Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama

Enríquez V.*; Hidalgo P.*

**Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito, Ecuador*
e-mail: vodia.enriquez@gmail.com; phidalgo@ieee.org

Resumen: La gestión operativa de un centro de datos no siempre es suficiente para mantener su correcto funcionamiento. Existen riesgos de seguridad de la información que pueden provocar impactos negativos sobre los objetivos de la organización. Este artículo desarrolla una metodología para gestionar el riesgo como parte de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los lineamientos de la Norma ISO/IEC 27005. La metodología se enfoca en la valoración de activos, impactos y riesgos, como parte del Análisis de Riesgos; en la Evaluación del Riesgo y en la aplicación de controles sobre los activos de información de un Data Center de gama alta.

Palabras clave: Data Center, SGSI, ISO 27001, ISO 27005, Análisis de Riesgos

Abstract: Data center's operational management is not always sufficient enough to keep its right operation. There are information security risks that can cause negative impacts on the organization goals. This article develops a methodology to assess information risks as part of an Information Security Management System (ISMS), guided on the standard ISO/IEC 27005. This methodology focuses on the Risk Analysis, including the assessment of actives, impacts and risks; Risk Evaluation and security controls to mitigate the impacts that affects the information assets of a high availability Data Center.

Keywords: Data Center, ISMS, ISO 27001, ISO 27005, Risk Analysis

1. INTRODUCCION

La información de una empresa es uno de los activos más importantes que posee debido a que tiene un impacto directo en las decisiones del negocio. Muchas de estas empresas han delegado a Data Centers privados la gestión, mantenimiento y administración de los equipos de infraestructura para centrarse en el desarrollo de su propio negocio.

Esto ha llevado a un aumento en la demanda de servicios tales como hosting, housing y cloudcomputing que exigen la implementación de Centros de Datos más seguros y robustos.

La norma ANSI/TIA–942-A establece los lineamientos de diseño de Data Centers de gama alta, cuya infraestructura está destinada a preservar la seguridad física de la información con altos niveles de redundancia, pero no asegura un buen manejo de la información.

Con el fin de lograr este objetivo es necesario el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), que permita realizar una adecuada administración de la información, asegurando que los procedimientos y los controles sean capaces de contrarrestar de manera efectiva los distintos incidentes de seguridad que puedan ocurrir [1].

Entre las etapas necesarias para el establecimiento de un SGSI, se encuentra la Gestión de Riesgos, que permite identificar y valorar los distintos riesgos de seguridad. Varios organismos han propuesto guías para dicha gestión, como el estándar ISO/IEC 27005 [2]de la Organización Internacional de Normalización (ISO). Sin embargo, la ISO 27005 no es una metodología de riesgos que especifique como valorar los impactos y riesgos de seguridad, por lo que el artículo presenta un método que se acopla a los lineamientos detallados en dicha norma.

2. DATA CENTERS Y GESTIÓN DE RIESGOS

2.1 Niveles de disponibilidad en la infraestructura de un data center

Data Center (DC), Centro de Datos o Centro de Procesamiento de Datos (CPD) es aquella ubicación empleada para albergar los sistemas de información y sus componentes asociados, como sistemas de almacenamiento y

telecomunicaciones, los cuales son necesarios para el procesamiento de la información de una organización.

Generalmente incluye fuentes de alimentación de respaldo, conexiones redundantes de comunicaciones, controles de ambiente (por ejemplo, aire acondicionado) y otros dispositivos de seguridad [3].

Los Data Centers deben ser capaces de continuar con su funcionamiento normal bajo eventos adversos que puedan presentarse. Dicha disponibilidad puede lograrse con la implementación de conexiones, elementos, áreas o servicios redundantes.

El estándar ANSI/TIA-942-A incluye 4 niveles de disponibilidad (Tiers) para la infraestructura de un Data Center, los cuales están definidos por el Uptime Institute [4].

El Tier I posee una infraestructura básica y es susceptible tanto a interrupciones planeadas como accidentales, el Tier II contiene componentes redundantes que reducen las interrupciones, el Tier III permite realizar cualquier mantenimiento planeado sobre cualquier componente de la infraestructura sin interrupciones en la operación y el Tier IV es tolerante a fallos provocados por cualquier tipo de eventos [5]. El trabajo se enfocará a los centros de datos de gama alta Tier III y IV debido a que sus infraestructuras permiten el funcionamiento de actividades sin interrupciones.

La Tabla 1 muestra un resumen de los requerimientos de los 4 niveles de tiering.

Tabla 1: Resumen de tiering de los Data Centers [4]

	Tier I	Tier II	Tier III	Tier IV
Componentes activos para soportar equipos de TI	N	N+1	N+1	N después de algún fallo
Rutas de distribución	1	1	1 activa y 1 alterna	2 activas simultáneas
Mantenimiento concurrente	No	No	Sí	Sí
Tolerancia a fallos	No	No	No	Sí
Aislamiento independiente de sistemas	No	No	No	Sí
Tiempo de parada del sistema al año	28.8 horas	22 horas	1.6 horas	0.8 horas
Porcentaje de disponibilidad del sistema para el usuario	99.671	99.749	99.982	99.991

2.2 Modelo de gestión de riesgos de la ISO/IEC 27005

El estándar ISO/IEC 27005 plantea una guía que permite identificar y estimar los riesgos, así como mitigarlos a un nivel aceptable, utilizando un plan de seguridad. Está diseñado para asistir al establecimiento del SGSI, especificado en la norma ISO 27001, utilizando el enfoque de manejo de riesgos [6]. La Fig. 1 muestra el proceso de gestión de riesgos.

3. INFRAESTRUCTURA DE UN DATA CENTER DE ALTA DISPONIBILIDAD

Para valorar los riesgos de seguridad es necesario identificar los activos que soportan los servicios y procesos del data center. Entre los servicios que brinda un data center se encuentran los siguientes: Housing, Hosting, Cloud Computing, Respaldos (backups), Storage, Servicios por demanda, Monitoreo de recursos, Video vigilancia, Seguridad perimetral [7, 8, 9, 10].

El estándar ANSI/TIA-942-A presenta cuatro subsistemas (Telecomunicaciones, Arquitectónico - Estructural, Eléctrico y Mecánico) incluidos en la infraestructura de un Data Center de alta gama, de los cuales se desglosan a continuación algunos activos que corresponden a cada subsistema [11]:

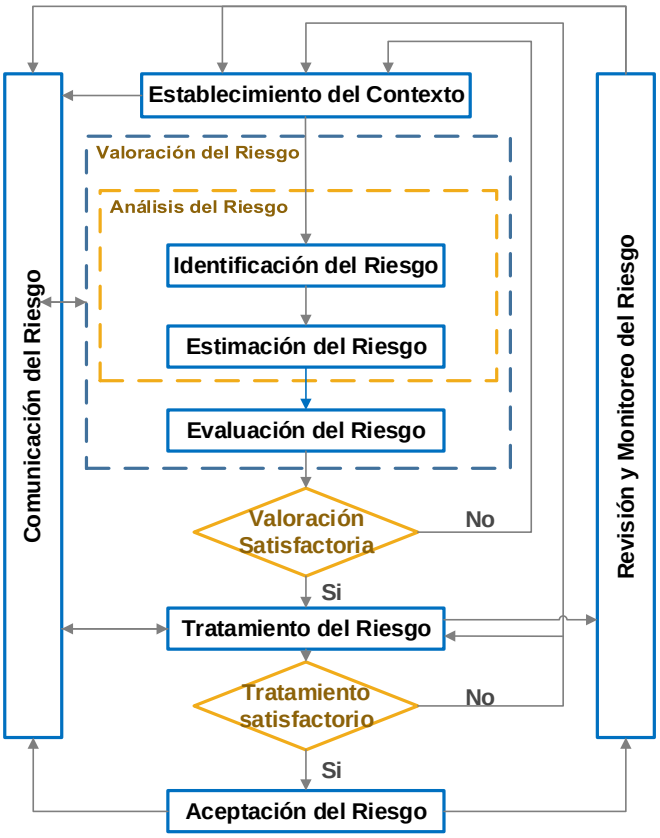

Figura 1: Proceso de Gestión de Riesgos [6]

- Activos de Documentación: Procedimientos operativos, contratos, oficios, manuales, discos extraíbles, estaciones de trabajo, laptops, agendas electrónicas, etc.

- Activos de Software: Correo, sistema de helpdesk, Active Directory, sistemas operativos, software de monitoreo y aplicaciones de las PCs, etc.

- Activos del Sistema de Telecomunicaciones: Switches, routers, firewalls, cableado estructurado, Sistemas de Control de Acceso (ACS), servidores de storage y virtualización, etc.

- Activos del Sistema Eléctrico: Generadores, transformadores, tableros, Switches de Transferencia Automática (ATS), Sistemas de Alimentación Ininterrumpida (UPS), baterías y Unidades de Distribución de Energía (PDU), etc.

- Activos del Sistema Mecánico: Chillers, bombas, tanques de expansión, Unidades Manejadoras de Aire (UMA) y válvulas de control, etc.

- Activos del Sistema de Control de Incendios: Detectores de incendios, sirenas, paneles de aspiración, paneles de control, tanques de gas, extintores y botones de incendio, etc.

- Activos del Sistema de Control de Acceso: Lectores de proximidad, lector iris/huella digital, cerraduras, barras de pánico, paneles de control, tarjetas inteligentes y trap-doors, etc.

- Activos del Sistema de Video vigilancia: Cámaras interiores, cámaras exteriores y Grabadoras de Video en Red (NVR), etc.

4. METODOLOGÍA DE VALUACIÓN DE RIESGOS

La Valuación del Riesgo consta de las siguientes actividades: Análisis del Riesgo (Identificación y Estimación del Riesgo) y Evaluación del Riesgo. Para completar dichas actividades se propuso una metodología propia enfocada en la valoración de activos, impactos y riesgos, misma que está basada en otras existentes como: MAGERIT [12], OCTAVE [13], metodologías descritas en la norma ISO/IEC 27005, NIST SP 800-30 [14], entre otras.

La metodología utiliza una valoración cualitativa con un equivalente cuantitativo dispuesto en una escala de 5 valores que van del 1 al 5 (1 - Muy Bajo, 2 - Bajo, 3 - Moderado, 4 - Alto y 5 - Muy Alto), lo que permite realizar cálculos mediante fórmulas matemáticas. La escala de valores podría aumentar o disminuir su número de niveles según se requiera [15, 16].

Los criterios de valuación, niveles de escalas, así como lo que se considera insignificante (1 - Muy Bajo) o crítico (5 - Muy Alto) depende de cada organización en conformidad a su propia realidad.

4.1 Valoración de Activos

Las amenazas no atacan directamente a los procesos o servicios, sino a los activos que los soportan, por lo que para su valoración se consideraron ciertos factores que inciden sobre estos, como el costo original o de reemplazo y los costos de las posibles consecuencias debido a la pérdida de confidencialidad, integridad y disponibilidad, como resultado de un incidente [6].

Si bien existen varias áreas que garantizan la seguridad de la información (confidencialidad, integridad, disponibilidad, trazabilidad, no repudio, contabilidad, etc.), se utilizó como base los tres conceptos más utilizados: Confidencialidad, Integridad y Disponibilidad [2].

Los costos de consecuencias están definidos para cada requerimiento de seguridad (confidencialidad, integridad y disponibilidad). Éstos son: Pérdida de reputación y confianza del cliente (Rep), Pérdida de ventaja competitiva (VCo), Violación asociada a la información privada, (IP), Violación del contrato de confidencialidad del cliente (CC), Violación de la ley y regulaciones (LR), Interrupción del servicio (IS), Interrupción de la administración y gestión (Adm) e Incumplimiento del contrato del cliente (CCl) [6, 17, 13].

El valor de un activo en cada requerimiento de seguridad será la suma de los costos de sus respectivas consecuencias:

$$V_C = Valor_{(\text{Confidencialidad})} = Rep + Vco + IP + CC + LR \quad (1)$$

$$V_I = Valor_{(\text{Integridad})} = Rep + IS + Adm + CCl + LR \quad (2)$$

$$V_D = Valor_{(\text{Disponibilidad})} = Rep + IS + Adm + CCl + LR \quad (3)$$

El valor total de un activo será la suma del costo del activo más los valores en cada requerimiento de seguridad (V_C, V_I, V_D), lo que dará como resultado su Nivel de Importancia (NI) para el cumplimento de los procesos principales del Data Center.

$$NI = Valor_{(Costo)} + Valor_{(\text{Confidencialidad})} + Valor_{(\text{Integridad})} + Valor_{(\text{Disponibilidad})} \quad (4)$$

Como ejemplo, aplicando (1) (2) (3) y (4) para el activo switch de core se obtienen los siguientes valores de confidencialidad, integridad, disponibilidad y Nivel de Importancia, como se muestra en (5) (6) (7) y (8):

$$V_C = 3 + 5 + 5 + 5 + 3 = 21 \rightarrow 5 \quad (5)$$

$$V_I = 2 + 3 + 3 + 2 + 2 = 12 \rightarrow 2 \quad (6)$$

$$V_D = 5 + 5 + 5 + 5 + 5 = 25 \rightarrow 5 \quad (7)$$

$$NI = 5 + 5 + 2 + 5 = 17 \rightarrow 5 \quad (8)$$

En conformidad con los criterios de valoración y la aplicación de las escalas de equivalencia (ej.: 21 → 5), se determina que el activo tiene una valoración de Muy Alto (valor de 5) en las dimensiones de confidencialidad, disponibilidad y costo, y Bajo (valor de 2) en Integridad.

Además por su valor de 5 en el Nivel de Importancia, se concluye que el switch de core es Crítico para el Data Center. El detalle de la justificación de la selección de los valores de los activos y su cálculo se presenta en [11].

La Fig. 2 muestra el Nivel de Importancia de los activos del Data Center.

4.2 Valoración de Impactos

El impacto es la medida del daño sobre el activo derivado de la materialización de una amenaza. Para la valoración de los

impactos es necesario estimar el Grado de Afectación para cada uno de los requerimientos de seguridad definidos. que causan las amenazas, el Impacto (I) se lo calcula usando:

$$I_{(\text{Confidencialidad})} = NI \times Grado\,\text{de}\,Afectacion_{(Confidencialidad)} \quad (9)$$

$$I_{(\text{Integridad})} = NI \times Grado\,\text{de}\,Afectacion_{(\text{Integridad})} \quad (10)$$

$$I_{(\text{Disponibilidad})} = NI \times Grado\,\text{de}\,Afectacion_{(\text{Disponibilidad})} \quad (11)$$

Para obtener una valoración del Impacto Total (It), ésta se calculará como la suma de los impactos en cada requerimiento de seguridad, en conformidad con (12):

Conociendo el valor del activo (NI) y el grado de afectación

$$It = I_{(\text{Confidencialidad})} + I_{(\text{Integridad})} + I_{(\text{Disponibilidad})} \quad (12)$$

4.3 Valoración de Riesgos

Después de identificar los escenarios de incidentes, es necesario valorar la probabilidad de ocurrencia de cada escenario. Esto se puede realizar tomando en cuenta la frecuencia de la amenaza y la facilidad de aprovechar una vulnerabilidad.

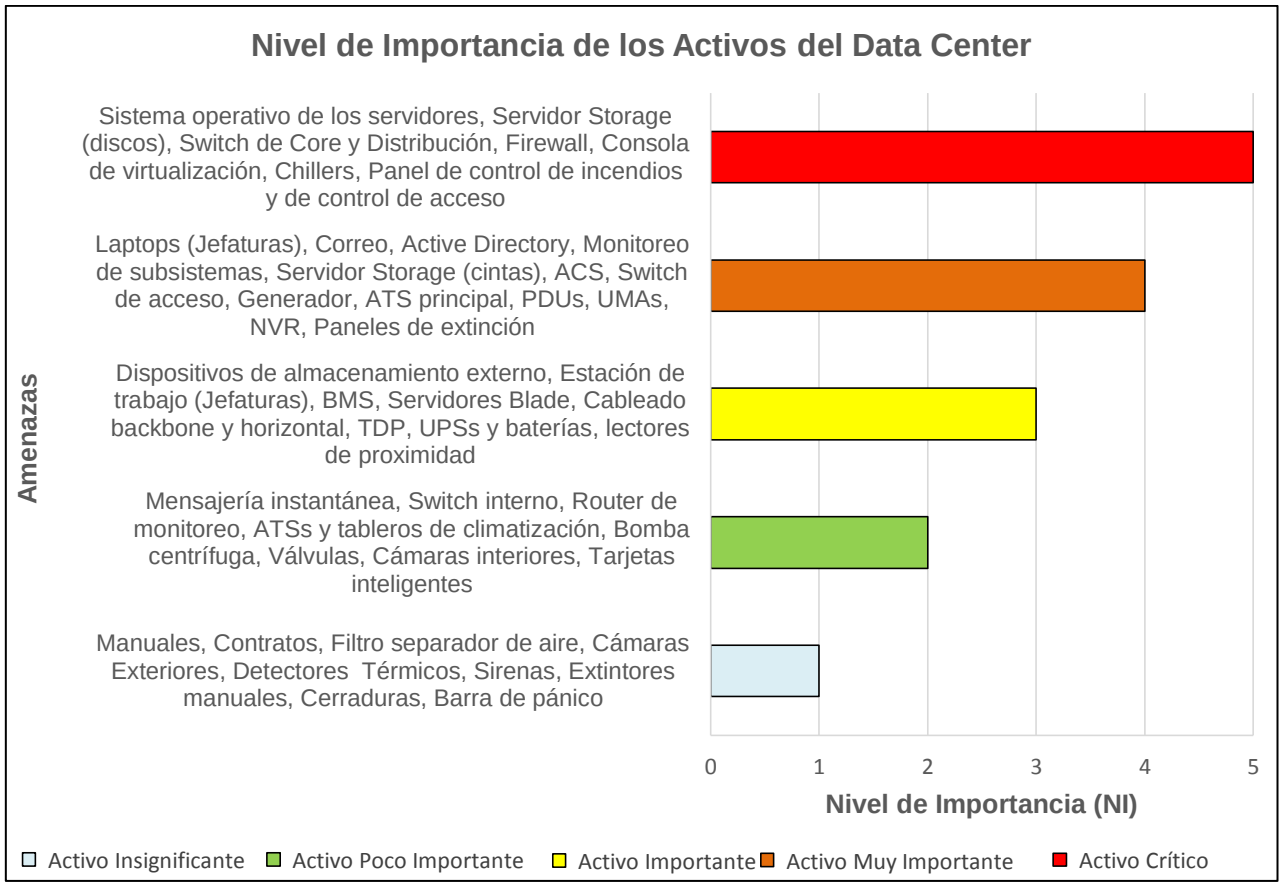

Figura 2: Clasificación de los activos del Data Center de acuerdo a su Nivel de Importancia

El Riesgo estimado es la combinación de la probabilidad de ocurrencia de un incidente y su Impacto; y se lo calcula utilizando (13) (14) y (15):

$$Riesgo_{(\text{Confidencialidad})} = Probabilidad \times I_{(Confidencialidad)} \quad (13)$$

$$Riesgo_{(\text{Integridad})} = Probabilidad \times I_{(\text{Integridad})} \quad (14)$$

$$Riesgo_{(\text{Disponibilidad})} = Probabilidad \times I_{(\text{Disponibilidad})} \quad (15)$$

El Riesgo Total (Rt) es la suma de los riesgos en cada requerimiento de seguridad y se lo determina mediante (16):

$$Rt = Riesgo_{(\text{Confidencialidad})} + Riesgo_{(\text{Integridad})} + Riesgo_{(\text{Disponibilidad})} \quad (16)$$

El Análisis y Evaluación de Riesgos se enfocó solamente a los activos descritos en la sección 3, que soportan los procesos y servicios del Data Center y el detalle de todos los cálculos se encuentra en [11].

Se tomaron en consideración las siguientes amenazas que pudieren causar daño a los activos [17, 13]:

- Daño Físico: Fuego, Agua, Desastre Industrial.
- Desastres Naturales: Fenómeno Sísmico, Volcánico, Meteorológico, etc.

- Pérdida de Servicios Esenciales: Corte del suministro eléctrico, climatización, comunicaciones, etc.
- Compromiso de la Información: Fugas de información, Espionaje remoto, Hurto de medios o documentos, Recuperación de medios reciclados, etc.
- Fallas Técnicas: Avería de origen físico o lógico, Errores de mantenimiento, Caída del sistema por agotamiento de recursos, etc.
- Acciones no Autorizadas: Manipulación del software y equipos, Uso no previsto de equipos, Destrucción de información, etc.
- Compromiso de Funciones: Errores de los usuarios, Errores de configuración, Suplantación de la identidad del usuario, Abuso de privilegios de acceso, Ataque destructivo, Extorsión, etc.

Como ejemplo de aplicación de la metodología para el activo switch de core se selecciona la amenaza *Modificación de la Configuración del switch*. Aplicando (9) (10) (11) y (12), se muestran los resultados del impacto en (17) (18) (19) y (20).

La amenaza tiene diferentes grados de afectación e impactos para cada requerimiento de seguridad, obteniéndose valores de Muy Alto (valor de 5) para integridad y disponibilidad y Moderado (valor de 3) para confidencialidad. También se verifica que el Impacto Total es Muy Alto (valor de 5) de acuerdo a los criterios establecidos.

$$I_{(\text{Confidencialidad})} = 5 \times 2 = 10 \rightarrow 3 \quad (17)$$

$$I_{(\text{Integridad})} = 5 \times 5 = 25 \rightarrow 5 \quad (18)$$

$$I_{(\text{Disponibilidad})} = 5 \times 5 = 25 \rightarrow 5 \quad (19)$$

$$It = 3 + 5 + 5 = 13 \rightarrow 5 \quad (20)$$

Los valores de riesgo para el activo se muestran en (21) (22) (23) y (24).

La ocurrencia de la amenaza es Muy Probable (valor de 4), lo que conlleva a riesgos Muy Altos (valor de 5) en integridad y disponibilidad y un riesgo Moderado (valor de 3) en confidencialidad. El Riesgo Total presenta una valoración de Muy Alto (valor de 5).

$$Riesgo_{(\text{Confidencialidad})} = 4 \times 3 = 12 \rightarrow 3 \quad (21)$$

$$Riesgo_{(\text{Integridad})} = 4 \times 5 = 20 \rightarrow 5 \quad (22)$$

$$Riesgo_{(\text{Disponibilidad})} = 4 \times 5 = 20 \rightarrow 5 \quad (23)$$

$$Rt = 3 + 5 + 5 = 13 \rightarrow 5 \quad (24)$$

La Fig. 3 muestra un ejemplo de comparación de los valores de Impacto Total, Probabilidad de Ocurrencia y Riesgo Total de las amenazas para el activo switch de core.

5. EVALUACIÓN DE RIESGOS

En base a los resultados del Análisis de Riesgos del ejemplo se determina que las amenazas que tienen mayor impacto sobre el switch de core son las siguientes: sniffers, puertos habilitados, modificación y eliminación de la configuración, errores de configuración, suplantación de identidad, abuso de derechos, ocupación enemiga y extorsión.Las de mayor probabilidad de ocurrencia y por consiguiente mayor riesgo son las siguientes: modificación y eliminación de la configuración, ingreso de personal no autorizado, suplantación de identidad y abuso de derechos.

Los datos resultantes de la Estimación del Riesgo servirán para seleccionar la opción de tratamiento de riesgo más adecuada. La norma ISO/IEC 27005 define 4 formas para tratar el riesgo: aceptar, reducir (aplicar controles), evitar y transferir el riesgo. La Tabla 2 muestra las opciones de tratamiento de riesgo seleccionadas en conformidad con los valores de impacto y riesgo [11].

Tabla 2: Criterios de aceptación y tratamiento del riesgo

Aceptación y Tratamiento del Riesgo			
I	**Rt**	**Nivel**	**Acción**
1	1	Muy Bajo	Aceptar el Riesgo
2	2	Bajo	
3	3	Moderado	Reducir el Riesgo
4	4	Alto	
5	5	Muy Alto	

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL DATA CENTER

Según la Evaluación de Riesgos, la mayoría de amenazas pueden ser tratadas mediante la reducción de sus niveles de riesgo, en conformidad con los criterios de aceptación de la Tabla 2.

Para lo cual se seleccionarán controles y se generarán políticas.Muchas amenazas pueden ser solventadas aplicando el mismo control y una amenaza puede requerir varios controles diferentes para su mitigación.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL DATA CENTER

Según la Evaluación de Riesgos, la mayoría de amenazas pueden ser tratadas mediante la reducción de sus niveles de riesgo, en conformidad con los criterios de aceptación de la Tabla 2. Para lo cual se seleccionarán controles y se generarán políticas.

Muchas amenazas pueden ser solventadas aplicando el mismo control y una amenaza puede requerir varios controles diferentes para su mitigación.

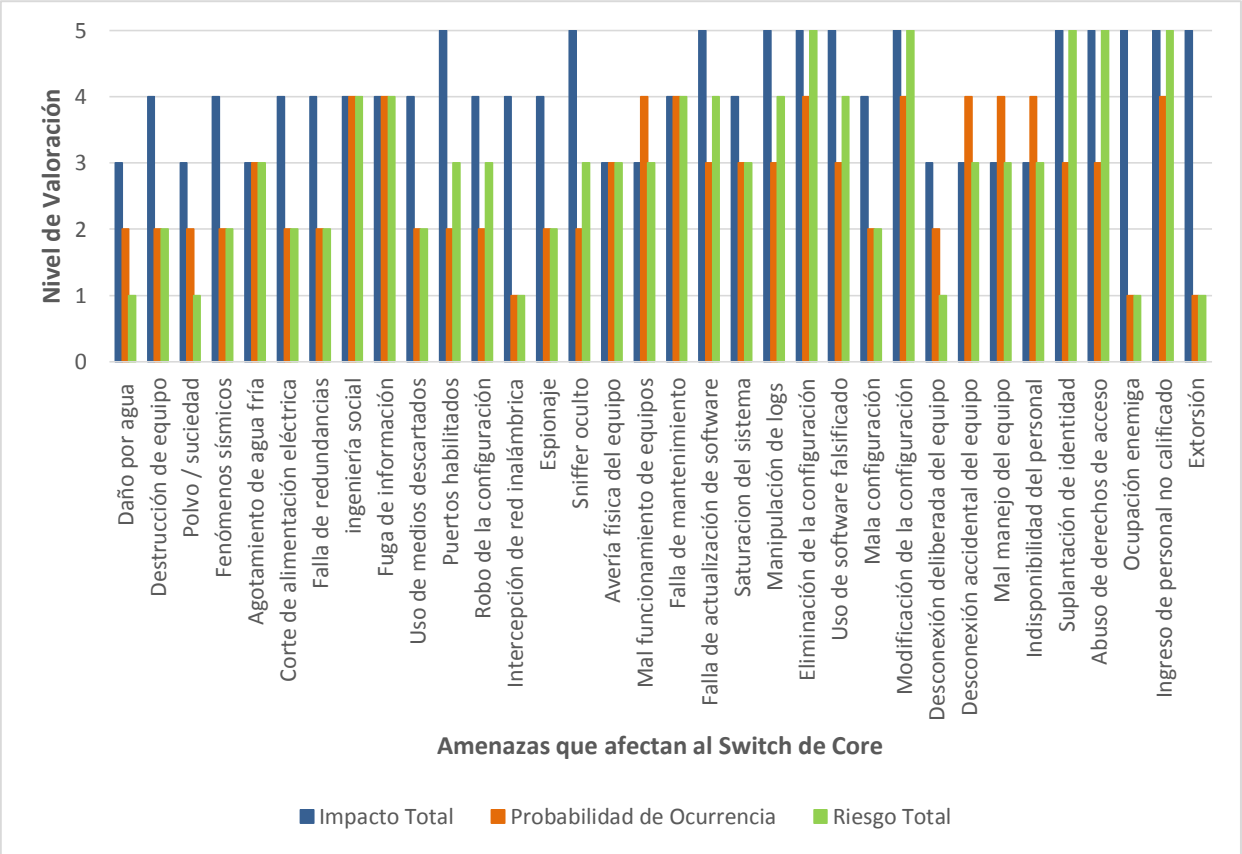

Figura 3: Análisis y Evaluación de Riesgos para el Switch de Core del Data Center

7.1 Políticas de Seguridad de la Información del Data Center de alta gama

Como proceso final del establecimiento del SGSI es necesario establecer una Política de Seguridad que permita gestionar e implementar de una manera adecuada los procesos, controles y normas de seguridad de la información del Data Center.

Para la elaboración de la Política se toma como base el modelo propuesto por la norma ISO/IEC 27002, la cual establece lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización [18].

Las políticas son de aplicación general y deben ser complementadas con procedimientos y guías de buenas prácticas detallas para cada tipo de amenazas [19].

Algunos ejemplos de políticas para gestionar la información relacionada con el switch de core se detallan a continuación. El desglose total de las políticas que aplican para todo el Data Center se encuentra especificado en [11].

7.2 Política de Organización de la Seguridad de la Información

Todos los empleados del Data Center y personal externo deben firmar un Acuerdo de Confidencialidad para preservar la información de infraestructura de red, datos, servicios, contraseñas de acceso, direccionamiento IP, configuraciones, etc.

7.3 Política de Gestión de Activos

- Los activos de red deben estar debidamente inventariados.
- Los equipos de red por ningún motivo serán utilizados con fines personales o didácticos.
- Se prohíbe la destrucción, adjudicación o modificación deliberada de la información y/o configuración existentes en los equipos de red.
- Los equipos de red no deben ser desconectados o reubicados sin autorización del Propietario del Activo y las Jefaturas.

7.4 Política de Seguridad de Recursos Humanos

- El personal será sometido a la verificación de sus antecedentes antes de su contratación.
- Todo el personal que desempeña funciones en el Data Center, deberá recibir una adecuada capacitación y actualización periódica en materia de seguridad de la información.
- Para los empleados que violen la Política de Seguridad de la Información, se seguirá un proceso disciplinario formal contemplado en las normas estatutarias, legislativas o penales.
- Se retirarán los derechos de acceso a los equipos de red cuando el empleado termine su contrato de trabajo.

7.5 Política de Seguridad Física y Ambiental

- El ingreso al Cuarto de Cómputo se controlará por verificación biométrica de huella dactilar e iris, tarjeta de proximidad y sistema trap-door.
- Todos los trabajos que se realicen en el Data Center deben ser notificados y autorizados.
- Los clientes no maniobrar equipamiento de red del Data Center.
- Los equipos de red que se vayan a eliminar o reutilizar en otra área, deberán ser revisados por el Departamento de TI, que será el responsable de la eliminación de la información.

7.6 Política de Gestión de Comunicaciones y Operaciones

- Los mantenimientos de los equipos, configuraciones o migraciones, serán planificados en horarios no laborables.
- Solo los Administradores de TI tendrán acceso a la gestión de los sistemas de información, red, servidores y storage.
- Los equipos de core deben tener copias o respaldos para garantizar la continuidad de las actividades.
- Los equipos de core y servidores críticos se localizarán en jaulas propias o racks que posean cerraduras seguras.
- Los equipos de red y servidores gestionarán diferentes privilegios y usuarios.
- Todas las conexiones que accedan a la red interna, deben pasar a través de los sistemas de defensa electrónica,
- como servicios de encriptación, IDS, IPS, firewall y autenticación.
- Todo el personal que trabaja en el Data Center está sujeto al registro de sus actividades.

7.7 Política de Control de Acceso

- Cada usuario tendrá un identificador único y personal, el cual será utilizado para monitorear y registrar las actividades que realice.
- El acceso remoto hacia los equipos de red se realizará únicamente mediante un protocolo seguro como SSH.
- Las contraseñas no deberán compartirse o revelarse bajo ninguna circunstancia.
- Se incorporarán Sistemas de Control de Acceso (ACS).
- Los puertos por defecto deberán ser cambiados, y los puertos de configuración y consola deberán tener controles de acceso.
- La transmisión de información en la red deberá cumplir protocolos que ofrezcan protección, como SSH, TSL, SSL, IPsec.

7.8 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- La instalación de nuevos sistemas operativos en equipos de red estará sujetos al análisis y evaluación de los riesgos inherentes a los cambios.
- Lo cambios en el equipamiento de red deberá seguir un procedimiento formal.

7.9 Política de Gestión de Incidentes de Seguridad de la Información

- Todo empleado del Data Center deberá reportar cualquier incidente, problema, debilidad o evento que pudiera derivar en un riesgo de seguridad.
- Los usuarios no deberán explotar la debilidad encontrada, ni tratar de solucionarla, sin seguir el debido proceso.
- El personal registrará la incidencia en un sistema informático de helpdesk y la escalará al departamento correspondiente para su mitigación si es necesario.

7.10 Política de Gestión de la Continuidad Comercial

- Se elaborarán los planes necesarios para la continuidad de las actividades del Organismo.
- Los planes de continuidad asumirán un proceso de pruebas y actualizaciones regulares para asegurar su funcionamiento.

- Los empleados deberán conocer los procedimientos de reanudación y recuperación de actividades

8. RESULTADOS

8.1 Controles de Seguridad de la Información

Para el ejemplo del activo switch de core se mencionan algunos de los controles que permitirán disminuir la probabilidad y el impacto de las amenazas: Para proteger al switch de daños físicos pueden aplicarse varios controles como: uso aceptable, trabajo en áreas seguras, seguridad de oficinas y medios, y ubicación de los equipos.

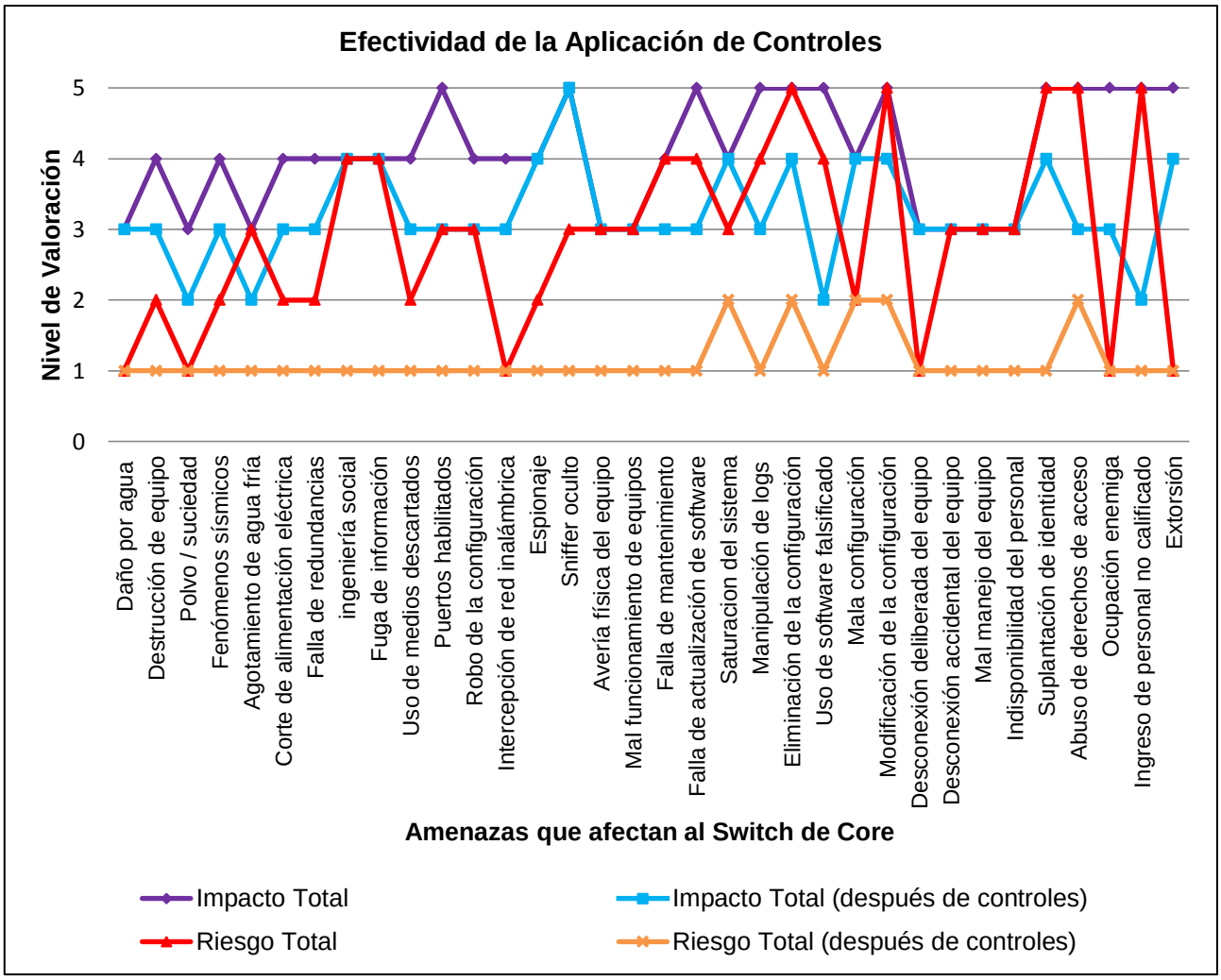

Figura 4: Análisis y Evaluación de Riesgos para el Switch de Core después de la aplicación de controle

Las políticas de protección contra amenazas externas, gestión de mantenimientos y control de servicios provistos por terceros reducen los impactos de las amenazas ambientales y garantizan la continuidad de los servicios esenciales como climatización, comunicaciones y energía eléctrica, que soportan el funcionamiento del switch de core. Los términos y condiciones del empleo, así como la capacitación de personal permiten controlar las acciones no autorizadas y los errores de ejecución o mantenimiento de equipos.

Los acuerdos de confidencialidad mitigan las amenazas de ingeniería social, divulgación de información y espionaje interno. Para evitar que personal nocivo ingrese al Data Center con el objetivo de comprometer la seguridad de la información se pueden aplicar controles de selección de personal antes del empleo, así como tratamiento de la seguridad en contratos con personal externoPara la administración del switch a través de software se utilizarán los controles de gestión de software, controles criptográficos, controles contra códigos maliciosos, gestión de privilegios.

Los controles de acceso fisco a través de tarjetas inteligentes y bitácoras disminuyen la probabilidad de que personal no autorizado ejecute daños, modificaciones, robos o espionaje.

Los daños del switch causados por errores de mantenimiento, averías físicas y mal manejo del equipo pueden solventarse aplicando las políticas de gestión de cambios y mantenimiento de activos.

Los controles de red, control de acceso lógico, gestión de claves, autenticación de usuarios, minimizan la probabilidad de amenazas como puertas traseras, ingreso a la configuración del equipo, robo de información, etc.

Los controles de monitoreo permiten verificar las actividades que realiza el personal previniendo los accesos no autorizados, cambios en la configuración, desconexiones, abuso de derechos, entre otros.

También existen controles generales que son aplicables a todas las amenazas como la aplicación de la política de seguridad, distribución de responsabilidades de seguridad, registros de auditoría, gestión de eventos de seguridad y cumplimiento de requerimientos legales.

Una vez aplicados los controles y políticas para las amenazas del switch de core y realizando nuevamente el Análisis de Riesgos, utilizando la metodología de cálculo de riesgo descrita en la sección 4, se puede verificar la acción de los controles, como se muestra en la Fig. 4.

Analizando la Fig. 4, se puede constatar que muchos de los controles aplicados son de tipo preventivo, disuasivo y supresor, ya que reducen la probabilidad de ocurrencia de las amenazas bajando los valores de riesgos, pero no tienen influencia sobre los de impacto. La disminución del grado de impacto en algunas amenazas obedece a la implementación de controles generales y administrativos.

9. CONCLUSIONES

Con el fin de cumplir los parámetros establecidos por la Norma ISO/IEC 27005 para el Análisis de Riesgos y el alcance del SGSI del Data Center, se analizaron diversas metodologías, optándose finalmente por desarrollar una metodología propia que permitiera ajustarse de mejor manera a los objetivos propuestos.

Tanto el valor del impacto como el correspondiente al riesgo, deben ser considerados en el Tratamiento de Riesgos, priorizando la aplicación de controles en las amenazas que podrían provocar impactos y riesgos altos y, posteriormente, aquellas que se relacionan solamente con altos impactos.

La aplicación de ciertos controles puede eliminar o reducir de forma significativa los riesgos de seguridad. En el ejemplo del activo switch de core se verifica que los controles son mayoritariamente preventivos, reduciendo la probabilidad de ocurrencia de una amenaza, pero no otorgan medidas correctivas o de recuperación.

La efectividad de los controles varía dependiendo del tipo de activos a proteger, las dimensiones de seguridad consideradas y las amenazas que se pretende conjurar. Para medir la efectividad de los controles es necesario realizar una retroalimentación del Análisis de Riesgos utilizando la metodología propuesta.

REFERENCIAS

[1] Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos, ISO/IEC Estándar 27001, 2013.

[2] J. R. Vacca, Computer and Information Security Handbook, New York: Elsevier, 2013.

[3] Cisco Systems, Inc., «Data Center Architecture Overview,» de Cisco Data Center Infrastructure 2.5 Design Guide, San Jose, USA, 2014, pp. 1-1.

[4] Uptime Institute, Data Center Site Infrastructure Tier Standard: Topology, 2012.

[5] TIA, Telecommunications Infrastructure Standard for Data Centers ANSI/TIA-942-A, 2011.

[6] Information technology - Security techniques - Information security risk management, ISO/IEC Estándar 27005, 2008.

[7] TELCONET CLOUD CENTER, «CENTRO DE DATOS,» 2015. [En línea]. Available: http://www.telconet.net/servicios/datacenter.

[8] L. 3, «LEVEL 3 DATA CENTER FACILITIES,» 2015. [En línea]. Available: http://www.level3.com/es/products/data-center-services/.

[9] Claro, «Data center,» 2015. [En línea]. Available: http://www.claro.com.ec/wps/portal/ec/sc/corporaciones/multinacionales/data-center#info_01.

[10] SONDA, «Servicios,» 2015. [En línea]. Available: http://www.sonda.com/data-center/.

[11] V. Enríquez, P. Torres, Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para un Data Center Tier III de un Proveedor de Servicios de Internet (ISP) Tipo, de la Ciudad de Quito, DETRI, EPN, Quito, Ecuador, 2014.

[12] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I - Método, 2012.

[13] CERT, The OCTAVE Allegro Guidebook, v1.0, 2007.

[14] Guide for Conducting Risk Assessments, NIST Special Publication 800-30, 2012.

[15] CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS, «RISK MANAGEMENT - Concepts and Methods,» 2009. [En línea]. Available: https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-risk-management.pdf.

[16] OWASP, «OWASP Risk Rating Methodology,» 2015. [En línea]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[17] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos, 2012.

[18] Tecnología de la Información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información, ISO/IEC Estándar 27002, 2013.

[19] L. P. Aguirre, «Aplicaciones de MPLS, Transición de IPv4 a IPv6 y Mejores Prácticas de Seguridad para el ISP Telconet,» *Revista Politécnica* , vol. 32, nº 2, pp. 43-51, 2013.