Polo del Conocimiento

Pol. Con. (Edición núm. 35) Vol. 4, No 7
Julio 2019, pp. 174-195
ISSN: 2550 - 682X
DOI: 10.23857/pc.v4i7.1029

Recepción: 11 / 05 / 2019
Aceptación: 18 / 06 / 2019
Publicación: 05 / 07 / 2019

Ciencias de la computación y telecomunicaciones

Artículo de investigación

Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel

Risk and vulnerabilities analysis of the data network, in an ISP, using the standard ISO/IEC 2007:2008. Case study: Sistelcel enterprise

Análise de risco e vulnerabilidade da rede de dados, em um ISP, utilizando a norma ISO / IEC 2007: 2008. Estudo de caso: Sistelcel Company

Jackeline Elizabeth Ortiz-Lazo [I]
jeortizl@psg.ucacue.edu.ec

Jenny Karina Vizñay-Duran [II]
jviznay@ucacue.edu.ec

Correspondencia: jeortizl@psg.ucacue.edu.ec

I. Ingeniera en Sistemas, Estudiante, Tecnólogo Analista de Sistemas, Jefatura de Posgrados. Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Magíster en Evaluación y Auditoria de Sistemas Tecnológicos, Ingeniera en Sistemas, Sub Decana de la Unidad Académica de Tecnologías de la Información, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

En este trabajo de investigación se refiere a la presentación de un análisis de riesgos y vulnerabilidades de la información, utilizando la norma ISO 27005:2008 en donde nos permite identificar, analizar, evaluar los diferentes tipos de riesgo que se tiene en una organización, permitiendo establecer controles o salvaguardias con la finalidad de mitigar el riesgo.

Se efectuó un análisis analítico de la situación actual de la empresa, para determinar el estado real de la seguridad de la información, aplicando la norma ISO 27001, obteniendo como resultados la carencia de procesos y normas para su cumplimiento y ejecución.

Para que estos procesos se lleven a cabo se enumeraron todos los activos de la organización que fueron identificados mediante una metodología de buenas prácticas en normas y estándares (Magerit), que serán considerados para la valoración del activo (hardware, software, personas y datos), valoración del impacto e identificación de las vulnerabilidades.

Mediante el análisis de los riegos informáticos que se presenta en la organización, se aplicó una matriz de riesgo consiguiendo el Riesgo Inherente el cual dio una radiografía de la situación actual de la organización y posteriormente se propuso controles y se obtuvo el riesgo residual.

Los resultados de este trabajo aportan a la alta gerencia en la toma de decisiones, para el tratamiento del riesgo mediante normas, estándares y buenas practicas, sin afectar la información de la empresa y tener continuidad en el negocio y alcanzar los objetivos planteados por la organización.

Palabras clave: ISP; ISO 27005:2013; Magerit; riesgo; vulnerabilidades; impacto; amenaza.

Abstract

In this research work it refers to the presentation of an analysis of risks and vulnerabilities of information, using the ISO 27005: 2008 standard where it allows us to identify, analyze, evaluate the different types of risk that an organization has, allowing establish controls or safeguards in order to mitigate risk.

An analytical analysis of the current situation of the company was carried out, to determine the real state of information security, applying ISO 27001, obtaining as a result the lack of processes and standards for compliance and execution.

For these processes to be carried out, all the assets of the organization that were identified through a methodology of good practices in standards and standards (Magerit), which will be considered for the valuation of the asset (hardware, software, people and data) were listed , impact assessment and identification of vulnerabilities.

By analyzing the computer risks presented in the organization, a risk matrix was applied, obtaining the inherent risk which gave an x-ray of the current situation of the organization and subsequently proposed controls and obtained the residual risk.

The results of this work contribute to senior management in decision-making, for the treatment of risk through standards, standards and good practices, without affecting the company's information and having continuity in the business and achieving the objectives set by the organization .

Keywords: ISP; ISO 27005: 2013; Magerit; risk; vulnerabilities; impact; threat.

Resumo

Neste trabalho de pesquisa refere-se à apresentação de uma análise de riscos e vulnerabilidades de informação, utilizando a norma ISO 27005: 2008 onde nos permite identificar, analisar, avaliar os diferentes tipos de risco que uma organização possui, permitindo estabelecer controles ou salvaguardas para mitigar o risco.

Foi realizada uma análise analítica da situação atual da empresa, para determinar o estado real da segurança da informação, aplicando a ISO 27001, obtendo como resultado a falta de processos e padrões de conformidade e execução.

Para que esses processos sejam realizados, todos os ativos da organização que foram identificados através de uma metodologia de boas práticas em padrões e padrões (Magerit), que serão considerados para a avaliação do ativo (hardware, software, pessoas e dados) foram listados , avaliação de impacto e identificação de vulnerabilidades.

Ao analisar os riscos computacionais apresentados na organização, foi aplicada uma matriz de riscos, obtendo-se o risco inerente que deu um raio-x da situação atual da organização e, posteriormente, propôs controles e obteve o risco residual.

Os resultados deste trabalho contribuem para a gestão sênior na tomada de decisão, para o tratamento de riscos através de padrões, normas e boas práticas, sem afetar as informações da empresa e ter continuidade nos negócios e atingir os objetivos estabelecidos pela organização. .

Palavras chaves: ISP; ISO 27005: 2013; Magerit; risco; vulnerabilidades; impacto; ameaça.

Introducción

La globalización, hoy en día, ha verificado que existe un crecimiento en la comunicación, entre varios países del mundo, estableciendo su comercio, ideologías y compartiendo culturas. A través de estos convenios, las organizaciones se encuentran susceptibles en su información por factores externos de su entorno.

Las organizaciones están vulnerables a la infiltración de su información, afectando su productividad, debiendo confrontar las exigencias de nuevas capacidades, permitiendo crear nuevas oportunidades viables para el negocio.

Las causas principales que originan estos incidentes son: hacking, malware, fallos en software, acceso no autorizados a sistemas, fallas en la red causando la no disponibilidad de los servicios de la información, etc.

El objetivo de los cibercriminales es diagnosticar el valor de los activos de la información de datos de una organización, por lo que se deben estructurar y establecer procedimientos a sus esquemas de protección y análisis de riesgos.

A nivel de la red interna del ISP (Internet Service Provider), se tienden a ser más vulnerables a los ataques mediante el uso del internet, causando la pérdida de información que poseen.

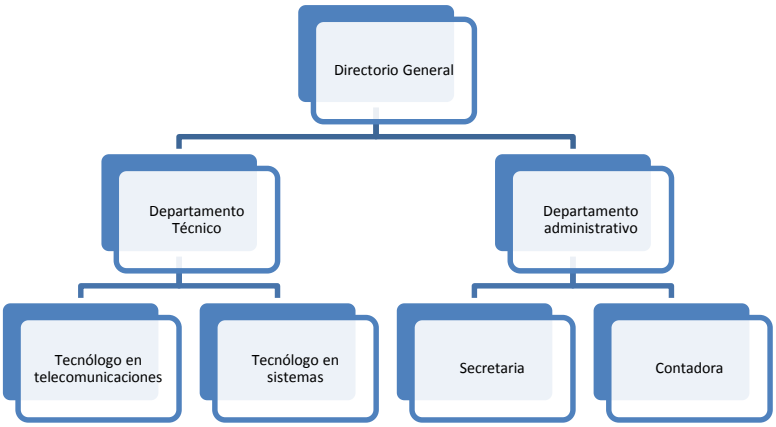
En la tercera edición del estudio Radar de Riesgo Tecnológico, publicado por KPMG, se identifican las tendencias en los riesgos relacionados a TI, basado en incidentes sucedidos durante el último año a nivel global, y, los agrupa en tres categorías: Seguridad (54.3%), Disponibilidad (36.2%) y Calidad de TI (9.5%). [1]

La empresa Sistelcel inicio sus actividades en el año 2009, en la ciudad de Cuenca, a cargo del Ing. Pablo Barreto, ofreciendo servicio de internet banda ancha, mediante fibra óptica, sin necesidad de línea telefónica.

El objetivo de desarrollar esta investigación, es analizar los riesgos y las vulnerabilidades presentes en los activos de la información, basados en el estándar ISO/IEC 27005:2008, cuya orientación se enfoque en minimizar la ocurrencia de los riesgos en el ISP.

El propósito que se persigue con este artículo, es elaborar un conjunto de recomendaciones que permiten dar tratamiento al riesgo en torno a las normas y estándares seleccionados.

Figura 1. Organigrama Empresa de Telecomunicaciones Sistelcel



En la figura 1 se muestra el organigrama de la Empresa de Telecomunicaciones que fue aprobada por parte de Supertel.

Desarrollo

Teoría de Riesgo

Riesgo: Se define como riesgo a la probabilidad que suceda algo a partir de las vulnerabilidades de un sistema, provocando un impacto en los activos de la empresa.

Impacto

El impacto de los procesos es el cumplimiento de los objetivos de la empresa, en donde se determinan los tiempos de recuperación objetivo (RTO) y el impacto asociado con la interrupción de los procesos por un determinado periodo.

Amenaza

Las amenazas producen acciones o situaciones negativas a la operatividad de la empresa, entidad u organismo. Se considera una amenaza los fallos de programación, los virus, uso inadecuado de

software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, entre otros.

Vulnerabilidad

Las vulnerabilidades son acciones inseparables a los activos que proveen las amenazas, se materialicen y llevan a esos activos a ser vulnerables. Las amenazas están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto. Entre otras, podríamos citar la falta de conocimiento del usuario, tecnologías inadecuadamente probadas, transmisión de datos por redes públicas, etc. Una vulnerabilidad común es contar con un antivirus no actualizado, lo cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado, la amenaza (virus), si bien potencialmente seguiría existiendo, no podría materializarse, ni, por lo tanto, crear daño alguno.

Tratamiento del Riesgo

Se define como tratamiento al riesgo al conjunto de actividades que se aplica, a partir de los riesgos evaluados, tiene como objetivo principal la aplicación de controles para reducir, aceptar, evitar o transferir el riesgo analizado.

Confidencialidad

Se define que la información no está disponible para las personas que no están autorizados a ella. Se debe establecer controles estrictos para las personas que necesiten el acceso a cierta información.

Integridad

Es la propiedad que busca mantener que la información no pueda ser modificada de manera inesperada.

Disponibilidad

Es la condición de que la información esté disponible, previene que los recursos sean eliminados o que estén inaccesibles, esto aplica no solo a la información, sino también a la infraestructura tecnológica en la empresa.

Análisis de Riesgo

Son las posibles amenazas de los activos de la organización y de los daños y consecuencias que pueden ocasionar las vulnerabilidades de la empresa.

Normas y estándares para la gestión de riesgos

Metodologías

ISO 27005:2008

El estándar ISO/IEC 27005:2008, define las directrices para elaborar el proceso de análisis de riesgos. Éste forma parte de la familia ISO 27000, y sirve de complemento a las dos primeras normas de la familia, ISO/IEC 27001:2005 e ISO/IEC 27002: 2005.La propuesta es similar al AS/NZS y contempla los siguientes sub-procesos como se muestra en la figura 2.

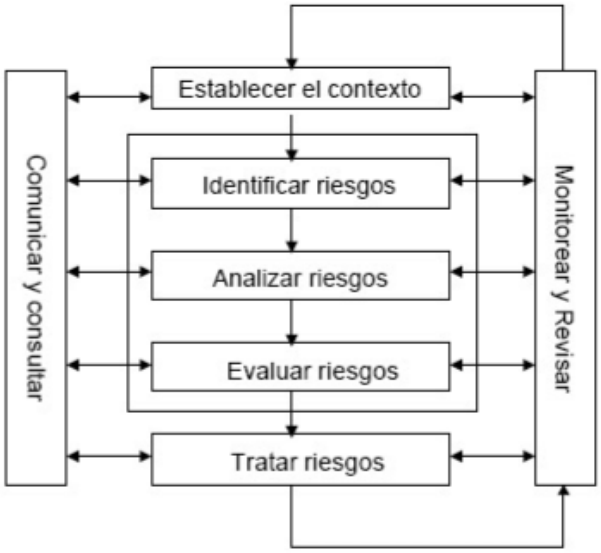


Figura 2. Proceso de la Gestión de Riesgo ISO/IEC 27005

Establecimiento del contexto: Recolecta la información más importante de la empresa para establecer los límites y el alcance.

Valoración de riesgos: Realiza de forma cualitativa y cuantitativa los riesgos en donde prioriza y evalúa conforme a los objetivos de la empresa.

Identificar el riesgo: De acuerdo a la identificación de los activos de la empresa se puede determinar la causa de la pérdida de información y entender cómo, dónde y por qué puede ocurrir.

- Análisis de riesgo: Se calcula la magnitud del riesgo al que está expuesta la empresa, en donde se determina el valor y las medidas se debe tomar para proteger los datos de la empresa de acuerdo a las normas y estándares.
- Evaluación del riesgo: Posterior al análisis de riesgo, se prioriza cada uno de los riesgos encontrados en la empresa.
- Tratamiento de riesgos: Se selecciona los controles de seguridad que se implantará para mitigar el riesgo.

Comunicación del riesgo: La finalidad es entender el impacto del riesgo y de comunicar al gerente de la empresa.

Monitorización y revisión de riesgo: Tener un seguimiento de los controles que se deben implementar para asegurar que funcione adecuadamente, es necesario establecer auditorías internas, y mantener la documentación correcta.

MAGERIT

Metodología española promovida por el Ministerio de Administraciones Públicas de España y desarrollada por el Consejo Superior de Administración Electrónica (CSAE), para la gestión y análisis de riesgos de los sistemas de información, que en sus tres libros: "Método", "Catalogo de elementos" y "Guía de técnicas", sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos como se detalla en la figura 3.

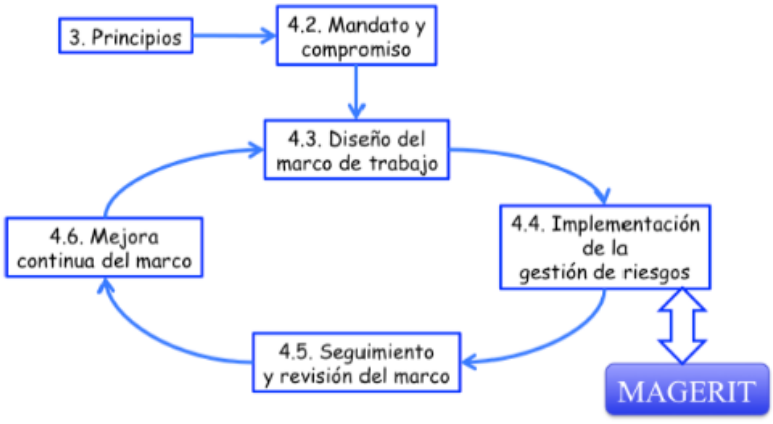


Figura 3. Metodología Magerit

Fases de Magerit

- Caracterización de activos
- Caracterización de amenazas
- Caracterización de salvaguardas

- Estimación del estado del riesgo

Esta metodología realiza procesos para el análisis y gestión de los riesgos en los sistemas informáticos, el objetivo principal es mitigar el riesgo y sensibilizar a los gerentes de las empresas la protección de los activos más importante y seleccionar el personal adecuado que cumple con el perfil.

Metodología

Al tratarse de una investigación descriptiva, se selecciona como técnica para la recolección de datos una encuesta y una serie de atributos calificativos; se aplicará el método cualitativo y cuantitativo para obtener una indicación general del riesgo y determinar los más relevantes que pueden afectar a la empresa.

Esta investigación inicia con un autodiagnóstico basado en la norma ISO 27001, se continúa con la selección de una metodología de análisis de riesgos.

Luego de seleccionada la metodología (Magerit), como parte de la misma, se procede a elaborar un inventario de los activos de la información que posee la empresa, para tener un panorama completo de los activos que gestionan la información.

En base a los activos determinados, se procede a evaluar el riesgo a nivel de hardware, software, personas y datos.

Finalmente, con los resultados del análisis de riesgos se procede a establecer un conjunto de recomendaciones que brinden tratamiento al riesgo, basado en normas y estándares.

Resultados

Se realiza un análisis inicial de la seguridad de la información utilizando una encuesta y un formulario de la norma ISO 27001, como reporte de impacto se verifica que está en un 61% en la seguridad de la información y en un 39% no cumple con los procesos de políticas de seguridad, organización de la seguridad, clasificación y control de los activos, seguridad del personal, seguridad física, gestión de comunicaciones y operaciones, control de acceso, desarrollo y mantenimiento.

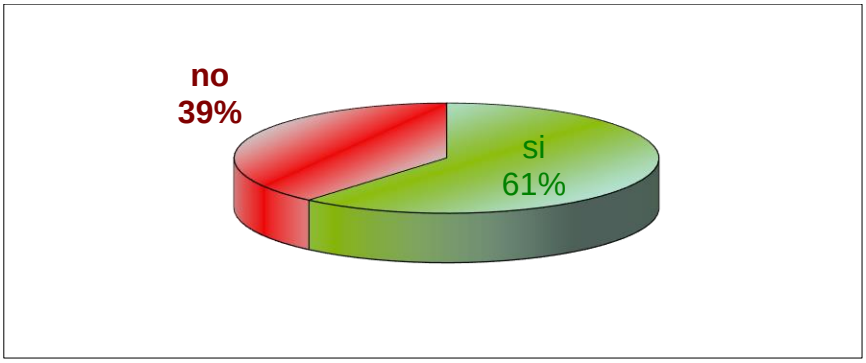


Figura 4. Resultado autodiagnóstico general

En la figura 4 el 39% corresponde a la carencia de documentación de la seguridad de los SI, no existe mecanismos para la comunicación y control de las políticas de seguridad, así como no tiene establecido información sobre incidencias, vulnerabilidades y no cuenta con un proceso de la seguridad de la información, en la seguridad física carece de controles frente al acceso de personal no autorizado, seguridad para los equipos retirados exteriormente y la seguridad de equipos móviles, en el control de Acceso no existe un registro formal no hay protección de los equipos desatendidos, carece de políticas de limpieza en el puesto de trabajo, a nivel del teletrabajo y la computación móvil no cuenta con procedimientos adecuados.

Determinación activos

Un activo es algo que tiene valor o utilidad en sus operaciones y continuidad para la organización. Sobre estos activos de información, es necesario proteger y asegurar las operaciones correctas para el giro del negocio, por lo tanto, estos deben ser clasificados según el tipo de activo.

Se puede identificar los activos de la empresa para el tratamiento de la información (hardware, software, personas, datos) en donde deben agruparse de acuerdo a las funciones que establecen para el tratamiento de la información, la empresa cuenta con diferentes activos para un desempeño optimo que permita analizar el valor de cada uno y para el desarrollo de su trabajo diario.

Hardware (Equipamiento informático)

En los equipos de hardware se encuentra los siguiente

- Servidores: De aplicación y Base de Datos
- Impresoras: Dispositivo multifunción para el área administrativa y técnica
- Cámaras de seguridad: Están colocadas en puntos estratégicos por parte de la empresa.

- Televisores: Se encuentra ubicada en el área técnica
- Teléfonos: Se encuentran ubicados en el área administrativa y en el área operativa
- Computadoras de escritorio: Se encuentran ubicadas en el área administrativa
- Portátiles: Es de uso de la parte del jefe técnico y del personal de planta externa.
- Switch: Está ubicado en el cuarto de equipos
- Router: Está ubicado de acuerdo a la necesidad de cada área.

Software

Aplicaciones que tiene la empresa.

- Sistemas operativos: Windows 10
- Antivirus: Nod 32
- ERP: Software para la administración de los clientes.
- Office: Paquete de Microsoft Officce 2010

Datos

- Base de Datos: Donde almacena toda información de la empresa se tiene mediante un contratista en la nube.

Personas

Personal que se tiene en la organización.

- Gerente de Sistemas Líder a nivel del área técnica
- Contratista Base de Datos: Proveedor de almacenamiento de la información de la empresa
- Jefe de Soporte: Encargado de las aplicaciones técnicas de la empresa
- Personal Técnico: Equipo de instalaciones y soporte técnico
- Clientes: Usuarios que se presta el servicio.
- Contadora: Se encarga de toda la parte contable de la empresa a través del servidor en la nube
- Secretaria: se encarga de recepción de requerimientos y agenda electrónica del personal de acuerdo al trabajo que se realiza.

Valoración de los Activos

La valoración del Activo de la organización es un perjuicio si el Activo se ve dañado en dicha dimensión, en la tabla 1 se determina los criterios calificativos y el valor que se utilizara en la evaluación de los activos.

Tabla 1. Valoración de los activos

Valor	Nivel	Dependencia	Funcionalidad	Pilares de Información
1	BAJO	Ningún activo depende de este, para brindar servicios a los usuarios.	Capacidades tecnológicas muy limitadas.	La integridad, y no interrupción del activo afecta de manera insignificante a la entrega de servicios a los usuarios.
2	MODERADO	Pocos activos dependen de él, para brindar sus servicios.	Capacidades tecnológicas limitadas.	La integridad, y no interrupción del activo afecta en parte a la entrega de servicios a los usuarios.
3	ALTO	Una gran cantidad de activos depende de él, para brindar sus servicios	Capacidades tecnológicas avanzadas.	La integridad, y no interrupción del activo afecta significativamente a la entrega de servicios a usuarios
4	MUY ALTO	Un numero bastante considerable de activos dependen de este para entrega de servicios a los usuarios	Activos con capacidades tecnológicas muy avanzadas	La divulgaci´n, modificación y no disponibilidad del activo puede afectar gravemente a la entrega de servicios a los usuarios
5	CRÍTICO	Todos los activos dependen de él, para brindar los servicios a usuarios	Capacidades tecnológicas de última generación.	La integridad, y no interrupción del activo afecta totalmente a la entrega de servicios a los usuarios

Tabla 2. Valoración del Impacto

		Dimensiones de Seguridad			Escala valoración	Valoración Activo	Valoración del impacto
Tipo de activo	Descripción del Activo	Confidencialidad	Integridad	Disponibilidad			
Hardware	Servidores: De aplicación y Base de Datos	5	5	5	5	Crítico	Directo
	Impresoras: Dispositivo multifunción para el área administrativa y técnica	4	4	4	4	Alto	Indirecto

Pol. Con. (Edición núm. 35) Vol. 4, No 7, julio 2019, pp. 174-195, ISSN: 2550 - 682X

	Cámaras de seguridad: Están colocadas en puntos estratégicos por parte de la empresa.	3	4	4	3	Alto	Directo
	Televisores: Se encuentra ubicada en el área técnica	3	3	3	3	Medio	Indirecto
	Teléfonos: Se encuentran ubicados en el área administrativa y en el área operativa	4	4	4	4	Alto	Indirecto
	Computadoras de escritorio: Se encuentran ubicadas en el área administrativa	5	5	5	5	Muy Alto	Indirecto
	Portátiles: Es de uso de la parte del jefe técnico y del personal de planta externa.	5	5	5	5	Crítico	Indirecto
	Switch: Está ubicado en el cuarto de equipos	5	5	5	5	Crítico	Indirecto
	Router: Está ubicado de acuerdo a la necesidad de cada área.	4	3	4	4	Alto	Indirecto
Software	Sistemas operativos: Windows 10	5	4	5	5	Muy Alto	Indirecto
	Antivirus: Nod 32	5	3	5	4	Muy Alto	Indirecto
	ERP: Software para la administración de los clientes.	5	5	5	5	Crítico	Directo
	Office: Paquete de Microsoft Officce 2010	3	3	3	3	Medio	Indirecto
Datos	Base de Datos: Donde almacena toda información de la empresa en donde tiene mediante un contratista en la nube.	5	5	5	5	Crítico	Directo
Personas.	Gerente de Sistemas Líder a nivel del área técnica	5	4	5	4	Muy Alto	Directo
	Contratista Base de Datos: Proveedor de almacenamiento de la información de la empresa	5	5	4	4	Muy Alto	Indirecto
	Jefe de Soporte: Encargado de las aplicaciones técnicas de la empres	5	5	5	5	Muy Alto	Directo
	Personal Técnico: Equipo de instalaciones y soporte técnico	4	5	4	4	Alto	Directo

	Clientes: Usuarios que se presta el servicio.	4	4	4	4	Alto	Directo
	Contadora: Se encarga de toda la parte contable de la empresa	4	4	4	4	Alto	Indirecto
	Secretaria: se encarga de recepción de requerimientos y agenda electrónica del personal de acuerdo al trabajo que se realiza.	4	3	4	4	Alto	Indirecto

En la tabla 2 se ha determinado el valor de cada activo y del impacto se relaciona de acuerdo al grado de éxito del incidente como el impacto Directo se ha considerado de ser la reposición del valor financiero del activo perdido, el costo del activo por adquisición, instalación, configuración, también el precio por operaciones suspendidas a nivel del impacto indirecto se ha considerado el costo de oportunidad, nuevos recursos para el reemplazo de un activo, el costo de operaciones interrumpidas, la mala utilización de la información,

Identificación de amenazas

Las amenazas pueden ser de tipo naturales, físicas o ambientales, humanas o accidentales, técnicas, organizacionales.

Tabla 3. Origen de la amenaza

Clasificación	Descripción
A	Accidentales: Clasifica las acciones humanas que pueden dañar accidentalmente los activos de información
D	Deliberadas: Clasifica todas las acciones deliberadas que tienen como objetivo los activos de la información
E	Ambientales: Clasifica todos los incidentes que se basa en acciones

Tipo	Amenazas	Accidentales	Deliberadas	Ambientales
Acciones no autorizadas	Procesamiento ilegal de la información		X	
	Acceso no autorizado al sistema		X	

	Ataques contra el sistema		X	
	Copia fraudulenta del software		X	
	Corrupción de los datos		X	
	Ingreso de datos falsos o corruptos	X	X	
	Acceso forzados al sistema	X	X	
	Suplantación de identida		X	
	Uso de softeare falso o copiado	X	X	
	Uso no autorizado del equipo		X	
Compromisos de la información	Espionaje remoto		X	
	Divulgación	X	X	
	Robo de Equipo		X	
	Robo de información		X	
	Robo de medios o Documentos		X	
	Robo de Entregable		X	
	Manipulación con software		X	
	Recuperación de medios reciclados o desechados		X	
Daño Fisico	Daño por agua	X	X	X
	Daño por fuego	X	X	X
	Destrucción del equipo o de los medios	X	X	X
	Polvo corrosión, congelamiento	X	X	X
Eventos naturales	Fenómenos climáticos			
	Inundaciones			
	Sismo			
Fallas Técnicas	Saturación del sistema de información		X	X
	Errores en el sistema		X	
	Falla del equipo		X	
	Incumplimiento en el mantenimiento del sistema de información		X	X
	Mal funcionamiento del Equipo		X	
	Mal funcionamiento del software		X	
Perdida de los servicios esenciales	fallas en el equipo de telecomunicaciones		X	X
	Perdidas de suministro de energía		X	X

Tabla 4. Identificación de vulnerabilidades

Tipo de Activo	Amenaza	Vulnerabilidades
	Accidente Importante	**Sobrecargas**
Hardware	Daño por agua	Ubicación en una área susceptible de inundación
	Daño por fuego	Ubicación en áreas susceptibles
	Error en el uso	Configuración incorrecta de parámetros
	Falla del equipo	Mantenimiento insuficiente
	Mal funcionamiento del Equipo	Contaminación mecánica
	Perdida de suministro de energía	No hay energía para el funcionamiento de los dispositivos y continuar con el proceso de trabajo
	Polvo, corrosión, congelamiento	Deterioro del hardware
	Uso no autorizado del equipo	Falta de revisiones regulares por parte de la gerencia
	Destrucción del Equipo o de medios	falta de esquemas de reemplazo periódico
	Hurto de equipo	Perdida de información
		Falta de procesos disciplinarios definidos en el caso de incidentes de SI
Software	Ataques contra el sistema	Perdida de información
	Copia fraudulenta del software	Falta de disponibilidad
	Corrupción de los datos	Utilización de los programas de aplicación a los datos errados en términos de tiempo
	Error en el usuario	Configuración incorrecta de parámetros
	Errores en el sistema	Disponibilidad de la información
	Incumplimiento en el mantenimiento del sistema de información	Falta de procedimientos de control de cambios
	Copia fraudulenta del software	Falta de disponibilidad
	Mal funcionamiento del software	Disponibilidad del servicio
	Uso de software falso o copiado	Falta de disponibilidad
	Hurto de la información	Almacenamiento sin protección
	Uso no autorizado del equipo	Perdida de información
	Falla en el equipo de Telecomunicaciones	Conexión deficiente de los cables
	Negación de Servicio	Disponibilidad de la información
	Acceso no autorizado al sistema	Almacenamiento sin protección
Persona	Incumplimiento en la disponibilidad del personal	Ausencia del Personal
	Suplantación de identidad	Sesiones de usuarios habilitadas

Datos	Corrupción de los datos	Utilización de los programas de aplicación a los datos errados en términos de tiempo
	Hurto de información	Almacenamiento sin protección
	Ingreso de datos falsos o corruptos	Disponibilidad de la información
	Acceso forzado al sistema	Almacenamiento sin protección
	Manipulación con Software	Falta de copias de respaldo
		Descarga y uso no controlado de software
	Saturación del sistema de información	falta de mantenimiento
	Daño por fuego	ubicación en una área susceptible
	Daño por agua	Ubicación en una área susceptible de inundación
	Destrucción del Equipo o de medios	falta de esquemas de reemplazo periódico
	Hurto de equipo	Falta de procesos disciplinarios definidos en el caso de incidentes de SI
	Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad
	Procesamiento ilegal de la información	Fuga de información
		Falta de mecanismos de monitoreo
		Habilitación de servicios innecesarios
	Abuso de derechos	Falta de procedimiento formal para el registro y retiro del registro de usuarios
	Hurtos de medios o Documentos	Almacenamiento sin protección
	Divulgación	Sesiones de usuarios habilitadas
		Fuga de información
		Susceptibilidad a la humedad, el polvo y la suciedad
	Recuperación de medios reciclado o desechados	Perdida de información
	Hurto del entregable	Disponibilidad de la información
	Suplantación de identidad	Sesiones de usuarios habilitadas
	Error en el uso	Configuración incorrecta de parámetros
	Espionaje Remoto	Arquitectura insegura de la red
		Transferencia de contraseñas autorizadas
	Uso no autorizado del equipo	Falta de revisiones regulares por parte de la gerencia

En la Tabla 3 podemos determinar que una de las amenazas con mayor riesgo son los crimines computacionales por el incremento de hacker, cracker entre otros, el impacto para la entrega de servicios es grave por la afectación de los usuarios afectando el tiempo de recuperación del servicio.

Las amenazas de tipo natural como el sismo a pesar de ser muy imposibles se deben tomar en cuenta ya que generarían un impacto alto en la entrega de los servicios para los usuarios.

Los servidores, los switchs, routers, etc., deben tener mejores medidas de seguridad con la finalidad de evitar daños no deseados. El continuo funcionamiento es primordial para la empresa.

El nivel de riesgo de los errores personales se termina como alto en los activos analizados por lo que se debe tener en cuenta concientizar al personal que administra la red de datos.

Una vez determinados los riesgos, se utiliza una escala del 1 al 5, y se realiza una ponderación de la calificación al jefe del Departamento de TI colocan en la probabilidad de ocurrencia del riesgo y el impacto negativo que tendría el mismo para el cumplimiento de los objetivos organizacionales, obteniendo así el riesgo inherente como se observa en la figura 5.

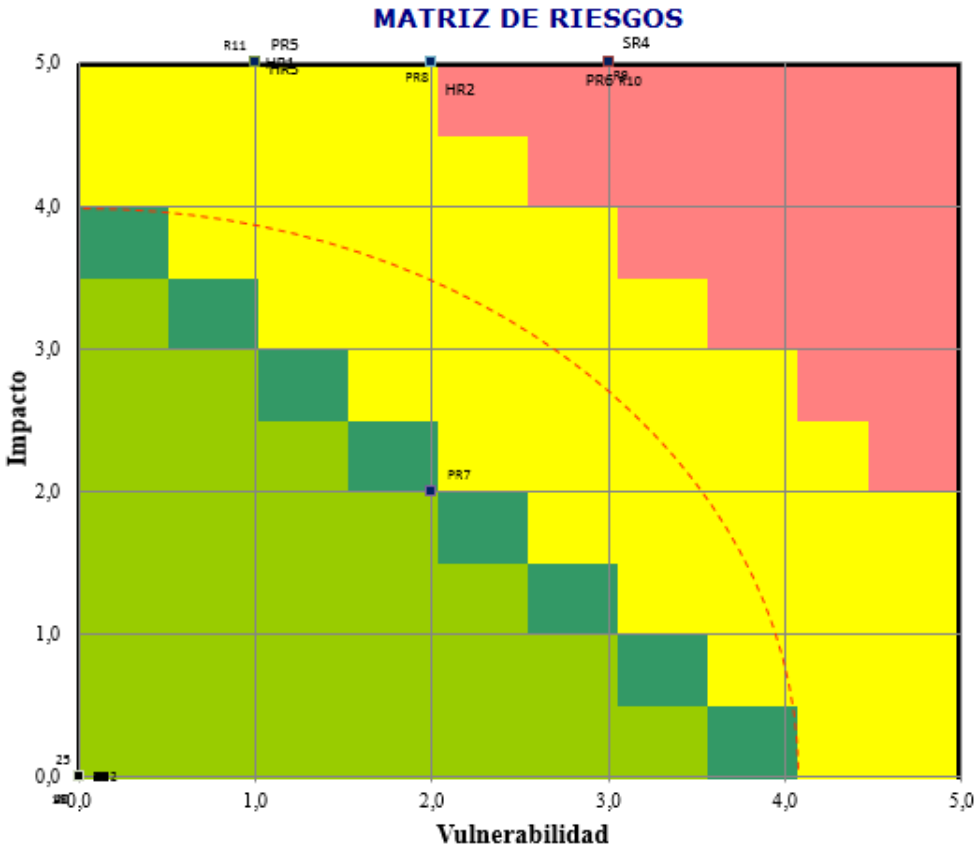


Figura 5. Riesgo Inherente

En la tabla 5 se encuentran los riesgos estudiados y los controles propuestos.

Tabla 5. Controles propuestos a los riesgos hallados

Código	Riesgo	Controles Propuestos
DR1	Uso no controlado de los Activos de la información	Elaborar y mantener un inventario actualizado de todos los activos importantes.
HR2	Falla eléctricas	Se transferir al riesgo para la protección física contra daños por fuego, inundación y otras formas de desastres naturales o causador por el hombre.
HR3	No existe controles de seguridad física adecuados	Se debería implementar controles de seguridad física
SR4	Falla de software (antivirus, Gestor de Base de Datos)	Se debe controlar y realizar procedimientos que garanticen los respaldos periódicos de información
PR5	Perdida de Personal	Realizar una gestión de conocimientos ante la ausencia de un empleado
PR6	Crimen computacional	Realizar políticas de seguridad
PR8	Incorrecta administración del Sistema Informático	Realizar políticas que regulen el uso de sistemas informáticos de acuerdo al perfil de usuarios
HR9	Falla de Componentes	Se debería implementar pruebas periódicas antes el uso o puesta en producción
HR10	Mal funcionamiento en los equipos	Realizar capacitaciones en el uso de los equipos a los usuarios
D11	Falta de Normas	Realizar un plan de contingencia

Luego de aplicar los controles ahí los riesgos se sitúan del área roja a la amarilla, y de la amarilla a la verde, porque esto indica que el riesgo ha disminuido, por lo tanto, se obtiene una matriz de Riesgo Residual como se muestra en la figura 6.

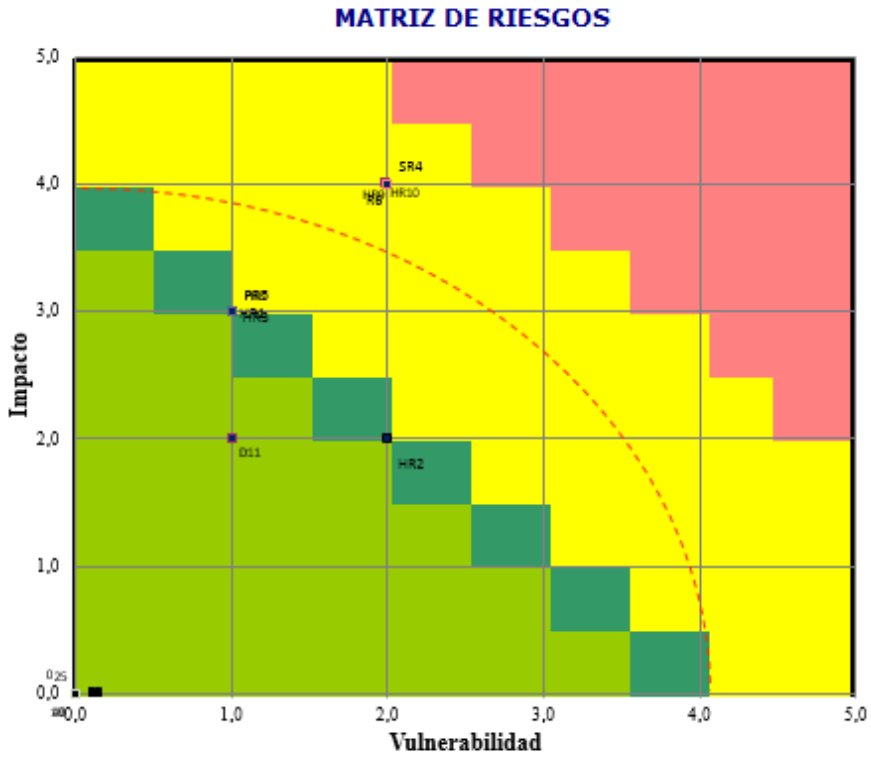


Figura 6. Riesgo Residual.

Conclusiones

- El autodiagnóstico expone que, al determinar los activos de la empresa y las vulnerabilidades encontradas, se presentó gráficamente el riesgo inherente antes de aplicar controles, se puede observar que la empresa está en una zona vulnerable, a partir de este análisis la importancia de establecer controles para su mitigación.
- En las tablas para el tratamiento del riesgo se clasificaron los activos de mayor importancia y se establecieron controles para elaborar y mantener un inventario actualizado, transferir el riesgo para la protección física, implementar controles de seguridad, realizar procedimientos de respaldo periódicos de información, realizar capacitaciones, políticas de seguridad, plan de contingencia y medidas para asegurar la información de la empresa que podrían quebrantar con la continuidad de la organización.
- Por la falta de capacitación sobre los riesgos que puede presentar la empresa y el manejo inadecuado de los sistemas informáticos, se deben establecer políticas de seguridad claras para los usuarios que manejan para cada uno de los activos de la empresa.

- Los resultados de esta investigación identifican el valor de los activos de la información desde un análisis de riesgo, por lo tanto, la empresa debe establecer un esquema de protección, permitiendo invertir de forma inteligente en diferentes iniciativas de seguridad de la información.

Referencias Bibliográficas

"Las tendencias en los riesgos relacionados a TI |." [Online]. Available: http://www.itahora.com/actualidad/seguridad/las-tendencias-en-los-riesgos- relacionados-a-ti/. [Accessed: 08-Dec-2017].

I. R. Narváez Barreiros, "Aplicación de la norma Iso 27001 para la implementación de un SGSI en la fiscalía general del estado," Pontif. Univ. Católica del Ecuador, 2013.

H. Alemán Novoa and C. Rodríguez Barrera, "Metodologías para el análisis de riesgos en los sgsi," Publicaciones e Investig., vol. 9, no. 0, p. 73, Oct. 2015.

J. Muñoz and Jorge, "Diseño de un plan estratégico para la seguridad de la información de CIAS & Profesionales S.A.S," 2018.

ISO 25012." [Online]. Available: http://iso25000.com/index.php/normas-iso-25000/iso-25012?limit=5&limitstart=0. [Accessed: 08-Dec-2017].

N. Yaraghi and R. G. Langhe, "Critical success factors for risk management systems," J. Risk Res., vol. 14, no. 5, pp. 551–581, May 2011.

S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An enhanced risk assessment framework for business continuity management systems," Saf. Sci., vol. 89, pp.201–218, Nov. 2016.

M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," Appl. Comput. Informatics, vol. 9, no. 2, pp. 107–118, 2011.

S. Morimoto, S. Shigematsu, Y. Goto, and J. Cheng, "Formal verification of security specifications with common criteria," in Proceedings of the 2007 ACM symposium on Applied computing - SAC '07, 2007, p. 1506.

W. G. Carrera Villamarín and S. J. Garcia Venegas, “Diseño de un modelo de gestión de riesgos de seguridad de la información basado en el acoplamiento de la norma ISO/IEC 27005:2008 y el Método Octave,” 2013.