómo un hacker está compitiendo con una persona responsable de seguridad. A un hacker se le puede hacer fácil violar cualquier sistemas que sea vulnerable, y a un responsable de seguridad, se le dificultará reparar los daños que fueron afectados. (Tipos de datos, recuperar la información que se perdió, verificar la información existente, etc.) , es por eso que debe buscar una manera para proteger la información de estas amenazas, lo cual, normalmente se logra implementando controles de seguridad que deben seguirse por los empleados para asegurar que las amenazas no puedan incurrir en la información que maneja una empresa.

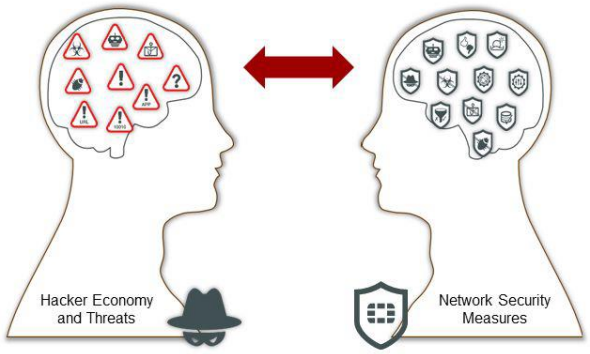


Figura 7 Hacker contra la seguridad
Fuente:
https://gm1.geolearning.com/geonext/fortinet/coursesummary.CourseCatalog.geo?id=22507230283

Spam

Este virus se distribuye por medio de un mensaje de correo y te puede llegar correos desconocidos con un nombre raro, también pueden llegar correos basura que no tienen ningún valor, cada vez que se envía un correo se puede infectar la máquina de un amigo compañero, podemos observar un ejemplo como se muestra en la figura 8.

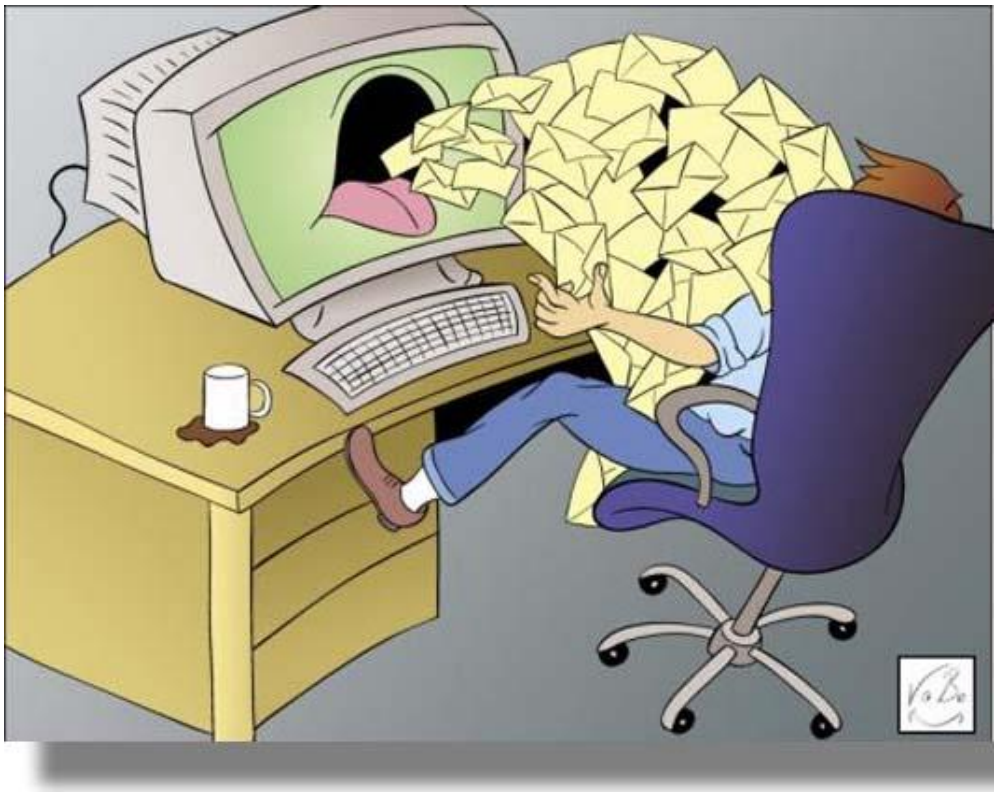


Figura 8 SPAM

FUENTE:https://elfidios.files.wordpress.com/2010/03/spam-email.jpg

Phishing

El termino Phishing es utilizado para referirse a uno de los métodos más utilizados para estafar y obtener información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. El estafador, conocido como phishier, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico.

Como se muestra en la figura 9 y 10 se puede observar un claro ejemplo de phishing. Supuestamente es un correo de Telmex solicitando que se realice un pago por la cantidad de $10,791.00, cuando le das click en ver el recibo Telmex, te direcciona a otra página, el link no dice Telmex viene con otro nombre diferente y nada que ver con Telmex, se recomienda cuando llegan estos tipos de correos, levantar un Ticket para eliminar el incidente y no pueda infectar más máquinas en la operación.

Todo este tipo de correos debe ser identificado y reportado para evitar que los empleados proporcionen información confidencial de la empresa y puedan poner en riesgo su confidencialidad, integridad y disponibilidad.

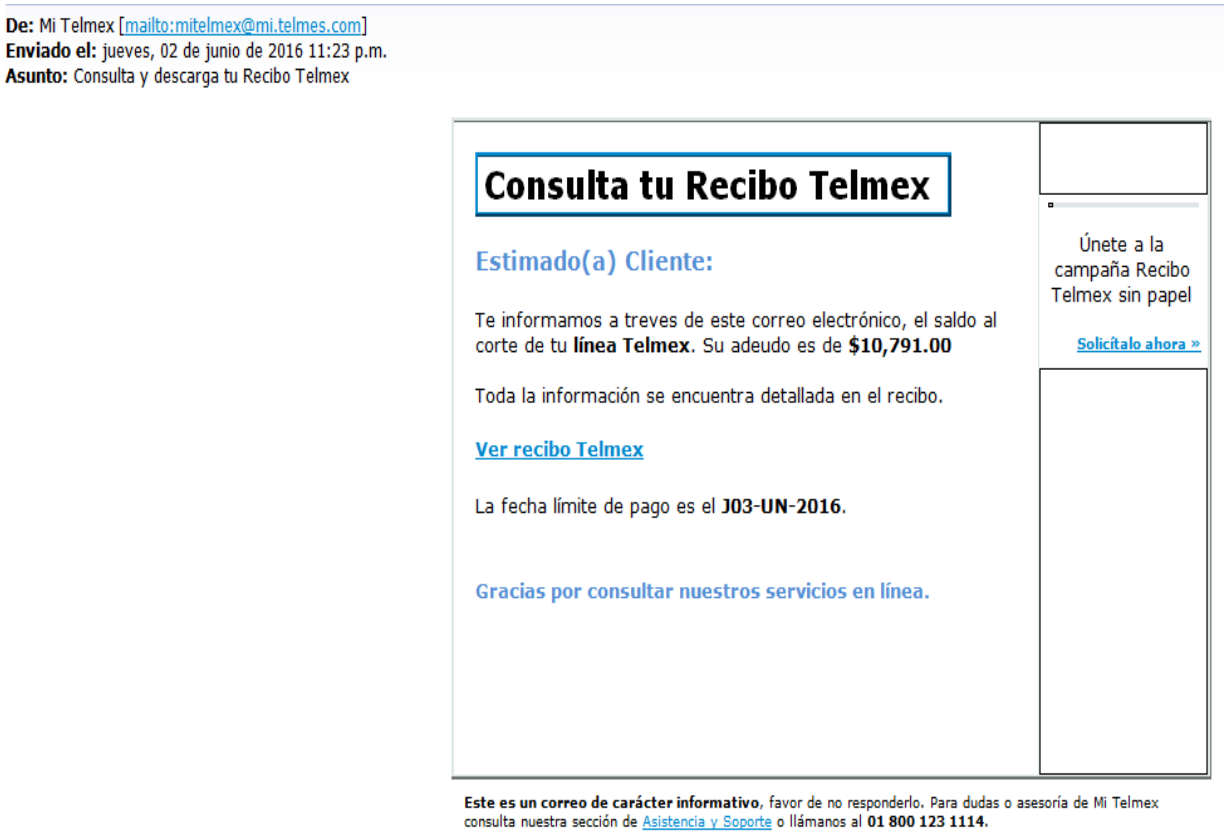


Figura 9 Ejemplo de Phishing

Fuente: Este virus llego a un correo corporativo.

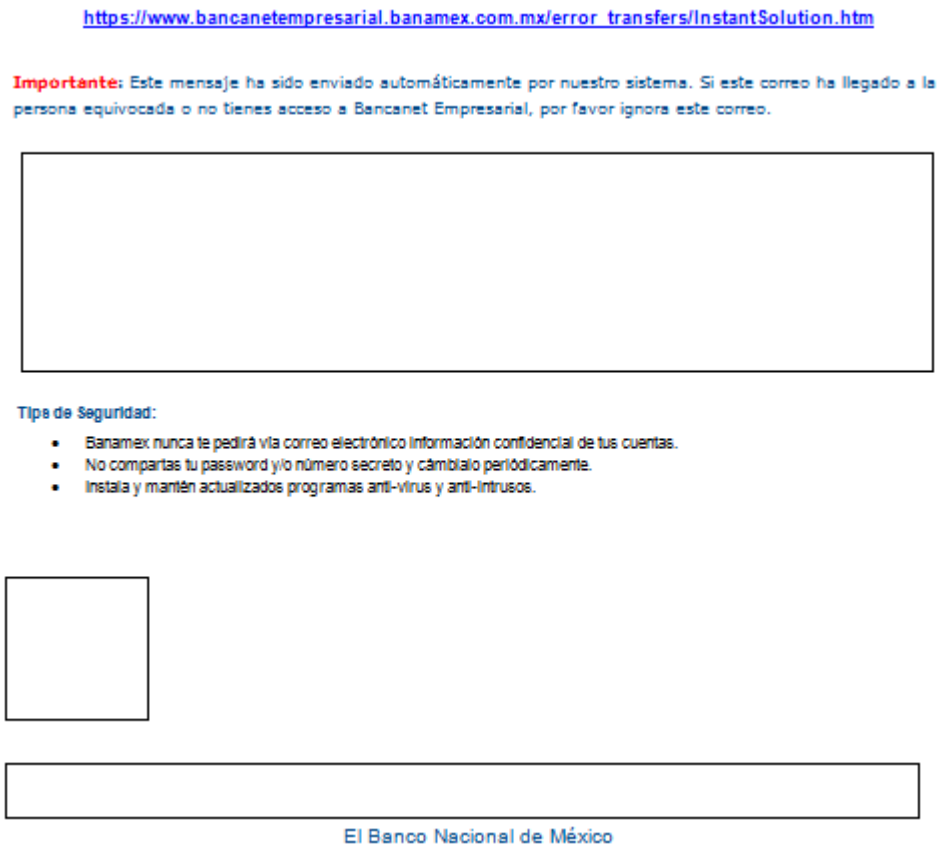


Figura 10 Ejemplo de Phisihing
Fuente: Este virus llego a un correo corporativo.

Ransomware.

Es un programa maligno que se instala en la computadora, una vez que tiene el control remotamente ya no te permite hacer nada y él tiene el control, se apodera de tu sistema, para poder negociar te piden una cantidad de dinero para que puedas utilizar toda la información, podemos verlo como ejemplo; un criminal secuestró a tu familia, lo primero que te dicen que tienes que hacer, es un depósito, en caso contrario puede que no veas a tu familiar, así funciona. El Ransomware es en inglés Ransom “rescate” y ware “Software”. Ejemplo de un equipo infectado en la figura 10.

Figura 11 Ejemplo de Ramsonware
Fuente:
http://wubingdu.cn/%e4%bb%8a%e5%b9%b4%e7%9a%84%e5%a8%81%e8%83%81%ef%bc%9a cryptolocker/

Gusanos (Worms)

Pueden no ser considerados como virus, ya que para replicarse no necesitan infectar otros archivos. Los gusanos realizarán una serie de copias de sí mismos (sin tener que infectar ningún otro archivo) a la máxima velocidad posible y enviándose a través de la red. Debido a esa replicación a alta velocidad pueden llegar a saturar la red a través de la que se propagan. Los canales más típicos de infección son el Chat, correo electrónico.

Troyanos o caballos de Troya.

Se puede llegar a pensar que los troyanos no son realmente virus, ya que no poseen su principal característica: auto reproducción. A pesar de esto, al igual que los gusanos, ambos son tratados como virus a la hora de ser detectados por los antivirus. Su nombre hace referencia a la historia griega, así su objetivo consiste en introducirse en el sistema como un programa aparentemente inofensivo, siendo verdaderamente un programa que permite el control remoto de dicho sistema. Al igual que los virus, pueden modificar, eliminar, ciertos archivos del sistema y a mayores pueden capturar datos confidenciales (contraseñas, números de tarjetas de crédito, etc.), y enviarlos a una dirección externa.

Maliciosos Internos

Robo de información.

Que todos los empleados puedan importar información en las bases de datos que se maneja dentro de la empresa, uno de los puntos más importantes para robar la información es que desde su equipo envíe por correo información sensible, que tenga habilitado los puertos, para poder utilizar los dispositivos extraíbles, como un USB para poder importar o exportar cualquier tipo de información.

No maliciosos

Empleados ignorantes.

Son aquellos empleados que no cubren el perfil que se está requiriendo para el puesto, ya que si no se contrata con el perfil adecuado el empleado no tendrá mucho conocimiento de sus actividades que realizará, a veces no es suficiente con la capacitación, la concientización de seguridad de la información que se les brinda es muy poco, si no tienen los conocimientos básicos será más difícil de aprender los conceptos de seguridad de ISO 27001, como la clasificación de la información, qué información debe estar en el Repositorio, carpetas en Red, qué

información deberá estar en escritorio y en la carpeta de mis documentos, qué personas deben tener privilegios en la herramienta de gestión.

Amenazas Desastres naturales

Incendios.

Una amenaza de incendios puede ser un poste de luz, que se queme, un transformador, un corto circuito, esto puede afectar gravemente la planta de luz de la empresa y provocar un incendio.

Inundaciones.

Una amenaza de inundación podría ser que la empresa tenga empleados trabajando en el sótano o en la planta baja donde se pueda inundar el corporativo y afectar todos los activos como computadoras, UPS, archiveros, información física (papeles), inmobiliario. Para estas amenazas se debe contar con un sitio alterno donde no afecte las mesas de servicio.

Terremotos

Amenazas de terremoto se podría decir que es muy poca la probabilidad de que haya un terremoto en la ciudad de México, si llegara a ocurrir, en la empresa no le afectará ya que se encuentra en buen lugar donde está diseñado para estas amenazas.

Otras Amenazas

Fallas de equipos.

Todos los equipos deberían tener mantenimiento por parte de los proveedores, por lo menos una vez al año para evitar cualquier amenaza.

Fallas eléctricas como Facilities Management “Gestión de Instalaciones”.

Que los facilities “Gestión de Instalaciones” no tengan una buena estructura de instalaciones eléctricas, también entra en esta categorización, las canastillas o canaletas para los cables de internet, infraestructura de TI, gestión de acceso.

10.2.3 Identificar Vulnerabilidades

Para cada activo-amenaza, se deberán identificar vulnerabilidades que tenga el activo, que pueda permitir que la amenaza se materialice.

10.2.4 Identificar Controles Existentes

Se deberán identificar controles existentes que ayuden a salvaguardar el proceso ante las amenazas-vulnerabilidades identificadas para los activos. Eventualmente los controles lograrán aportar seguridad a más de un activo identificado. Los controles disminuyen o ayudan a justificar la vulnerabilidad de los activos.

10.2.5 Identificar Consecuencias

Son los daños que provocaría que se materialice una amenaza, afectando que nuestros clientes se queden sin servicio, esto puede ocasionar hasta cancelación de contratos de nuestros clientes.

10.3 Análisis de riesgo

Es una aproximación metódica siguiendo una serie de pasos, para identificar y determinar el nivel de riesgos, que se van a tratar con ayuda de una matriz de riesgos.

Para que se obtenga la información de la matriz de riesgos se requiere de la participación de diferentes áreas de responsabilidad dentro de la empresa, con una lluvia de ideas y poder identificar más fácil los Activos, Amenaza, Vulnerabilidad, Impacto negativo, Riesgo y Probabilidad en un corto tiempo.

En el formato de matriz de riesgos mostrado se menciona los códigos y algunos tipos de activos, donde se deben llenar los Riesgos, Amenazas, Vulnerabilidades, identificados en el análisis de riesgos.

10.3.1 Evaluar Impacto de las Consecuencias

Determinar impacto: Se debe cuantificar el daño que se produciría si la vulnerabilidad es explotada por la amenaza. Corresponde al impacto identificado, como se muestra en la tabla 4.

Nivel de Impacto (IMPACTO).

Mínimo: Activo(s) que su ausencia no afecta la operación o entrega del servicio, si el nivel del impacto es muy bajo, se acepta el riesgo.

Menor: Activo(s) que su ausencia afecta parcialmente la operación o entrega del servicio, no se toman acciones, para trabajarlo se acepta el riesgo.

Moderado: Activo(s) que su ausencia afecta la operación o entrega del servicio, se acepta el riesgo pero no es tan grave para la UUNN.

Mayor: Activo(s) que su ausencia significa entregar un servicio degradado o deficiente, es un activo parecido al No aceptable también se tienen que atender de forma urgente.

No Aceptable: Activo(s) que su ausencia impide la entrega del servicio, este activo requiere atención urgente.

IMPACTO		
Valor	**Descripción**	**Impacto al negocio**
5	No Aceptable	Acontecimiento importante con la pérdida de sistemas críticos.
4	Mayor	Acontecimiento significativo que afecta sistemas críticos.
3	Moderado	Impacto moderado con la pérdida de eficacia.
2	Menor	Impacto de menor importancia que requiere trabajo adicional.
1	Mínimo	Efecto insignificante sobre las operaciones.

Tabla 4 Impacto

Fuente: Autoría propia

10.3.2 Evaluar Probabilidad de Incidencia

Determinar probabilidad: Se debe identificar una probabilidad de ocurrencia de la explotación de la vulnerabilidad por la amenaza considerando los controles actuales, como se muestra en la tabla 5.

Niveles de Probabilidad.

Remota: el evento no ocurre nunca o casi nunca

Improbable: si bien el evento puede ocurrir, el periodo entre uno y otro evento puede ser muy grande.

Probable: es posible que ocurra el evento con una frecuencia baja.

Altamente probable: existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo, pero la frecuencia no es alta.

Casi Cierta: el evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta.

PROBABILIDAD		
Valor	**Descripción**	**Periodicidad**
5	Casi cierta Probable	A diario.
4	Altamente Probable	Semanalmente.
3	Probable	Mensualmente.
2	Improbable	Una vez al año.
1	Remota	Cada varios años.

Tabla 5 Probabilidad

Fuente: Autoría propia

10.3.3 Determinar el Nivel de Riesgo

Determinar el riesgo: La dupla Impacto-Probabilidad de un riesgo se grafican en una tabla de doble entrada y de esta forma se obtiene gráficamente los riesgos que tienen probabilidad de ocurrencia y que causan daño al cumplimiento de los objetivos de negocio planteados a la unidad en estudio. Esta tabla la denominaremos Cuadro de Riesgo, Tabla 6 y 7.

Cuadro de Riesgos Identificados					
IMPACTO					
5 - No Aceptable	MODERADO	MODERADO	MAYOR	NO ACEPTABLE	NO ACEPTABLE
4 - Mayor	MODERADO	MODERADO	MAYOR	MAYOR	NO ACEPTABLE
3 - Moderado	MENOR	MENOR	MODERADO	MODERADO	MAYOR
2 - Menor	MENOR	MENOR	MODERADO	MODERADO	MODERADO
1 - Mínimo	MENOR	MENOR	MENOR	MENOR	MODERADO
	1 – Remota	2 – Improbable	3 - Probable	4 - Altamente Probable	5 - Casi Cierta
	PROBABILIDAD				

Tabla 6 Cuadro de Riesgos Identificados

Fuente: Autoría propia

Como se puede ver el resultado de un impacto y probabilidad, es muy sencillo se tuvo que realizar una tabla ya con los resultados, para obtener un resultado de riesgo se tiene que realizar de la siguiente manera:

Ejemplo, Riesgo=impacto*probabilidad, Mínimo*Remota=Menor.

IMPACTO	PROBABILIDAD	RESULTADO
Mínimo	Remota	Menor
Menor	Remota	Menor
Moderado	Remota	Menor
Mayor	Remota	Moderado
No Aceptable	Remota	Moderado
Mínimo	Improbable	Menor
Menor	Improbable	Menor
Moderado	Improbable	Menor
Mayor	Improbable	Moderado
No Aceptable	Improbable	Moderado
Mínimo	Probable	Menor
Menor	Probable	Moderado
Moderado	Probable	Moderado
Mayor	Probable	Mayor
No Aceptable	Probable	Mayor
Mínimo	Altamente Probable	Menor
Menor	Altamente Probable	Moderado
Moderado	Altamente Probable	Moderado
Mayor	Altamente Probable	Mayor
No Aceptable	Altamente Probable	No Aceptable
Mínimo	Casi Cierta	Moderado
Menor	Casi Cierta	Moderado
Moderado	Casi Cierta	Mayor
Mayor	Casi Cierta	No Aceptable
No Aceptable	Casi Cierta	No Aceptable

0	NO ACEPTABLE
0	MAYOR
0	MODERADO
0	MENOR
0	Riesgos

Tabla 7 Cuadro de resultados de Nivel de Riesgo

Fuente: Autoría propia

10.4 Evaluación del riesgo

10.4.1 Evaluar los niveles de riesgo basado en el criterio de evaluación

De acuerdo a los niveles de riesgo estimados del análisis de riesgo se determinan las prioridades para el tratamiento.

La organización ha determinado que se **ACEPTAN** todos los riesgos valorados como **1, 2 y 3.**

Los riesgos que son valorados como **4 y 5**, **deben ser tratados**, tomando en consideración el impacto financiero que su implementación demande.

Riesgo = Probabilidad * Impacto.

Nivel de Riesgo	Prioridad de atención
5	1
4	2
3	N/A
1 y 2	N/A

10.5 Tratamiento del riesgo

Para el tratamiento se tiene que llenar el formato de control de riesgos, en el campo responsable/seguimiento y Actividades, tiene que ir una serie de actividades que se tiene que realizar para el tratamiento del riesgo, como se muestra en la tabla 8 anterior.

Riesgo residual, es el riesgo resultante de la aplicación de los controles necesarios, para el tratamiento de un riesgo y reducir el riesgo por completo con la ayuda del cuadro riesgos.

El riesgo residual también es una medida que permite comprender el éxito de la implementación de los controles de seguridad utilizados.

10.5.1 Seleccionar opciones de tratamiento de riesgos

Tratamiento de riesgo **Aceptar**. Reconocer la existencia del riesgo y sus consecuencias sin tomar ninguna medida directa sobre ellos, el CISO es el que toma la decisión y es el responsable de tomar el riesgo.

Tratamiento de riesgo **Eludir o Evitar.** Utilizando un activo distinto o modificando el proceso, de manera que las amenazas originales ya no lo afecten.

Tratamiento de riesgo **Transferir**. Es decir, mover el riesgo para que una entidad distinta asuma las consecuencias de la materialización de las amenazas, por ejemplo si el riesgo son las personas, hay mucha rotación de personal por los salarios, entonces contrato un call center donde cubra la cantidad de vacantes que requiero y ya estoy transfiriendo el Riesgo.

Tratamiento de riesgo **Mitigar**. Lo cual significa adoptar medidas que minimicen la vulnerabilidad que permite la existencia del riesgo, todos los riesgos que se tengan que mitigar se tienen que atender lo más pronto posible porque son urgentes, que pueden ser una amenaza para la operación, el coordinador de la UUNN tiene que ser responsable de darle seguimiento, que se ejecuten conforme las actividades que se planearon, al final este riesgo tiene que reducirse al mínimo.

10.5.2 Elaborar plan de tratamiento de riesgos

Por cada riesgo identificado critico o mayor se tiene que llenar un formato de control de riesgo, todo formato de riesgo no debe tener ningún campo vacío, en caso contrario el formato no se revisará para la aprobación y autorización de la gerencia, Ejemplo, si se tiene 10 riesgos críticos y/o mayores, el total deben ser 10 formatos de control de riesgos, los formatos deben ser como se muestra en la tabla 8.

Todos los riesgos que salieron como menor y moderado, solo se tiene que llenar un solo formato, en el formato viene una opción del código de riesgo, es ahí donde vamos a poner el código de N de riesgos Ejemplo (PER-1, FIS-2, DOC-3).

El coordinador de seguridad de la información tiene que llenar todos los formatos por cada riesgo que se tenga, después de llenar los formatos se pasará a revisión con el CISO oficial de seguridad de la información para dar el Vo.Bo. Después del visto bueno se tendrá que realizar una junta con el coordinador de SI, con el Gerente de la UUNN y el director de la empresa o representante de la dirección para la aprobación, autorización y firmar los controles que se tienen que implementar.

Formato de Control de Riesgos.

NOMBRE RIESGO:							
CÓDIGO RIESGO							
IDENTIFICADO POR							
FECHA:							
OPCIÓN DE TRATAMIENTO DEL RIESGO							
ACEPTAR		**ELUDIR**		**TRANSFERIR**		**MITIGAR**	**x**
Confidencialidad	**X**	**Integridad**	**X**	**Disponibilidad**	**X**		
Control	**Fecha inicio Imp.**	**Fecha termino imp.**	**Responsable Imp.**	**Responsable Seguimiento**	**Actividades**	**Entregables**	**Obs. Plan**
C2							
C3							

Tabla 8 Formato de Control de Riesgos

Fuente: Autoría propia

10.5.3 Evaluar riesgo residual

Es el riesgo que queda después de implementar un control, no hay riesgo que este en ceros, un ejemplo de un riesgo residual, si tengo un servidor, pero no cuento con una planta de luz, un UPS, la probabilidad es alto de que me quede sin servicio, para este riesgo tengo que implementar un control (comprar una planta de luz y un UPS), el riesgo residual será muy bajo de que me quede sin servicio.

10.5.4 Implementar plan de tratamiento de riesgos

Se realizara un plan de tratamiento de riesgos, donde se tiene que dar seguimiento los controles que se implementaron, en este plan se pretende que se dé seguimiento, se ejecuten los controles, ir midiendo el avance de los riesgo, para el plan se hará un formato donde contenga, código de riesgo, referencia de la norma, cual es el control que se va implementar, amenaza, vulnerabilidad, responsable de implementación, fecha de inicio de implementación, fecha final de implementación, nomenclatura (NI, D, A, EI, I), nivel de riesgo “mayor”, riesgo residual, evidencia.

Nomenclatura
No Iniciados=NI
En desarrollo=D
Aprobado=A
En Implementación=EI
Implementados = I

Por cuestiones de seguridad, no se puede visualizar al 100% el formato de gestión de riesgos de Seguridad de la Información, como se muestra la de la tabla 9.

FORMATO DE PLAN DE TRATAMIENTO DE RIESGOS GESTION DE SEGURIDAD DE LA INFORMACIÓN

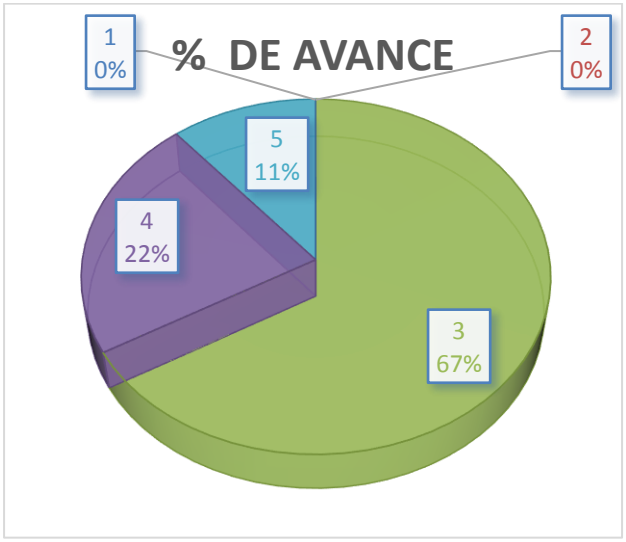
Gerencia de Mesas de Servicio

CÓD. DE RIESGO	Ref. Norma 27000	Control	Amenaza	Vulnerabilidad	Estrategia de Reducción de Riego	Responsable de implementación	Fecha de Inicio de Implementación	Fecha de Fin de Implementación	NI	D	A	EI	I	Total	Nivel de Riesgo Inicial	Cobertura	Riego Residual	Efectividad	Seguimiento Comentarios
DOC-1															MAYOR	80.00%	20.00%		
FIS-2															MAYOR	70.00%	30.00%		
PER-3															MAYOR	70.00%	30.00%		
SOF-2															MAYOR	90.00%	10.00%		
SOF-5															MAYOR	70.00%	30.00%		
SOF-7															MAYOR	80.00%	20.00%		
SOF-8															MAYOR	80.00%	20.00%		

SOF-9														MAYOR	60.00%	40.00%			
SOF10														MAYOR	70.00%	30.00%			
								Total	0	0	6	2	1	9					
								%	0.000%	0.000%	66.67%	22.22%	11.11%	100.00%					

Tabla 9 Plan de tratamiento de riesgos

Fuente: Autoría propia/CISO



RIEGO RESIDUAL:
NIVEL DE SEVERIDAD X (1 -% COBERTURA)
TABLA DE RIESGO
NO ACEPTABLE
MAYOR
MODERADO
MENOR

10.6 Aceptación del riesgo

10.6.1 Aceptar plan de tratamiento de riesgos

Aceptar el plan es el mismo que el punto 10.6.2, ambos van de la mano solo que esta primero el plan para el tratamiento de riesgo como se muestra en la tabla 9.

10.6.2 Aceptar Riesgo Residual

La dirección y el oficial de seguridad de la información “CISO” toman la decisión de aceptar el Riesgo, cuando se acepta un riesgo es porque genera costo y no tiene caso para una inversión en el activo, prefieren tomar el riesgo así sea Mayor o No aceptable, a veces hay empresas que no pueden pagar para el tratamiento del riesgo.

10.7 Comunicación y consulta sobre riesgos

Se debe de comunicar solo a las personas involucradas como: Director Genera, Gerencia del SD, Coordinadores de SI, CISO, Auditores Internos o Calidad, Consultores de SI. Cada dos meses se realiza un comité de seguridad “Reunión”, donde se presentan todo la información sobre los riesgos como:

- Evaluación de riesgos y nivel de riesgo.
- Amenazas, vulnerabilidades, consecuencias.
- Plan de tratamiento de riesgos.
- Avance de gestión de riesgos y sus resultados.
- Métricas de gestión de riesgos.
- Hallazgos.
- Informe de seguridad de la información.

Toda esta información está en el repositorio, solo las persona autorizadas pueden consultar este tipo de información, está disponible en cualquier momento que se requiera, si hay personas que requieran consultar, pero no tienen acceso se pide

apoyo con el dueño del repositorio y el decide si le da acceso o solo le brinda los datos que requiera.

10.8 Monitoreo y revisión de los riesgos

Cada gerencia se encarga de monitorear sus propios riesgos. La organización de cada unidad de negocio, debe de asegurarse de supervisar los siguientes:

- Nuevos activos de gestión de riesgos.
- Valores de activos modificados.
- Nuevas amenazas.
- Nuevas vulnerabilidades.
- Mayor impacto y consecuencia, que resulte en un nivel aceptable.
- Incidente de seguridad de la información.

Cada año se tiene que realizar un análisis de riesgos, con la finalidad de obtener nuevos activos, vulnerabilidades, riesgos y amenazas.

El resultado de este monitoreo, revisiones y evaluación de seguridad será entrada al procedimiento de Gestión de Riesgos.

11 Concientización y formación profesional de seguridad de la información

Concienciación.

El mejor plan de seguridad es dar una plática de concienciación, se propone que cada colaborador que elabora en la empresa y nuevo ingreso, tome el curso de concientización, es por ello que se requiere enseñarles a tener una cultura en la seguridad la información, tener conciencia, son tres principios básicos de esta cultura.

- Una política de seguridad corporativa.
- Una normativa segura “Reglamento Interno SD”.
- Una formación continua, recordándole a todo el personal sus actividades que deben de realizar dependiendo de cada puesto que tengan.

Se debe de hacer un comunicado de concienciación, poner propaganda en las entradas de las instalaciones, en las pantallas de escritorio, en el gafete, en los baños, comunicado por correo, en la nube, en el sistema de sonda plus.

Formación Profesional de SI.

Cuando existe un nuevo ingreso, cambio de puesto, cambio de área, nuevo rol, se debe capacitar al empleado mínimo un mes, la cual va a depender del perfil del puesto que se requiere y actividades que va a realizar, para el rol de seguridad de la información, se capacitará y se enseñará cómo realizar un análisis de Riesgo, y en caso de que no cuente con estos cursos básicos se le brindará un curso de ITIL y uno de ISO/IEC 20000.

Cuando me asignaron el nuevo rol de coordinador de seguridad de la información no contaba con los cursos anteriormente mencionados, tuve una capacitación durante tres meses, al mismo tiempo estaba tomando curso de ITIL y otro de ISO/IEC 20000; después de tomar la capacitación, la gerencia toma la decisión

para que el empleado presente un examen de certificación oficial, depende del puesto que tiene.

Las empresas que solicitan personal para cubrir puestos de seguridad informática requieren que el candidato cuente con base a un estudio de mercado con al menos una certificación como las siguientes:

- ISO/IEC 27001
- CISM
- CISSP
- CISA
- ITILv3
- COBIT 5

MATRIZ RAZI.

La matriz RAZI "Responsible, Accountable, Consulted, and Informed" se define e identifican las responsabilidades con la ejecución de las actividades del proceso, ayuda a definir roles y responsabilidades, como se muestra en la Tabla 10.

	Rol	**Descripción**
R	Responsable (Encargado).	Rol que realiza la actividad y es responsable por su ejecución, si vemos del lado de la mesa de servicio el encargado seria el coordinador de seguridad de la información que está dando seguimiento al riesgo.
A	Accountable (Responsable)	Rol que se encarga de aprobar la actividad y asegurarse de que se realice correctamente, normalmente también se identifica como el gestor del proceso de seguridad de la información.
C	Consulted (consultado)	Rol que posee información para iniciar o concluir la actividad.

I	Informed (Informado)	Rol que debe ser informado sobre el progreso y resultados de cada actividad.

Tabla 10 Matriz RACI

Fuente: Autoría propia

11.1 Medidas preventivas y correctivas de riesgos

11.1.1 Ciclo de Incidente

Incidente es una interrupción no planificada, también se conoce como una falla de algún activo, un ejemplo de un incidente es que el disco duro no funcione.

El ciclo de incidente cuenta con las siguientes etapas: Amenazas, Incidentes, Daños y Recuperación, como se muestra en la figura 12.

- Preventivos: Es prevenir cualquier tipo de activo antes de que ocurra un incidente.
- Reductivos: Reducir la amenaza con la ayuda de los controles.
- Detectivos: Detectar los incidentes.
- Represivos: Detener las amenazas antes de que ocurra cualquier daño.
- Correctivos: Que ya se corrigió el daño que se tenía.
- Evaluado: ya se evaluó la amenaza.

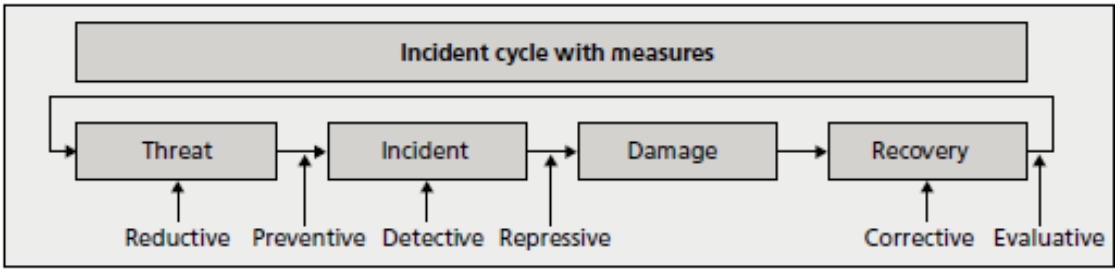


Figura 12 Ciclo de incidente

Fuente: Foundations of IT Security Based on ISO27001/27002

11.1.2 Auditorías Internas o/e Externas

La auditoría es la revisión y la evaluación de los controles, sistemas de gestión de seguridad de la información, de los procesos, equipos, instalaciones, en la auditoria se deberán evaluar en general los sistemas de información como, procedimientos, archivos, controles, con la finalidad de ser más eficiente en el servicio.

Realizar auditoria interna por lo menos dos veces al año y una auditoria externa al año, validar que se estén cumpliendo las políticas, controles, reglamentos internos del UUNN, en caso que se tenga algún hallazgo se tienen que cerrar lo más pronto posible, existen algunos tipos de hallazgos como, No conformidad menor o mayor, Observaciones, Oportunidad de mejora, se utilizara un formato para llenar los hallazgos como se muestra en la tabla 11 y 12.

Hallazgo: Evidencia de la auditoría, de tipo cualitativa o cuantitativa, recopilada en función de los criterios de auditoría. Es una desviación del Sistema de Gestión del Servicio, que resulta en No Conformidad, Observación (No Conformidad potencial) y Oportunidad de Mejora. De estas se desprenden: Acción Correctiva y Acción Preventiva. Cabe destacar, que dentro de esta descripción se encuentran los incumplimientos de un requisito normativo, una política, un procedimiento, un instructivo, un reclamo u otro, como se muestra en la tabla 12.

No conformidad Menor: Es el incumplimiento de la norma, que se cumplió el seguimiento pero de forma incorrecta, pero no pone en riesgo significativo la calidad del producto o servicio, las no conformidades menores son normalmente controladas para implantar correcciones.

No conformidad mayor es un incumplimiento, de forma clara y/o sistemática, a uno o más requisitos de la norma, esto significa que no se cumplió o no se dio seguimiento al hallazgo y no fue ni tratado o cerrado.

Observaciones. Es el mínimo de errores que se detectaron, pero si se deja de hacer y no se les da el tratamiento correcto, se puede convertir en no conformidad. Ejemplo, se realiza una lista blanca de Software que se tiene instalado en las máquinas, después se envía la lista a TI para que ejecute el software que se deben tener instalados, pero si el responsable de seguridad de la información no tiene una evidencia como (correo, imprimir pantalla, minuta), que si está funcionando correctamente, si no se demuestra que se está dando seguimiento, se tomará como una observación.

ACCIÓN CORRECTIVA: Acción ejecutada para eliminar la causa de una no-conformidad detectada u otra situación.

ACCIÓN PREVENTIVA: Acción ejecutada para eliminar la causa de una observación (potencial No Conformidad).

Formato de Referencia Auditoria.

Es un ejemplo de cómo se llena un Informe de Auditoria interna de seguridad.

<table>
<tr><th colspan="2">REFERENCIA AUDITORIA: AUI-DS-GSI-02</th></tr>
<tr><td colspan="2">AREA O UNIDAD DE NEGOCIO AUDITADA: MESAS DE SERVICIO</td></tr>
<tr><td>AUDITOR LÍDER:
CISO</td><td>FECHA AUDITORÍA:</td></tr>
<tr><td>AUDITORES:
Delfino Vázquez García</td><td>OBJETIVO DE LA AUDITORÍA:

Revisar:
1.- Atención de hallazgos de Auditorias previas de SI.
2.- Cumplimiento de la norma ISO/IEC 27001:2013
3.- Cumplimiento de la Políticas y Procedimientos de Seguridad de la Información</td></tr>
<tr><td>AUDITADOS:
Pedro
Pepe
Pablo</td><td rowspan="2">METODOLOGÍA UTILIZADA:

Mediante entrevistas, revisión documental y recorrido físico, se revisaron los objetivos de la auditoria con apoyo de la lista de verificación.</td></tr>
<tr><td>RESUMEN DE HALLAZGOS:
No Conformidades:
Observaciones:
Oportunidades de Mejora:</td></tr>
</table>

FORTALEZAS DETECTADAS

DEBILIDADES DETECTADAS

NO CONFORMIDADES		
N°	**HALLAZGO**	**REFERENCIA NORMATIVA**
1		
2		

OBSERVACIONES		
N°	**HALLAZGO**	**REFERENCIA NORMATIVA**
1		

Resumen

Hallazgos	Cantidad
No Conformidad	**0**
Observación	**0**
Oportunidad de Mejora	**N/A**

Tabla 11 Formato de Referencia Auditoría

Fuente: Autoría propia

Oportunidad de mejora.

Una mejora es cuando podemos automatizar algún procedimiento, sistema, informes, reuniones del CAB Change Advisory Board “Consejo consultor de Cambios”. Un ejemplo de mejora, los días miércoles se lleva a cabo una reunión de cada cambio que se realizará de algún activo es igual a un CI o CI´s (elemento de configuración, anteriormente se tenían tres reuniones en diferentes salas de cada UUNN, actualmente lo que se sugiere es que se junten las tres UUNN en una sola reunión.

Formato de Registro de Hallazgos.

REGISTRO DE HALLAZGOS				
SECCIÓN I		**DETECCIÓN**		
DIVISIÓN	GERENCIA	RESPONSABLE	PROCESO	
SERVICIOS	Mesas de Servicio	DELFINO VAZQUEZ GARCIA	RECLAMO CLIENTE	
FECHA	PROCESO	MOEBIUS NUMERO DE REGISTRO	SERVICIO O PRODUCTO NO CONFORME	
			AUDITORÍA INTERNA	X
28/07/2016	GSI	GSD-ASI-01	AUDITORÍA EXTERNA	X

SECCIÓN II			**DESCRIPCIÓN**	
NORMA			TIPO DE HALLAZGO	CÓDIGO GSD-ASI-01
ISO 9001:2008		ISO 20000:2011	NO CONFORMIDAD	X
		X	OBSERVACIÓN	X
			OPORTUNIDAD DE MEJORA	X
REQUISITO NORMATIVO				
DESCRIPCIÓN DEL HALLAZGO				

SECCIÓN III	**ACCIÓN INMEDIATA**
FECHA	RESPONSABLE
	Delfino Vazquez Garcia

SECCIÓN IV	**ANÁLISIS DE CAUSA**
¿Por qué	
¿Por qué	
¿Por qué	
¿Por qué	
¿Por qué	
FECHA	RESPONSABLE
	Delfino Vazquez Garcia

SECCIÓN V						
ACCIÓN CORRECTIVA	X	ACCIÓN PREVENTIVA		OPORTUNIDAD DE MEJORA		
Objetivo:						
ACTIVIDAD		No.	RESPONSABLE	FECHA COMPROMISO		ENTREGABLE
FECHA				RESPONSABLE		

SECCIÓN VI	**SEGUIMIENTO DE LA ACCIÓN**
FECHA PROGRAMADA	RESPONSABLE
	Delfino Vazquez Garcia
FECHA REALIZADA	RESPONSABLE
	Delfino Vazquez Garcia

SECCIÓN VII	**VERFICIACIÓN DE LA EFICACIA**
FECHA PROGRAMADA	RESPONSABLE
	CISO
FECHA REALIZADA	RESPONSABLE
	CISO

Tabla 12 Formato de Registro de Hallazgos

Fuente: Fuente: Autoría propia

11.2 Mejora continua

Revisar, analizar y hacer recomendaciones de oportunidades de mejora.
Mejora continua proporciona guía para:

- Mejorar los servicios.
- Mejorar la efectividad y eficiencia de los procesos de seguridad de la información.
- Medir procesos y servicios.

Debemos de mejorar en la Unidad de Negocio cómo automatizar un informe de seguridad de la información, si anteriormente se realizaban tres informes por diferentes unidades de negocio ahora se tiene que realizar un solo informe en general.

La valoración del riesgo, lo que se recomienda es que por lo menos una vez al año se tiene que hacer un análisis de riesgo completo para todos los activos de información, revisión documental de políticas, procesos, instrucciones de trabajo, hardware, software, facilities (infraestructura).

Mejoras
Se implementó un reglamento interno para la UUNN de SD, se realizó una visita a sus lugares del personal de la empresa para que firmara el reglamento interno.
Se implementó una política de pantallas limpias, cada cinco minutos se bloquea la pantalla si se deja de utilizar la máquina de escritorio o laptop, esto aplica a todo el personal.

El coordinador del SD realizará un recorrido a todas las mesas, realizará pre auditoría al personal, revisará que no tengan instalado ningún software no autorizado.

11.3 Informe de seguridad de la Información

Cada fin de mes se tiene que entregar un informe de incidentes de seguridad de la información junto con los KPI´s.

Informe es donde se tiene la finalidad de dar a conocer el seguimiento y control de seguridad de la información de la UN “Mesas de Servicio que no se ha llevado a cabo en el mes correspondiente”, si se obtiene un incidente de seguridad, se tiene que documentar en el informe y se le dará seguimiento hasta cerrar el Incidente, solicitando la evidencia de cuál fue la causa raíz del problema y la solución del incidente.

KPI’s

KPI’s (Indicadores Clave de Desempeño) son utilizados para juzgar la eficiencia y la eficacia, con la reducción del porcentaje de objetivos no cumplidos.

CAB

Se realizan reuniones los miércoles para la aprobación de cada cambio de activo o CI´s que se tiene en el CAB “Consejo Consultor de Cambios”, para esto se tiene las 7 Rs que son las preguntas que se toman en cuenta para poder aprobar un RFC “formato de solicitud cambio”, para cada cambio de activo se tiene que llenar un RFC, todos los campos deben ser llenados y entendibles, en caso contrario se le regresará el formato del RFC y hasta que lo envíe con la corrección puede seguir con el proceso de cambio, como se muestra en la tabla 13.

Existen tres tipos de cambios: Normal, Emergente, Estándar.

Normal: Se realiza una reunión con todos los involucrados de diferentes áreas para aprobar el cambio de cualquier tipo de activo.

Emergente: Solo cuando hay un cambio emergente este tipo de cambio no se puede esperar hasta la siguiente reunión del CAB ya sea que lo requiera el cliente

o puede ser un incidente mayor, para un cambio emergente piden la autorización del responsable del CAB, el responsable del activo y el Director de la empresa.

Estándar: Es cuando ya fue discutido por las 7 Rs y aprobado por el CAB después de ser documentado, esto apenas esta como pre-aprobado. Se le dice así, porque cuando se está realizando la ejecución del cambio pueda que no tenga éxito el 100% del cambio, en caso de fallar se realizara el Rollback.

Las 7 Rs.

¿Quién REQUIERE el cambio?

¿Cuál es la RAZÓN del cambio?

¿Cuál es el RETORNO esperado del cambio?

¿Cuáles son los RIESGOS implicados en el cambio?

¿Cuáles son los RECURSOS necesarios para realizar el cambio?

¿Quién es el RESPONSABLE de la construcción, prueba e implementación del cambio?

¿Cuál es la RELACIÓN entre éste y otros cambios?

Formato de RFC

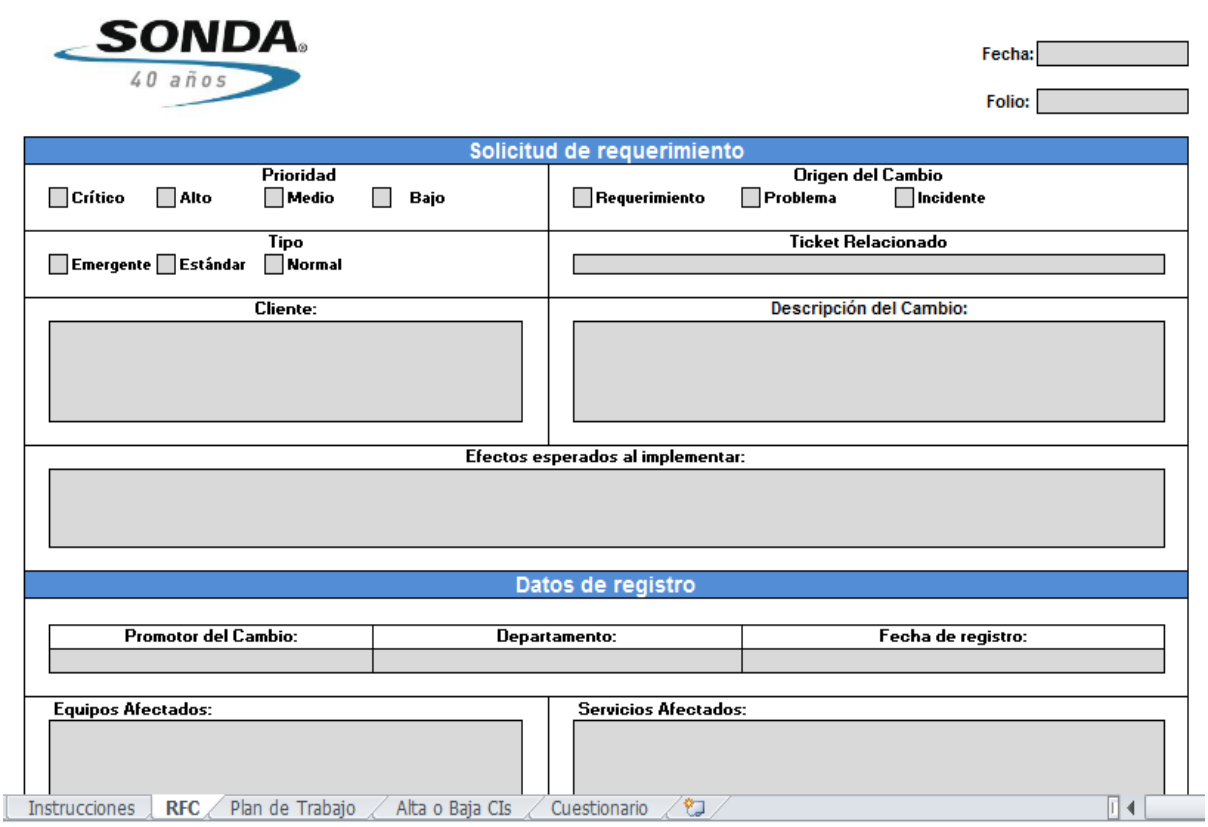


Tabla 13 Formato de RFC

Fuente: Autoría propia / CISO

12 Conclusión y Recomendaciones

El presente proyecto titulado “Propuesta de Gestión de Seguridad de la Información de Mesas de Servicio de la Empresa Sonda México S.A de C.V.” se realizará con el objetivo de lograr que la empresa sea competitiva, eficiente, eficaz y proporcione calidad en el servicio a clientes.

Al aplicar la metodología Magerit, se llevará a cabo el Análisis de Riesgo que permitirá conocer riesgos, amenazas, vulnerabilidad, para cada tipo de activo de la UUNN. Al concluir el análisis se implementarán políticas, controles, procedimientos de seguridad de la información, clasificando todo tipo de información, seguridad física y lógica, con la finalidad de disminuir el mínimo de riesgos. Se pretende que la empresa sea certificada en la norma ISO/IEC 27001:2013.

El crecimiento en las TI ha ido en aumento, es por ello que la seguridad de la información debe de crecer al mismo paso. Día a día se debe de buscar cómo proteger la información ante los nuevos riesgos que van apareciendo.

Todos los empleados se deben apegar a los lineamientos establecidos para mantener la seguridad de los activos y así obtener un buen resultado y evitar cualquier amenaza, al principio no será fácil para los usuarios seguir los lineamientos porque muchos de ellos están en contra de las políticas, sin embargo se debe de crear conciencia y proporcionar los fundamentos de seguridad de la información de acuerdo a las normas ISO/IEC 27001, e ISO/IEC 27002.

El término de implementar un SGSI bajo la norma ISO/IEC 27001:2013 no significa contar con seguridad máxima en la información de la organización, no existe una seguridad al 100 %, porque si lo fuera se tendría que encerrar en un cuarto un Data Center con un candado y ponerlo al fondo del mar que nadie lo pueda ver ni tocar, esto sería una seguridad máxima.

Esto significa que la empresa al cubrir los requerimientos y buenas prácticas establecidas en dicha norma, permitirá establecer una mejora continua (plan, do, check y act).

La empresa brinda cursos, capacitación, certificaciones, para tener más profesionistas dentro de la empresa, con una amplia gama de vastos estudios, para poder realizar las actividades de acuerdo el puesto que se le asigne. Para para el puesto de coordinador de seguridad se requieren cursos de ISO/IEC 27001, ISO/IEC 27002, ITIL, ISO/IEC 20000.

Recomendaciones

Se recomienda implementar los controles de la norma ISO/IEC 27001:2013, la cual está conformada por 14 dominios, 35 objetivos de control y 114 controles. Se anexa la familia de ISO/IEC 27000.

Se realizan las siguientes recomendaciones:

Un programa de concientización de seguridad de la información a todo el personal que elabora en la empresa, este programa será dirigida para el personal de: Operación, Administrativos, Agentes, Analistas, Coordinadores, Gerentes, Seguridad privada, “policías”, recepcionistas.

Comunicación de las Políticas, Procedimientos, Reglamentos internos del SD; la difusión será transmitida por correo, propaganda en las puertas de las entradas, en las credenciales, en los escritorios de las pantallas de las PCS.

Cada reglamento interno, política, procedimiento, control, que se realizase se debe de firmar por el empleado.

Tener una reunión cada fin de mes con las personas involucradas a la seguridad de la información, gerencia, coordinadores de MS, coordinador de seguridad de la información, para revisar el informe de incidentes de seguridad, el avance del tratamiento de los controles, y los controles a implementar.

Contar con controles de prohibiciones de los activos, no instalación de software no autorizado, bloqueo de puertos USB, DVD.

Política de acceso de internet para todos los usuarios, que no puedan abrir paginas prohibidas, videos, redes sociales.

Política de control de claves de usuario, que se cambie la contraseña cada 90 días.

Política de correos restringidos, (No abrir correos de Hotmail, Gmail, Outlook,) al menos que sea corporativo.

Política de respaldo de información, cada 15 días solo se hará un respaldo de información más valiosa para la operación.

Hacer una política de pantallas limpias, para todos los equipos Laptop y monitor, que deben tener un bloqueo de pantalla, después de cierto tiempo que ya no se estén utilizando, y los usuarios de los sistemas deben tener un password seguro que les permita volver a activar los monitores, para que en caso de que se levanten de su lugar y su máquina se bloquee, para que no cualquier persona pueda acceder a la información que estaba siendo manejada por el usuario.

Algunas de las recomendaciones ya están implementadas, los controles ya están liberados y en ejecución, Enseguida se muestra una lista de lo que ya se realizó.

Un programa de concientización de seguridad de la información a todo el personal que elabora en la empresa, este programa se aplicó para el personal de Operación, Administrativos, Agentes, Analistas, Coordinadores, Gerentes, Seguridad privada, “policías”, recepcionistas.

Reuniones de fin de mes con las personas involucradas en la seguridad de la información (gerencia, coordinadores de MS, coordinador de seguridad de la información) para revisar el informe de incidentes de seguridad, el avance del tratamiento de los controles, y los controles a implementar.

Controles de prohibiciones de los activos, no instalación de software no autorizado, se permitirá solo la lista blanca de la herramienta de gestión (aplicación, Software, Sistema), bloqueo de puertos USB, DVD, con la ayuda de la herramienta de MACAFI “ePO”, nos ayudara a bloquear los puertos y la instalación de cualquier software.

Política de respaldo de información, cada 15 días solo se hará un respaldo de información más valiosa para la operación.

Política de pantallas limpias, para todos los equipos Laptop y monitor, que deben tener un bloqueo de pantalla, después de cierto tiempo que ya no se estén utilizando, y los usuarios de los sistemas deben tener un password seguro que les permita volver a activar los monitores, para que en caso de que se levanten de su lugar y su máquina se bloquee, para que no cualquier persona pueda acceder a la información que estaba siendo manejada por el usuario.

This is to certify that

Delfino Vazquez Garcia

Has achieved the

ITIL® Foundation Certificate
in IT Service Management

Effective from
29 February 2016

Certificate number
5455175.20509616

Candidate Number
5455175

Peter Hepworth, CEO, AXELOS

drs. Bernd W.E. Taselaar, CEO, EXIN

This certificate remains the property of the issuing Examination Institute and shall be returned immediately upon request.

Certificación ITIL

13 Glosario

A

Activo: Es todo aquel que tiene valor dentro de una organización.

Access Point: Punto de Acceso inalámbrico.

Accountable (Responsable): Rol que se encarga aprobar la actividad y asegurarse de que se realice correctamente, normalmente también se identifica como el gestor del proceso de seguridad de la información.

Avaya: El servicio de telefonía es de fundamental importancia para poder establecer el contacto con nuestros clientes y poder ofrecerles los servicios correspondientes.

ALE: Expectativa de Pérdida Anual (Annualized Loss Expectancy o ALE por sus siglas en inglés), que permite modelar el impacto que los riesgos de seguridad puede tener sobre los activos de una organización.

C

CAB: Change Advisory Board (Consejo consultor de Cambios).

CI: Configuration Item (Elemento de Configuración)

CISO: Chief Information Security Officer (Oficial de Seguridad de la Información).

Consulted (consultado): Rol que posee información para iniciar o concluir la actividad.

D

DOC: Todo tipo de documentos físicos y electrónicos, como puede ser Políticas, procedimientos, Instructivos, Manuales, Formatos de Permisos, Capacitación, contratos, Normas, Informes.

DVD: Digital Versatile Disc (Disco Versátil Digital).

F

Facilities Management: Gestión de Instalaciones, Operación de Servicios) Función responsable por gestionar el Ambiente físico en el que se ubica la Infraestructura de TI. La Gestión de instalaciones cubre todos los aspectos de la Gestión del Ambiente físico, como por ejemplo, la electricidad y la refrigeración, Gestión de Acceso a los edificios y Monitorización del ambiente.

Funciones: es un equipo o grupo de personas que realizan uno o varios procesos y actividades, las funciones crean su propio cuerpo de conocimientos a través de la experiencia que va adquiriendo.

FIS: Activos Físicos, por ejemplo: Salas de Cómputo, laboratorios, UPS, Baterías de planta de Luz, Servidores, Biométricos, Ventiladores.

I

IT (TI): Information Technology (Tecnologías de la Información).
INT: Activo Intangible como la imagen Corporativa.
INF: Activos de Información como, Registros, Contraseñas del sistema, Password, Nombre del Usuario
Informed (Informado): Rol que debe ser informado sobre el progreso y resultados de cada actividad.
ISO: Organización Internacional de Estandarización, es una federación de alcance mundial integrada por cuerpos de estandarización nacionales.
ITIL: Information Technology Infrastructure Library, (Biblioteca de Infraestructura de Tecnologías de Información) es un modelo de operación para el manejo de servicios de tecnologías de Información.
ISMS: Information Security Management System.

K

KPI's: Key Performance Indicator (Indicadores Clave de Desempeño) son utilizados para juzgar la eficiencia y la eficacia, con la reducción del porcentaje de objetivos no cumplidos.

L

Laptops: Computadora personal portátil.

M

MS: Mesa de Servicio

N

NICE: Avaya permite la grabación de forma ordenada el ingreso y salida de todas las llamadas, los usuarios, agentes, proveedores.
NOC: Network Operation Center, usados para monitorear redes.

P

PC: Computadora personal de escritorio.
PDCA: Acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).
PER: También es un activo Personas que entregan el servicio, Agentes, Soporte en sitio, Coordinadores e/y Supervisores, Gerentes, Analistas, Gerente de la Unidad de Negocio.
Planta de Energía: Sistema de emergencia la luz comercial.

R

Responsable (Encargado): Rol que realiza la actividad y es responsable por su ejecución, si vemos del lado de la mesa de servicio el encargado seria el coordinador de seguridad de la información que está dando seguimiento al riesgo.
Rollback: Quiere decir que regresa al estado anterior como estaba antes.
Roles: un grupo de responsabilidades, actividades, que son asignadas a un proceso y esto puede ser asignado a una persona o equipo.
RFC: Request for Change “formato de solicitud cambio”.

S

SD: Service Desk.
SGSI: Sistema de Gestión de seguridad de la Información.
SER: Activos asociados a servicios por ejemplo, suministradores, proveedores.
SOF: Todo el Software está dentro del activo como, Sistemas operativos, Aplicaciones, Antivirus, Fortinet, Avaya, Moebius, Remedy, telefonía Cisco, WebEx.
SOC: Security Operation Center, se utiliza para monitorio de seguridad Física.

T

TT: Ticket.
TIC: Tecnologías de la Información y Comunicaciones.

U

UUNN: Unidad de Negocio.
USB: Universal Serial Bus.
UPS: Unidad de Almacenamiento Ininterrumpida.

V

Vo.Bo: Visto Bueno.

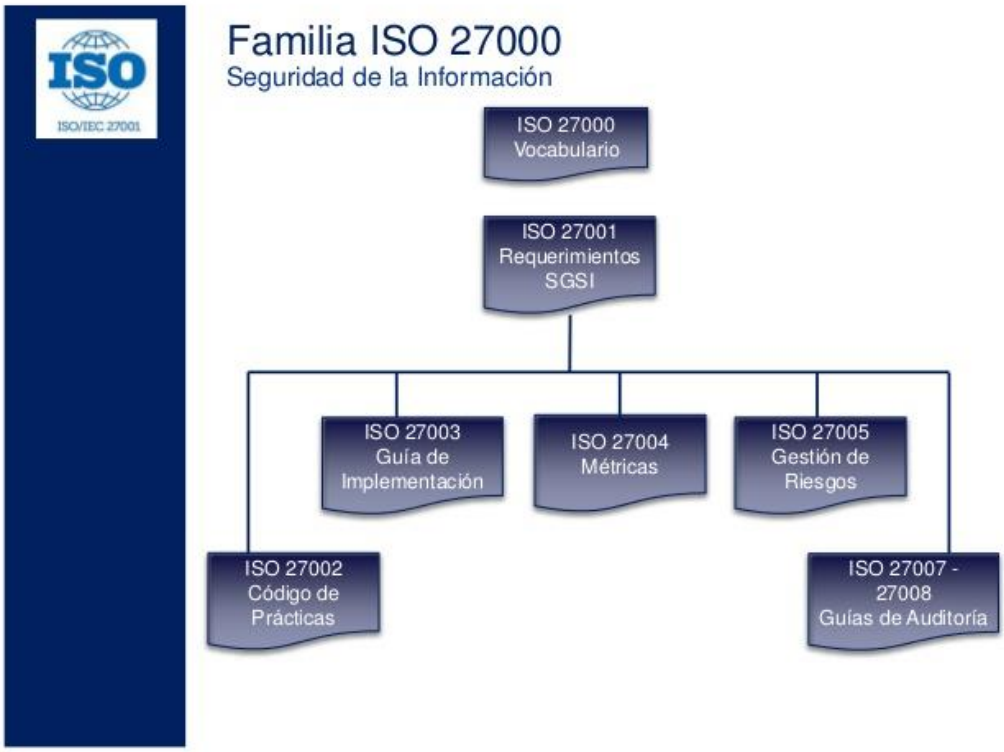
14 Anexos

Normas de la Familia ISO 27000.

- ISO 27000 – vocabulario estándar para el SGSI.
- ISO 27001 – especifica los requisitos para la implantación del SGSI.
- ISO 27002 – código de buenas prácticas para la gestión de seguridad de la información.
- ISO 27003 – directrices para la implementación del SGSI.
- ISO 27004 – métricas para la gestión de seguridad de la información.
- ISO 27005 – gestión de riesgos en seguridad de la información.
- ISO 27006 – requisitos para acreditación de organizaciones que proporcionan certificación de SGSI.
- ISO 27007 – Es una guía para auditar al SGSI.
- ISO 27799 – Es una guía para implementar ISO 27002 en la industria de la salud.
- ISO 27035 – actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

https://lciso27000.wordpress.com/category/familia-iso-27000/

http://www.iso27000.es/iso27000.html



http://image.slidesharecdn.com/presentaciniso27001-141222161812-conversion-gate02/95/presentacin-iso-27001-3-638.jpg?cb=1419286720

15 Bibliografía

Andres, J. (17 de 01 de 2015). *Fundamentos de Seguridad Informática*. Obtenido de http://fundamentos-informaticos-introduccion.blogspot.mx/2015/01/fundamentos-de-seguridad-informatica.html.

COPYRIGHT, I. (30 de 08 de 2005). *ISO/IEC FDIS 27001.* Obtenido de ISO/IEC FDIS 27001: http://securitycn.com/img/uploadimg/20070924/183844756.pdf

Excellence, I. (04 de 06 de 2015). *ISO 27001: Ciclo de Deming*. Recuperado el 01 de 03 de 2016, de ISO 27001: Ciclo de Deming: http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/

Falcón, J. A. (Junio 2006). Firewall. La seguridad de la Banda Ancha. En J. A. Falcón, *La seguridad de la Banda Ancha.* Mexico: Alfaomega Grupo RA-MA.

final draft ISO/IEC FDIS 27001:2005. (Voting begins on: 2005, 06 30). *Technologies de l'information ó Techniques de sÈcuritÈ ó SystËmes*. Retrieved 03 01, 2016, from Technologies de l'information ó Techniques de sÈcuritÈ ó SystËmes: http://securitycn.com/img/uploadimg/20070924/183844756.pdf

fine, L. H. (2009). Seguridad en Centros de Computo . En L. H. Fine, *Seguridad en Centros de Computo Politicas y Procedimientos.* 2da Edicion Mexico: Trillas, S.A de C.V.

Fuente. (s.f.). *http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html*.

Fuente. (s.f.). *http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#01*.

Gil, P. C. (1996). Seguridad Informatica Técnicas Criptograficas. En P. C. Gil, *Seguridad Informatica Técnicas Criptograficas.* Mexico: Alfaomega Grupo Editor, S.A de C.V.

http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#01. (s.f.).

http://www.iso.org/iso/catalogue_detail?csnumber=43170. (s.f.).

http://www.iso27000.es/download/doc_sgsi_all.pdf. (s.f.).

INTERNATIONAL. (15 de 11 de 2009). *ISO copyright office.* Recuperado el 20 de febrero de 2016, de Risk management — Principles and: www.iso.org

Juan Jiménez, L. A. (11 de Julio de 2007). *ITIL® V3 Glosario v01.* Obtenido de ITIL® V3 Glosario v01: http://www.get-best-practice.co.uk/glossaries.aspx

Jule Hintzbergen,Kees Hintzbergen,André Smulders,Hans Baars. (Mayo 2010). *Fundations of Information Security* (Second edition, first impression, May 2010 ed.). (S. Newton, Ed.) Steve Newton.

Kenneth, E. K. (1997). *Análisis y diseño de sistemas.* Mexico: Pearson Educacción.

Martín, A. B. (s.f.). *Plan de Implementación de la* . Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/54243/1/AdrianBelmonteMartin_TFM.pdf.

Mendoza, M. Á. (01 de 07 de 2014). *Welivesecurity*. Recuperado el 30 de 09 de 2016, de Welivesecurity: http://www.welivesecurity.com/la-es/2014/07/01/calculando-perdidas-monetarias-riesgos-seguridad/

Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas. (10 de 2012). *PAe portal administracion electronica*, 3. Recuperado el 01 de 04 de 2016, de PAe portal administracion electronica:

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?comentarioContenido=0#.VyLiNEe2bIU

Montes, G. A. (Marzo 2002). Reingeniería de la Auditoría Informática. En G. A. Montes, *REINGENIERÍA de la AUDITORÍA INFORMÁTICA* (pág. 384). Mexico: Trillas, S. A. de C. V.

Seguridad, S. d. (s.f.). *http://www.significados.com/seguridad/*.

Tim Malone (Author), I. M. (2009, FEBRUARY 18). *AMAZON*. Retrieved AGOSTO 27, 2015, from ITIL V3 Foundation Complete Certification Kit - 2009: http://www.amazon.com/ITIL-Foundation-Complete-Certification-Kit/dp/1921573600