Implementando la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 en una Entidad del Estado

Implementing the Peruvian Technical Standard NTP-ISO / IEC 27001: 2014 In an Entity State

Santiago Domingo Moquillaza Henriquez[1], Flavio Nireo Carrillo Gomero[2]

Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú
Facultad de Ingeniería Electrónica y Eléctrica, Universidad Nacional Mayor de San Marcos, Lima, Perú

***Resumen*— Este artículo fue desarrollado para ofrecer una forma estructurada y sencilla de qué y cómo abordar la implantación de un Sistema de Seguridad de la Información (SGSI), en todos sus niveles, estando este diseño de implementación basado en la norma NTP-ISO/IEC 27001:2014. Un SGSI es el marco para garantizar la seguridad de la información, en función del tratamiento de unos niveles de riesgo obtenidos como consecuencia de considerar todos los posibles efectos que pueden ocurrir a causa de las vulnerabilidades de los activos que poseen información valiosa de la entidad y que podrían ser atacadas en función a las amenazas existentes.**

***Abstract*— The article was developed to provide a simple structure form and how to address the implementation of a System of Information Security (ISMS) in all levels, being this design implementation based on the ISO / IEC 27001: 2014. An ISMS is a framework to ensure information security, according to the treatment of risk levels obtained as a result of considering all possible effects that may occur because of the assets vulnerabilities that have valuable information of entity and that could be attacked according to existing threats.**

Palabras Claves - SGSI, NTP-ISO/IEC 27001:2014, seguridad de la información

Key Words – ISMS, NTP-ISO/IEC 27001:2014, information security.

I. INTRODUCCIÓN

Actualmente los Sistemas de Gestión y de Información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de información en general requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de los activos de sus clientes, la disminución de sus costos y el incremento de sus utilidades.

La finalidad en la entidad del estado, es la de evaluar los riesgos que enfrenta la organización, identificar las amenazas de los activos, evaluar las vulnerabilidades y probabilidades de ocurrencia, además de estimar el impacto potencia en la organización.

Por tal razón, debemos tener en cuenta los requisitos legales, normativos, reglamentarios y contractuales que deben de cumplir la organización, sus socios comerciales, sus contratistas, los prestadores de servicios.

Por ende, la seguridad de la información consiste en combinar coherentemente las herramientas técnicas' de la seguridad y a la vez gestionar el comportamiento del Factor Humano tratando de reducir en la mayor medida posible las vulnerabilidades o posibles atentados contra la seguridad de la información y sistemas.

II. FUNDAMENTACIÓN TEÓRICA

A. ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada,

[1]Santiago D. Moquillaza Henríquez, E-mail: smoquillazah@unmsm.edu.pe
[2]Flavio N. Carrillo Gomero, E-mail: fcarrillog@unmsm.edu.pe
Recibido: Abril 2016 / Aceptado: Junio 2016.

enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración [1].

B. Norma Técnica Peruana NTP-ISO/IEC 27001:2014

Esta norma técnica ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener, y mejorar un Sistema de Gestión de Seguridad [2].

C. *Principios Básicos de la Seguridad de la Información.*

Para asegurar y garantizar la seguridad de la información, esta debe de cumplir con los siguientes principios básicos:

- **Confidencialidad:** es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
- **Integridad:** es la propiedad de mantener la información libre de modificaciones no autorizadas.
- **Disponibilidad:** cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones [3].

D. Necesidad de la Seguridad de la Información

Para toda organización, su información constituye uno de los activos más importantes y de mayor valor. La adecuada administración de la misma al interior de la organización, puede mejorar su desempeño la cual impacta en la calidad del servicio con nuestros clientes externos e internos. Por ello todos los elementos de la organización deben estar involucrados, con una cultura proactiva.

E. Vulnerabilidad

Según la norma [ISO/IEC 13335-1:2004] [4], es la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. La vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptibles a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas, porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Las Vulnerabilidades a las cuales los activos están expuestos pueden ser las siguientes:

- **Vulnerabilidad Física**: Son aquellos presentes en los ambientes en los cuales la información se está almacenando o manejando.
- **Vulnerabilidad Natural**: Son aquellas relacionadas con las condiciones de la naturaleza que puedan colocar en riesgo la información.
- **Vulnerabilidad de Hardware**: Los posibles defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos.
- **Vulnerabilidad de Software**: Los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red.
- **Vulnerabilidad de medios de almacenaje**: Los medios de almacenamiento son los soportes físicos o magnéticos que se utilizan para almacenar la información.
- **Vulnerabilidad de Comunicación**: Éste tipo de punto débil abarca todo el tránsito de la información.
- **Vulnerabilidad de Humana**: Esta categoría de vulnerabilidad está relacionada con los daños que las personas puedan causar a la información y al ambiente tecnológico que la soporta.

F. Amenazas

Según **ISO/IEC 13335-1:2004** [5] una amenaza es la causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o la organización.

La amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), sobre los elementos de un sistema.

Son agentes capaces de explotar los fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa, afectando a sus negocios.

Generalmente las amenazas se distinguen y dividen en tres grupos:

- **Amenaza Naturales**: Son sucesos de origen físico, condiciones de la naturaleza y la intemperie que podría causar daños a los activos, tales como fuego, inundación, terremotos, sobrecarga eléctrica, falta de energía eléctrica.
- **Amenazas Intencionales**: Son todas las acciones, causadas por la intervención humana, que violan la ley y que están penadas por estas, tales como los fraudes, vandalismo, sabotajes, espionajes, invasiones y ataques, robos y hurtos de información, entre otros.
- **Amenazas por negligencia y decisiones institucionales**: Son todas las acciones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas

menos predecibles porque están directamente relacionado con el comportamiento humano, tales como la falta de reglas, falta de capacitación, no cifrar datos críticos, mal manejo de contraseñas.

Pero también existen otras amenazas que son muy alarmantes y que se debe tener en consideración, como la falta de respaldo de datos, la perdida de la información por rotación, salida del personal, por abuso de conocimientos internos, y mal manejo de equipos y programas.

G. Amenazas por Internet

En el lenguaje informático, se denomina "amenaza" a la violación de la seguridad (confiabilidad, integridad, disponibilidad o uso legítimo), que podría efectuar una persona, maquina, suceso o idea, dada una oportunidad. Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son los siguientes:

- **Interrupción**: Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente. Por ejemplo, destruir un disco duro, cortar una línea de comunicación o deshabilitar un sistema de consulta.
- **Intercepción**: Este es un ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podrá ser una persona, un programa o una computadora. Ejemplos de este tipo de ataque son interceptar una línea para obtener información y copiar ilegalmente archivos o programas que circulan por la red.
- **Modificación**: Este es un ataque de una entidad no autorizada que consigue acceder a un recurso y es capaz de modificarlo. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación**: Este es un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema. Ejemplos de este ataque son insertar mensajes no deseados en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos

H. Política de Seguridad de la información

Una política de seguridad de la información es un conjunto de reglas o normas aplicadas a todas las actividades relacionadas al manejo de la información. Dentro de estas normas, son importantes las siguientes:

- **Revisión y actualización:** Anualmente o cuando la magnitud de los cambios lo justifiquen, se generará una nueva versión.

Como parte del proceso de mejora continua, semestralmente se procede a la revisión de la Política de Seguridad de la Información, a fin de reflejar los cambios producidos durante dicho periodo.

- **Publicación y distribución:** La política de Seguridad de la Información debe de ser comunicada a todos los usuarios de la entidad del estado, siendo de conocimiento y aplicación obligatorio para todo el personal de la entidad.
- **Capacitación:** La entidad del estado debe buscar de forma adecuada la formación y sensibilización del personal, contratistas y terceros involucrados respectos a la seguridad de la información para garantizar el cumplimiento de las normativas legales aplicables.
- **Violaciones a la política de seguridad:** Todo aquello que ocasione cualquier riesgo o pérdida para la organización pueden resultar en acción disciplinaria por parte de la organización cuya magnitud dependerá del tipo y severidad de la violación.
- **Gestión de seguridad de la información:** La Gestión del Riesgo de Seguridad es la coordinación de las actividades para dirigir y controlar una organización en torno al riesgo de seguridad, según ISO/Guide 73:2009, [6].
- **Plan estratégico:** La entidad del estado, sigue las normas en el cumplimiento y adaptación a la legislación vigente según la Resolución Nº 129-2014/DNB-INDECOPI [7]. (NTP-ISO/IEC 27001:2014), decidió implementar el Sistema de Gestión de Seguridad de la Información para estar a la altura de otras entidades y empresas y ser uno de los mejores en cuanto al control de riesgos e incidencias, pero relacionado con su plan estratégico.
- **Estrategias de seguridad:** Las políticas y los procedimientos de seguridad de los sistemas de información surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la organización.
- Un plan de seguridad en una organización debe estar soportado por políticas y procedimientos que definan ¿por qué proteger un recurso?, ¿qué debe hacer la organización para protegerlo?, y ¿cómo debe procederse para poder lograrlo? Para lograr esto es importante tener conocimiento de las vulnerabilidades y formas de ataque de los sistemas con que cuenta la organización.

Algunas de las herramientas usadas por los atacantes se describen a continuación:

- **Sniffers:** Son programas que se dejan ocultos en los servidores para que espíen las conexiones y se puedan detectar los logins, passwords y demás información.
- **Programas de ocultamiento (ZAPPERS):** Son programas que borran las huellas de los ataques que se han hecho en los sistemas.
- **Crakeadores**: Herramientas que permiten averiguar las claves de un sistema, aunque estén encriptados.

Una de las herramientas más utilizadas en la prevención de ataques externos por parte de los intrusos de Internet (Hackers) es el Firewall que ofrece seguridad de protección contra intrusos determinando que servicios de la red pueden ser accesado y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no autorizados y en caso de un ataque genera alarmas de seguridad.

Los Firewalls son una puerta de acceso entre el Internet y la red Interna, también pueden ser puertas de acceso entre diferentes subdivisiones de una red. Esta aplicación determina que paquete puede pasar y cual no. Puede operar a nivel de aplicación o sobre las capas de red o transporte.

- **Ingeniería Social:** Que **e**s la práctica de obtener información confidencial a través de la manipulación de usuarios que pertenecen al entorno de red para conseguir acceso a esa red desde el exterior [8]. La principal defensa contra la ingeniería social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas.

III. MÉTODO DE IMPLEMENTACIÓN

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

- *Plan* (planificar): establecer el SGSI.
- *Do* (hacer): implementar y utilizar el SGSI.
- *Check* (verificar): monitorizar y revisar el SGSI.
- *Act* (actuar): mantener y mejorar el SGSI.

La cual exige tener personas, procesos, tecnología, políticas, roles, normas, procedimientos bien establecidos o preparados. En la Fig. 1, se muestra en forma gráfica la secuencia de cada una de estas acciones para la gestión de riesgos.

A. Programación del Proyecto con personal de la Entidad

Este proceso permite que la alta dirección o gerencia de la entidad, sensibilice entender la importancia del proyecto del desarrollo e implementación del Sistema de Gestión de Seguridad de la Información y la necesidad del apoyo del recurso humano, factor clave para el inicio de la fase de levantamiento de información.

Fuente: https://docs.google.com/viewer

Fig. 1. Ciclo PDCA para la gestión de riesgos

Definir el alcance

Por la complejidad de la implementación de la norma, se recomienda a la entidad definir de manera sistemática el alcance del proyecto, en las áreas de Control de Activos y Seguridad de Recursos Humanos.

Control de activos: Para este punto se sugirió realizar un inventario de activos, para tener un control más riguroso de los mismos. Toda la información y activos asociados a los recursos para el tratamiento de la información, deberían tener un propietario y pertenecer a una parte designada de la entidad.

Para realizar un análisis de riesgo se parte del inventario de activos. Para determinar cuál era la situación actual de la entidad, se realiza un análisis de Gap.

El resultado de este análisis en la entidad del estado establece la diferencia entre el desempeño actual y el esperado, con un informe presentado con indicaciones sobre dónde están las deficiencias y "qué" falta para cumplir con cada requisito de la norma.

- **Análisis de Vulnerabilidades a nivel de acceso lógico:** La seguridad lógica concentra sus objetivos en la aplicación de procedimientos que resguarden el acceso a los datos y permisos a las personas autorizadas.

Los procesos de esta capitulo se desarrollan en el siguiente orden:

- Realizar un análisis de brechas con el fin de definir la declaración de aplicabilidad.
- Definir políticas y procedimientos aplicados al cumplimiento de la norma técnica peruana **NTP-ISO/IEC 27001:2014.**

- Entregar los resultados definidos del análisis de riesgos, declaración de aplicabilidad, políticas y procedimientos.
- Iniciar un proceso de análisis de riesgos, abarcando los procesos de valorización de activos, identificación de amenazas y vulnerabilidades, determinación de probabilidad de ocurrencia de una amenaza y valoración de riesgo.

- **Seguridad de los recursos humanos:** Tiene como objetivo asegurar que los empleados, contratistas y usuarios de terceras partes, entiendan sus responsabilidades y son aptos para ejercer las funciones para las cuales están siendo consideradas, con el fin de reducir el riesgo de hurto de la información, fraude o uso inadecuado de las instalaciones de la entidad. Para el análisis de control de activos y de la seguridad de los recursos humanos, se debería trabajar con la metodología MAGERIT, que es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Ver Fig.2.

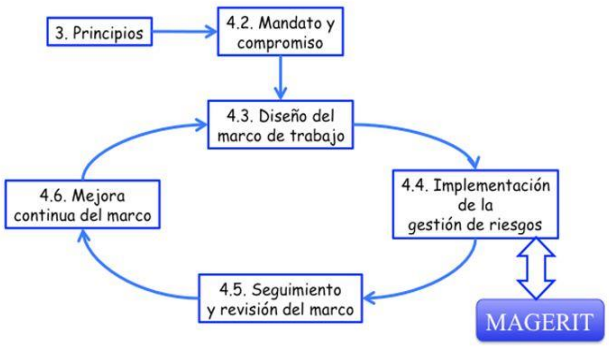

Fig. 2. ISO 31000-Marco de trabajo para la gestión de riesgos.

El análisis y gestión de los riesgos es un aspecto clave, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

Persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso [9].

B. Gestión y tratamiento de los riesgos

La gestión de los riesgos es el proceso por el cual se controlan, minimizan o se gestionan ya que un riesgo no se elimina. Los riesgos que afectan a los activos de la organización de la entidad, en este caso las medidas adecuadas para hacer frente a las mismas, se dispuso de varias alternativas para afrontar los riesgos: eliminar, transferir, asumir o mitigar el riesgo.

Todas las medidas implantadas se documentarán para permitir la gestión por parte de la organización. Una vez decididas las medidas que se aplicaran a los riesgos indicados, el cual expondrá el registro residual (es el nivel de riesgo aceptable por la organización bajo el cual estarán todos los riesgos de la misma).

Se han definido dos tipos de controles que se complementan: técnicos y organizativos.

Los controles técnicos tienen que quedar perfectamente documentados a través de procedimientos.

Los controles organizativos, pueden quedar documentados a través de procedimientos o políticas de seguridad.

C. Soporte metodológico y técnico

- **Manual de seguridad del SGI,** el cual queda dividido en 2 partes:
  - Política de seguridad. Declaración de alto nivel de objetivos, directrices y compromiso de la Administración General para acometer la gestión de seguridad de la información en los medios electrónicos, informáticos y telemáticos que se utiliza en la prestación de servicios públicos.
  - Normativa de seguridad. Medidas de seguridad de obligado cumplimiento. Es un compendio del conjunto de normas que soportan los objetivos recogidos en la política de seguridad de la información. En este nivel se describen los objetivos de seguridad y se anticipan las reglas generales de obligada adopción. Este apartado es el objetivo final perseguido por este documento [10].
- **Soporte de software,** aquí debe contar con software de apoyo para todo el proceso anteriormente descrito que cubra el proceso automático de implantación del Sistema de Gestión de Seguridad de la Información (SGSI) de manera que nos pueda los indicadores para realizar la mejora continua del Sistema.

IV. RESULTADOS ESPERADOS

A. Políticas de control de la información y de comunicación de seguridad

- Definición de roles y propuestas de asignación, estructura organizativa, políticas de control, planificación de actividades, responsabilidades, prácticas, procesos y recursos.
- Propuesta de alineación tecnológica frente a los procesos estratégicos de la organización.
- Entrega de un sistema de información para una mayor seguridad integral.
- Propuesta de un plan de continuidad del negocio permitiendo que la empresa u organización pueda recuperarse después de algún incidente que pudiese presentarse.
- Capacitación y concientización al Departamento de Sistemas sobre el impacto favorable que tendría el establecimiento de una política en ISO 27001.Entrega y socialización de anexos donde se describen riesgos de inventarios de servidores y estaciones de trabajo, declaraciones de aplicabilidad y la respectiva matriz de riesgos, calificando sus probabilidades y el impacto que este puede causar.
- Adicionalmente, se debe tener procedimientos de gestión de contraseñas, gestión de usuarios, políticas y establecimientos de gestión de monitoreo para la red, como para los enlaces dedicados con el proveedor de servicios de telecomunicaciones, políticas de control de acceso físico y lógico, recursos humanos, controles criptográficos y gestión de redes.

B. Prevención para la gestión de la continuidad del negocio.

Estos son algunos de los ejemplos que hemos encontrado en la prensa sobre los riesgos en materia de seguridad de la información y por ende que afectan a la continuidad del negocio

- Las fallas eléctricas causan el 90% de los incendios. Los problemas más comunes por los que se produce este tipo de siniestros son: la utilización de materiales no adecuados, un cálculo erróneo del sistema o contratar electricistas sin formación técnica.

- El 43% de las empresas privadas y públicas que sufren un desastre, sin contar con un Plan de Continuidad del Negocio, no se recuperan.

- El 51% sobrevive, pero tarda un promedio de dos años en reinsertarse en el mercado y solo el 6% mantiene su negocio a largo plazo.

- El 30% de las copias de seguridad y el 50% de las restauraciones fallan, según un informe de Enterprise Strategy Group. Durante este estudio muchos departamentos de Tecnología de la Información reconocían no estar seguros de ser capaces de recuperar los datos críticos del negocio y si podrían hacerlo en un tiempo razonable.[11]

- Para evitar estas y otras situaciones es necesario disponer de un Plan de Continuidad del Negocio. Este plan es la respuesta prevista por la empresa ante aquellas situaciones de riesgo que le pueden afectan de forma crítica.

En la Fig.2, se muestra los elementos a controlar que involucra desde el cumplimiento hasta las políticas de seguridad.

fuente: https://www.google.com.pe/search?q=SGSI+IMAGENES

Fig. 2. Elementos a controlar.

C. Proceso de certificación.

Al finalizar la implantación del Sistema de Gestión de Seguridad de la Información tenemos la opción de certificarlo, es decir, obtener un documento a través de un tercero de confianza que verifica su correcta implantación.

Con ello certificamos la gestión del sistema, pero no las medidas implantadas o la seguridad de la empresa. Lo que certifica es que la empresa gestiona adecuadamente la seguridad.

Para poder certificarlo, nuestro Sistema de Gestión de Seguridad de la información tiene que estar basado en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, Además, debe estar implantado y funcionando y tienen que existir evidencias que lo demuestren, en los registros de no conformidades, que mantiene el área.

V. RESUMEN DE UN CASO PRÁCTICO

Este caso práctico corresponde al ejecutado en la Facultad de Sistemas e Informática de la UNMSM sobre los riesgos en el Datacenter que se muestra a continuación mediante un inventario de activos expuestos a amenazas:

- Riesgos por amenazas de virus, troyanos, malware. *Probabilidad-de-Amenaza*Magnitud-de-daño*=0.27*1 = 0.27.

Administrando el Riesgo: Proxy bajo Sistema Operativo Open Source, con las reglas definidas,

antivirus con sus agentes respectivos, antimalware.

- Riesgos por integridad de la información por amenazas eléctricas las 24 horas.

*Probabilidad-de-Amenaza*Magnitud-de-daño*=0.1*1 = 0.1.

Administrando el riesgo: Backups respectivos, UPS, Pozos a tierra, claves seguras, servidor alternativo en caso de falla de disco, conexiones y tableros eléctricos.

- Riesgos por disponibilidad de la Información e integridad.

*Probabilidad-de-Amenaza*Conectividad*=0.03*1= 0.03.

Administrando el Riesgo: Implementando redes particulares Vlans, para aislar los problemas que pudiera haber en la red, gestión de claves y perfiles.

- Riesgos por confidencialidad:

Probabilidad de Amenaza por claves x Magnitud de daño=0.01*3=0,03

Administrando el riesgo: Coordinación con el usuario, Coordinaciones con el jefe de personal y usuarios cuando se da el proceso de rotaciones de personal, Administración de las claves, log de transacciones de auditoría, evaluación de discreción del sysadmin y dba.

Las probabilidades de amenaza son estimadas de incidencias del año anterior en base a 360 días del año, y la magnitud de daño se ha dado en base a una escala histórica de impactos ocurridos, se ha tomado del 1 al 4. Todas estas precauciones están recursivamente gestionadas en el ciclo PDCA de Deming.

VI. CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- Producto del SGSI, se dispone de la confiabilidad, integridad y disponibilidad.
- Se tiene identificados riesgos y los impactos asociados a desastres probables.
- Se tiene una cultura de prevención.
- Las vulnerabilidades siempre van estar latentes
- La seguridad está ligada a la continuidad del negocio

Recomendaciones:

- Hay que siempre estar al tanto de las normas a fin de adecuar a las modificaciones o adendas que puedan darse.
- Periódicamente hay que revisar los activos nuevos y existentes y observar el riesgo que lo rodea y el impacto en todo el Sistema.
- Constantemente hay que ver las estrategias con los usuarios de la empresa para inculcar la seguridad.
- La gente técnica de Sistemas o Informática tienen que estar atentos a los nuevos que causan destrozos tales como virus, gusanos, hacking, Cracking y manejar la discreción lo cual es clave para evitar la ingeniería Social.
- La seguridad también nos debe servir para realizar un plan de continuidad de negocio

REFERENCIAS

[1] Portal ISO 2700 en español. ``*Sistema de Gestión de la Seguridad de la Información´´*. http://www.iso27000.es/download/doc_sgsi_all.pdf

accesado: el 2 de mayo del 2016

[2] INDECOPY. ``*Norma Técnica Peruana NTP-ISO/IEC 27001:2014´´*.2014. https://canvas.utp.edu.pe/courses/8870/files/42244/download?download_frd=1

[3] M. Fernández. "*Concepto de Seguridad*". Universidad de Cadiz. 2014. http://www.mfbarcell.es/redes_de_datos/tema_14/redes_t14_seguridad1_conceptos.pdf

[4] IS/ISO/IEC 1335-1. "*Management of Information and Communications Technology Security, Part 1: Concepts and Models for Information and Communications Technology Security*". Bureau of Indian Standards. New Delhi. 2009. https://archive.org/stream/gov.in.is.iso.iec.13335.1.2004#page/n3/mode/2up

[5] IS/ISO/IEC-1335-1. "*Information technology-Security techniques-Management of information and communications technology security, Part 1: Concepts and models for Information and communications technology Security management* ". International Standard. First Edition, Switzerland. 2004.

[6] ISO. " ISO/Guide 73:2009". https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

[7] El Peruano. "*Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática*". Resolución Ministerial N°004-2016-PCM. http://busquedas.elperuano.com.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

[8] M. Meyers. "*Redes, Administración y Mantenimiento*". Ediciones Anaya Multimedia, pp 628. España. 2010.

[9] A. F. Diaz, G. I. Collazos, H. Cortez, L. J. Ortiz, y G. A. Herazo. "*Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad de nuestra señora de Gracia, alineado tecnológicamente con la norma ISO 27001*". Fundación Universitaria Konrad Lorenz. 2012.

http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

[10] Gobierno Vasco. "*Manual de Seguridad: Aplicaciones de Tramitación Telemática*". Dirección de Informática y Telecomunicaciones del Departamento de Justicia y Administración Pública. 2010.

http://www.euskadi.eus/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

[11] INTECO. "SGSI: Implantación de un SGSI en la empresa". Instituto Nacional de Tecnologías de la Comunicación. España. 2013.

http://pt.slideshare.net/kramerg/guia-apoyo-sgsi