FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de Investigación de fin de carrera titulado:

"DISEÑO DE UN MARCO DE REFERENCIA PARA EL ANÁLISIS DE VULNERABILIDADES A UN SEGMENTO DE LA RED CORPORATIVA DE UNA EMPRESA DE TELECOMUNICACIONES EN QUITO BASADO EN LAS PRINCIPALES METODOLOGÍAS DE PRUEBAS DE SEGURIDAD INFORMÁTICA".

Realizado por:

Ing. Andrés Leonardo Meza Castillo

Director del proyecto:

Msc. José Luis Medina Balseca

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

QUITO, 21 de Marzo de 2019

DECLARACIÓN JURAMENTADA

Yo, Andrés Leonardo Meza Castillo, con cédula de identidad 1721824256, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____
Andrés Leonardo Meza Castillo
C.C: 1721824256

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Msc. Jose Luis Medina Balseca.

Magister en Gerencia de Redes y Telecomunicaciones

CC: 1711330397

LOS PROFESORES INFORMANTES

Msc. Christian David Pazmiño Flores

Msc. Luis Fabian Hurtado Vargas

Después de revisar el trabajo presentado lo han calificado

como apto para su defensa oral ante el tribunal examinador

Msc. Christian David Pazmiño Flores	Msc. Luis Fabian Hurtado Vargas

Quito, 21 de Marzo de 2019

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____
Andrés Leonardo Meza Castillo
C.C: 1721824256

AGRADECIMIENTOS

A Dios, por permitirme finalizar con éxito otra meta profesional.

A mi familia, por apoyarme en cada paso que doy y estar siempre junto a mi en todo proyecto que me he propuesto.

Al Ingeniero José Luis Medina, su experiencia y conocimientos fueron de gran aporte para la realización de este trabajo, muchas gracias por el tiempo y consejos.

A los Ingenieros Alfonso Aranda y Patricio Samaniego por el apoyo, paciencia y experiencias, excelentes profesionales con los que tengo el gusto de trabajar día a día.

A las autoridades de la Universidad Internacional SEK que con sus gestiones y guías ayudaron en la consecución de este trabajo.

DEDICATORIA

Para Leonardo, Rocío, Anita, David, Peke y Teddy, todas mis metas son inalcanzables sin su apoyo incondicional, sus consejos y cariño son la base fundamental para seguir adelante y continuar cosechando más éxitos.

RESUMEN

El presente proyecto de investigación tiene como principal objetivo facilitar la gestión de identificación, análisis y remediación de vulnerabilidades existentes en un segmento de red configurada en el Centro de Datos de una Empresa de Telecomunicaciones en la ciudad de Quito, para ello se ha conformado un marco de referencia que reúne las mejores directrices de metodologías internacionales de seguridad informática como son OSSTMM, ISSAF, NIST, PTES, CIS y OWASP, mismas que entre sus valoraciones incluyen apartados técnicos y teóricos que fortalcen la postura de seguridad en las redes y servidores de un Data Center.

Para la conformación del marco de referencia, se ha realizado la identificación de los activos que se encuentran en la red así como su respectivo anásis de riesgos, posteriormente se han identificado vulnerabilidades informáticas en los equipos que brindan servicios tanto a usuarios internos como a clientes y por último se ha conformado el plan de mitigación para solucionar las debilidades identificadas.

Los resultados de este trabajo muestran que al aplicar el marco de referencia propuesto las vulnerabilidades del segmento de red disminuyeron considerablemente por lo que esta propuesta se recomienda sea aplicada en otras redes de la Empresa y dependiendo de la situación tecnológica pueda replicarse en otras instituciones.

Claves: Data Center, Gestión de Vulnerabilidades, OSSTMM, ISSAF, NIST, PTES, CIS, OWASP

ABSTRACT

The main goal of this research project is to facilitate the identification, analysis and remediation of existing vulnerabilities in a network segment configured in the Data Center of a Telecommunications Company in Quito, to reach that a framework has been created based on the best international information security methodologies guidelines such as OSSTMM, ISSAF, NIST, PTES, CIS and OWASP, which include technical and theoretical sections that strengthen the security posture in the networks and servers of a Data Center.

The new framework includes tests like identification of the assets that are in the network as well as their respective analysis of risks, the next step is look for known vulnerabilities in the servers that provide services to both internal users and customers and the last step is create a mitigation plan to solve the identified weaknesses.

The results of this research work show a decrease number of vulnerabilities when the framework is applied to the network segment, so this proposal is recommended to be applied in other networks in the same company and depending on the technological situation can be replicated in other institutions.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

Actualmente si consideramos que, al ingresar a cualquier servicio dispuesto en internet, todos los datos ingresados se encuentran en un servidor al que depositamos toda nuestra confianza, es sencillo suponer que estos equipos deben contar con toda la seguridad posible para resguardar nuestros datos, es así que en el mundo digital nace el concepto de seguridad informática y en especial la gestión de vulnerabilidades en infraestructura, que no es más que la forma en que identificamos debilidades en los servidores y proponemos las soluciones para mitigar riesgos para evitar posibles intrusiones que atenten contra la disponibilidad, integridad y confidencialidad de la información.

Pero no todo en el mundo de la seguridad informática se trata de asegurar sistemas, ya que es una disciplina muy amplia, existen profesionales que se especializan en realizar pruebas de vulnerabilidades contra los dispositivos con el objetivo principal de demostrar a las empresas sus debilidades principales y como un atacante puede aprovecharlas para realizar actividades maliciosas que van en contra de la ley, esto lo realizan siguiendo metodologías internacionales previamente establecidas que en algunos casos comparten ciertas técnicas para la identificación, evaluación, intrusión y reportería de hallazgos.

Adicionalmente, hay que tomar en cuenta que los servicios a los que nos conectamos constantemente mediante internet desde nuestros hogares o desde nuestros lugares de trabajo, generalmente se encuentran en un sitio dispuesto a proteger de amenazas tanto físicas como lógicas al que se le ha denominado *Data Center* o Centro de Datos, el cual debe cumplir varios estándares internacionales para que sea considerado como un lugar en donde los clientes pueden confiar y colocar ahí sus equipos.

Si agrupamos lo descrito en párrafos anteriores, tenemos que existen múltiples servicios disponibles tanto desde internet como desde redes privadas que se alojan en un Centro de Datos que debe ser protegido de amenazas, el proceso de identificación y

explotación de vulnerabilidades debe ser realizado por personal de seguridad informática especializado, siguiendo las mejores metodologías internacionales disponibles para este propósito, es por ello que en respuesta a esta necesidad se debe realizar un marco de referencia para la evaluación de vulnerabilidades eficaz, que fusione las técnicas y propuestas más reconocidas de distintas metodologías con la finalidad de facilitar el trabajo de un analista o consultor en el aseguramiento de un Centro de Datos al identificar brechas de seguridad antes que atacantes lo encuentren primero.

El marco de referencia propuesto está enfocado a validar la seguridad de los servidores de un segmento de red en un Centro de Datos, sin embargo, puede ser replicado en distintas redes de acuerdo a la necesidad empresarial y el personal que lo lleve a cabo, de esta forma, se pretende que el presente trabajo de investigación sirva como un referente para el aseguramiento de equipos y redes en empresas ecuatorianas.

Finalmente, para comprender la estructura del presente documento, se han dispuesto los siguientes capítulos:

- Capítulo I – Se establecen los criterios metodológicos que sustentan el trabajo de investigación realizado.
- Capítulo II – Contiene la teoría relevante a la investigación, es denominado como Marco Teórico.
- Capítulo III – Se muestra en análisis actual de la Empresa, las características y factores de riesgo del segmento de red del Centro de Datos.
- Capítulo IV - Se encuentra la propuesta del marco de referencia y su aplicabilidad al segmento de red del Centro de Datos
- Capítulo V – Muestra las conclusiones, recomendaciones y trabajo futuro del análisis realizado.

1.1. El problema de Investigación

1.1.1. Planteamiento del Problema

La Empresa de Telecomunicaciones, es líder en servicios de internet corporativo a nivel nacional y en los últimos años ha incrementado su catálogo comercial. Actualmente se ofertan servicios de telefonía IP, video seguridad, Centro de Datos y servicios de nube pública.

En nuestros días, la tendencia de las empresas es virtualizar o enviar sus equipos físicos a un Centro de Datos que brinde las capacidades necesarias para soportar una alta transaccionalidad mediante el uso de internet.

Por ello, la Empresa de Telecomunicaciones ha dispuesto dos Centros de Datos modernos que mantiene tecnología de última generación y que son utilizados por áreas internas de la empresa, así como por clientes que en búsqueda de optimización de recursos optan por este tipo de servicio.

El Centro de Datos más grande se encuentra en Guayaquil y se denomina CLOUD CENTER I y el segundo Centro de Datos se encuentra en la ciudad de Quito, los dos están certificados internacionalmente como TIER IV, para el caso de Guayaquil y TIER III para Quito, implementando estándares internacionales para un servicio de alta categoría para sus clientes.

Este crecimiento institucional ha demandado que la Empresa adquiera gran cantidad de equipos y tecnologías para poder soportar las operaciones internas, así como del creciente número de clientes, pero este incremento también aumenta significativamente las brechas de seguridad en la infraestructura, entre las que destacan, accesos no autorizados, fuga de información, denegación de servicio entre otros problemas que ponen en riesgo la continuidad del servicio en los Centro de Datos.

Si estos problemas de seguridad no son identificados oportunamente podrían significar un problema muy serio para la Empresa de Telecomunicaciones quienes podrían perder la

confianza de sus clientes, lo cual impactaría en la imagen institucional adquirida en sus más de 20 años de existencia y que adicionalmente representaría pérdidas económicas al no contar con los rubros mensuales de los clientes que abandonen los servicios institucionales.

Por último, si bien la Empresa ha realizado fuertes inversiones en relación a la adquisición de equipos de alta tecnología, no se ha definido un plan de análisis de vulnerabilidades a todos los segmentos de red corporativos, por lo que no se tiene una visión general de posibles accesos no autorizados que podrían existir debido a vulnerabilidades en los activos de información en redes descuidadas o en desuso.

Esto hace necesaria la creación de un marco de referencia que permita la identificación de los problemas de seguridad basados en los escenarios de riesgos que actualmente afectan a la estabilidad de la Empresa, en donde una intrusión a los Centros de Datos sería muy perjudicial ya que los atacantes podrían extraer información sensible de usuarios, clientes, proveedores y de más stakeholders y reposar en manos de la competencia o en un peor escenario ser vendida en el mercado negro para uso inadecuado por las mafias existentes en internet.

1.1.1.1. Diagnóstico

De forma general, se puede decir que la red que se ha dispuesto evaluar en el Centro de Datos de Quito, es una de las primeras en producción desde la creación de este sitio y no cuenta con una adecuada gestión de riesgos y vulnerabilidades para sus activos de información.

Al tratarse de una red anticuada, es altamente probable identificar problemas relacionados a falta de actualización de servidores, software obsoleto y sin soporte, versiones anticuadas de sistemas operativos, configuraciones por defecto, uso de protocolos inseguros entre otras vulnerabilidades que pueden poner en riesgo la seguridad de las redes empresariales y de clientes configurados en el Centro de Datos.

1.1.1.2. Pronóstico

Las constantes amenazas que se encuentran en internet podrían generar problemas muy serios en la Empresa si no son descubiertos oportunamente por la administración interna de la Empresa y pueda facilitar soluciones a las vulnerabilidades de la infraestructura.

De esta forma, equipos desactualizados podrían ser objetivos de ataques que deriven en accesos no autorizados al servidor poniendo en riesgo la seguridad general de los Centros de Datos, el uso de software anticuado u obsoleto conlleva serios problemas de seguridad ya que en varios casos el fabricante ya no ofrece mantenimiento ni actualizaciones por lo que vulnerabilidades conocidas podrían ser aprovechadas por atacantes para realizar intrusiones en sistemas de forma remota o interna dependiendo el caso, el uso de sistemas operativos considerados en desuso originan un riesgo bastante alto ya que al momento cuentan con muchas vulnerabilidades que son explotables y para las que se han publicado varios códigos de intrusión en internet, en donde el objetivo principales de éstos es acceder remotamente a los equipos o la elevación de privilegios en un activo o en una red corporativa.

En todos los casos previstos, se podría tener una intrusión a la arquitectura del segmento de red y consecuentemente acceder sin autorización al Centros de Datos si las vulnerabilidades identificadas no son atendidas oportunamente, tomando en consideración que los atacantes no descansan y se pueden tener intentos de acceso a cualquier hora y desde cualquier parte del mundo. Adicionalmente, se podría tener una indisponibilidad del servicio del segmento de red, ocasionando una seria afectación a los servicios internos y de clientes que utilizan las plataformas de virtualización.

1.1.1.3. Control del Pronóstico

Debido a que el riesgo de intrusión es alto si no se identifican correctamente las brechas de seguridad, una forma de controlar dicho riesgo es identificando los distintos riesgos asociados a los activos del segmento de red del Centro de Datos y posteriormente

efectuando escaneos continuos de vulnerabilidades hacia la infraestructura de dicha red y así evidenciar de primera mano los problemas relacionados a seguridad que se podría tener. Estos resultados serán utilizados para poder priorizar las acciones de remediación o mitigación, aplicando un marco de referencia que reúna características de metodologías líderes y vigentes que son utilizadas globalmente por empresas y profesionales especializados en pruebas de seguridad informática. Finalmente, el marco metodológico propuesto cambiará la forma en que se evalúan las vulnerabilidades en la Empresa, ya que las actividades internas de identificación de debilidades se ejecutarán de forma proactiva frente a las actividades actuales que son mayormente reactivas al suscitarse un evento de seguridad.

Adicionalmente, se puede definir nuevas políticas internas asociadas a estándares internacionales como por ejemplo ISO 27001 para la protección de equipos y servidores, procesos de hardening de servidores previo a la salida a producción, implementación de sistemas para el control de acceso a equipos y servidores, y por último la implementación de un proceso continuo de administración de eventos e incidentes en donde personal operativo vigile constantemente las alertas de los equipos internos de los Centros de Datos.

1.2. Formulación del Problema

Por el surgimiento de ataques informáticos hacia infraestructura desatendida, la Empresa no quiere estar involucrada en estos temas altamente perjudiciales que considera su mayor problema de seguridad ya que si la infraestructura de los Centros de Datos fuese comprometida, generaría una degradación en los servicios ofertados por la Empresa e impactaría negativamente a la imagen institucional.

Por estas razones, la Empresa ha visto la necesidad de llevar a cabo una evaluación de los riesgos y debilidades existentes en un segmento de su red corporativa ubicada en el Centro de Datos de Quito, aplicando técnicas detalladas en las principales metodologías de pruebas de seguridad informática y de esta forma conformar un marco metodológico que se pueda re-

utilizar para identificar y mitigar brechas de seguridad en otros segmentos públicos o privados y así evitar situaciones similares a las descritas en párrafos anteriores.

1.2.1. Objetivo General

Diseñar un marco de referencia de gestión de vulnerabilidades para un segmento de red corporativo del Centro de Datos de una Empresa de Telecomunicaciones en Quito basado en las principales metodologías de seguridad informática que sirva de estándar para la validación de debilidades en la infraestructura de dicha Empresa.

1.2.2. Objetivos Específicos

- Describir las mejores metodologías usadas para pruebas de vulnerabilidades mediante el análisis de modelos internacionales que permitan el diseño del marco de referencia para el segmento de red en el Centro de Datos de Quito.
- Identificar las vulnerabilidades existentes en el segmento de red corporativo del Centro de Datos de la Empresa en Quito, mediante escaneos automáticos que permitan la clasificación de vulnerabilidades.
- Desarrollar una matriz de escenarios de riesgos con las principales amenazas que posee el Centro de Datos para análisis del impacto de indisponibilidad de servicio en el segmento de red dispuesto por la administración de la Empresa.
- Diseñar la propuesta de referencia que utilice como base fundamental los análisis de riesgos y vulnerabilidades que permitan mitigar los problemas identificados en el segmento de red de la Empresa.

1.2.3. Justificación

El presente documento servirá para el fortalecimiento de la postura de seguridad del segmento de red y de los equipos existentes en el Centro de Datos de Quito de la Empresa de Telecomunicaciones, validando las brechas de seguridad existentes mediante técnicas propuestas por metodologías internacionales y proponiendo un marco de referencia que puede ser replicado en otras redes internas o puede ser adoptado por otras empresas nacionales. Técnicamente el proyecto es viable ya que se han utilizado documentos de libre distribución y herramientas para pruebas de vulnerabilidades que se encuentran disponibles en repositorios de sistemas operativos de código abierto.

Para conformar el marco de referencia, se han seleccionado las mejores metodologías de seguridad informática que son altamente reconocidas internacionalmente y que han sido adoptadas en distintos Centros de Datos para la mejora en la identificación de brechas de seguridad en sus redes internas.

1.2.4. Alcance

El marco de referencia propuesto en el presente trabajo de investigación abarca únicamente el análisis a servidores conectados al segmento de red objeto de pruebas y que posee direccionamiento IP tanto privado como público. Quedan excluidos los análisis realizados a equipos de networking siendo estos enrutadores, conmutadores, corta fuegos entre otros.

Las validaciones relacionadas a Denegación de Servicio no son consideradas ya que pueden afectar al correcto funcionamiento de los servicios proporcionados por la red y pueden ocasionar inestabilidad en otras redes del Centro de Datos de Quito.

1.2.5. Estado del Arte

En el Ecuador se han visto múltiples ataques a infraestructuras de varias empresas que han ocasionado problemas a su imagen corporativa o en el peor de los casos han generado

considerables pérdidas económicas. Por ejemplo, en el año 2016 un Banco en el austro ecuatoriano se vio afectado por una vulnerabilidad en el sistema de transaccionalidad bancaria SWIFT que le originó pérdidas de 12 millones de dólares (Trend Micro, 2016) , empresas públicas se han visto afectadas por problemas relacionadas al defacement, o cambio de imagen de la página principal (El Comercio, 2012), incluso un ex presidente sufrió de accesos no autorizados a sus redes sociales (El Telégrafo, 2014), causando mala propaganda al gobierno.

Un proceso de gestión de vulnerabilidades controlado tiene varias ventajas que pueden ser de gran ayuda para las instituciones, el documento escrito por (Carvajal, 2013) afirma que "La evaluación de la seguridad de un sistema por parte de un analista busca responder 3 preguntas básicas: ¿Qué puede ver un intruso en los sistemas atacados?, ¿Qué puede hacer un intruso con esa información?, ¿Hay alguien en el sistema atacado que se dé cuenta de los ataques o éxitos del intruso?" (p. 1)

Esta perspectiva puede aplicarse a cualquier entorno informático en donde los administradores busquen minimizar las afectaciones por parte de intrusiones a sus redes de datos, pero debido al crecimiento tecnológico que se ha visto en los últimos años, casi todas las instituciones han migrado sus operaciones a un lugar más amplio, y en muchas ocasiones que se encuentren fuera de sus instalaciones en los denominados Centros de Datos (Data Center), teniendo como premisa que se trata de un espacio muy importante para las empresas por lo que de acuerdo a lo indicado por Viteri (2013, pág. 14) "Es de prioridad para el Data Center de la institución, proteger la información mediante políticas y controles de Seguridad Informática para no encontrarse con dificultades ante amenazas constantes que afectan a los sistemas, o si los afectan no causen mayor impacto dentro de la organización."

Por ello, la importancia en tener control y conocimiento de posibles problemas relacionados a seguridad en las redes de los Centro de Datos es una de las principales

preocupaciones para los administradores y consecuentemente para los clientes que utilizan estos servicios.

De acuerdo a (Torres, 2010), existen distintos tipos de ataques que se pueden llevar a cabo en un Centro de Datos, por lo cual.

> "*A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema*" (p.55).

Pero todo esto carecería de sentido si, quien contrata o solicita estos servicios de auditoría especializada, no tiene claro el escenario de lo que en realidad desea obtener, es por ello que Pandey, Brijesh & Singh, Alok & Balani, Lovely (2015) formula tres preguntas esenciales: "¿Qué estás intentando proteger?, ¿Contra qué estás intentando proteger?, ¿Cuánto tiempo, esfuerzo, y dinero estás dispuesto a gastar para obtener una protección adecuada? " (p.3).

Estas simples preguntas ayudan a entender de mejor forma las necesidades internas y así poder brindar una guía adecuada en la identificación de debilidades en la red y proponer sus mitigaciones.

CAPÍTULO II

MARCO TEÓRICO

2.1. Data Center

Un *Data Center* o también denominado Centro de Datos, es un lugar que contiene determinadas características físicas de refrigeración, redundancia y seguridad, cuyo objetivo es alojar todo el equipamiento tecnológico de la Empresa, brindando seguridad y confiabilidad. Todas estas condiciones aseguran la disponibilidad de los servicios de red. (Pacio, 2014)

En estos centros de datos se almacenan toneladas de información y se procesan cantidades gigantes de información cada segundo, tan solo basta con imaginar el procesamiento y almacenamiento del Centro de Datos de empresas gigantes como son Google, Facebook y Amazon solo por nombrar algunos, que son compañías que tienen millones de usuarios al rededor del mundo y que su información es muy sensible y debe ser debidamente resguardada. En el Ecuador, empresas de telecomunicaciones han implementado sus propios Centros de Datos con la finalidad de que clientes locales no tengan que incurrir en costos elevados al contratar servicios en el exterior y en su lugar pueda tener una gestión más cercana y así responder oportunamente a las necesidades del mercado tecnológico.

Adicionalmente, con la creciente adopción del uso de la virtualización, los tradicionales Centros de Datos, donde se almacenaban cientos de equipos físicos, ahora han evolucionado y han constituido una nueva forma de ofrecer sus servicios implementando el denominado *Cloud Computing*, en donde los servicios de los clientes residen en equipos de virtualización en un denominado *Data Center Virtual,* el cual debe tener las mismas características de disponibilidad, integridad y confidencialidad como si se tratase de una implementación clásica.

Internacionalmente, a los Centros de Datos se los han clasificado de acuerdo a las capas de redundancia que tengan a su disposición, generalmente se lo ha escuchado con el

nombre de TIER, que fue una categorización ideada por el *Uptime Institute* el cual se encuentra formalizado en el estándar ANSI/TIA-942 el cual hasta la fecha de escritura del presente documento cuenta con 4 categorías que son:

- TIER I - Centro de Datos básico (99.67% de disponibilidad)

  Es un Data Center considerado básico y que puede ser susceptible a indisponibilidad del servicio ya sea por actividades planificadas como no planificadas.

  Los componentes básicos de este Data Center son:

  - Sistemas de aire acondicionado y distribución de energía.
  - Puede o no tener piso falso.
  - UPS o generador eléctrico.
- TIER II – Centro de Datos redundante (99.74% de disponibilidad)
  - Es un Centro de Datos que tiene componentes redundantes, esto lo convierte en un sitio un poco menos susceptible a interrupciones, mantiene los mismos componentes que tiene la Capa I adicionando al menos un sistema de contingencia de cada componente de la infraestructura.
- TIER III – Centro de Datos concurrentemente mantenibles (99.98% de disponibilidad)
  - Este tipo de Data Center cuenta con las capacidades técnicas para que se realicen actividades planificadas en cualquier componente de la infraestructura sin llegar a tener afectación a la operación. En esta capa, actividades realizadas sin previa planificación, descuidos o errores en las operaciones o fallas en alguno de los componentes del Centro de Datos, aún podrían ocasionar interrupción en el servicio brindado.
- TIER IV – Centro de Datos tolerable a fallos. (99.999% de disponibilidad)
  - Es un Data Center en donde se puede realizar cualquier actividad planificada sin interrupciones, también es tolerante a fallos o ante algún evento crítico no planificado.

2.2. Metodologías de Seguridad Informática

En este apartado se muestran las principales metodologías relacionadas a pruebas de vulnerabilidades, mostrando su aplicabilidad en distintos escenarios los cuales servirán posteriormente para el diseño del marco de referencia propuesto.

2.2.1. Metodología OSSTMM

OSSTMM (The Open Source Security Testing Methodology Manual), es una metodología de seguridad informática de distribución libre, es mantenida y desarrollada por la empresa ISECOM (Institute for Security and Open Methodologies), quienes además cuentan con procesos de certificación para pentesters y profesionales relacionados a seguridad para que cuenten con las habilidades necesarias para llevar a cabo auditorías con los lineamientos detallados en sus guías.

Actualmente, la metodología se encuentra en la versión número cuatro, pero aún es un documento que no se ha realizado su publicación oficial (también considerado como versión beta) y que se encuentra en revisiones finales, por lo que la versión estable y recomendada para ejecución de auditorías es la número tres.

La metodología está disponible para su descarga en el sitio oficial de ISECOM (www.isecom.org)

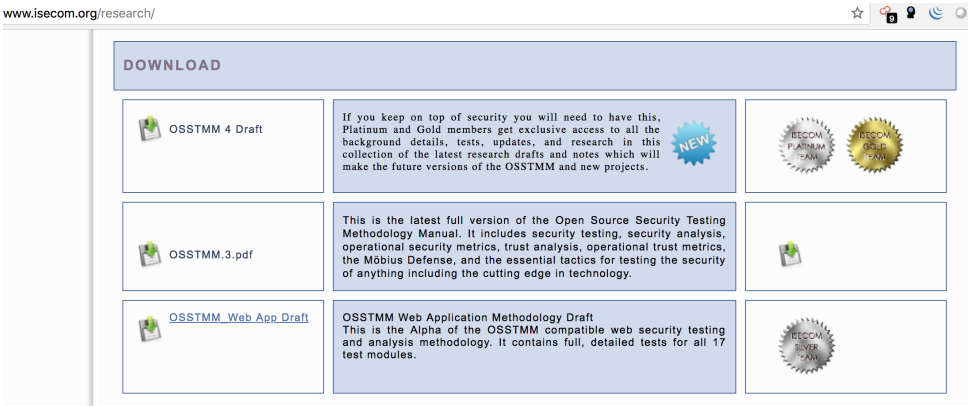


Figura 1. Sitio Oficial de OSSTMM
Fuente: www.isecom.org

Este tipo de metodología se ha convertido en casi un estándar que ha sido adoptado por varios especialistas de seguridad internacionalmente, esto se debe principalmente al orden de las pruebas que se proponen y la facilidad de acceso a la información.

Para tener una idea global, la metodología OSSTMM divide sus ámbitos de pruebas de la siguiente forma:

- Seguridad de la Información
    - Inteligencia Competitiva
    - Revisión de Privacidad
    - Recolección de Documentos
- Seguridad de los Procesos
    - Pruebas de Solicitud
    - Pruebas de Sugerencia dirigida
    - Pruebas de Personas Confiables
- Seguridad en las Tecnologías de Internet
    - Logística y Controles
    - Exploración de la Red
    - Revisión de Privacidad
    - Verificación de Vulnerabilidades
    - Detección de Intrusos
    - Contingencia
    - Denegación de Servicios
- Seguridad en las Comunicaciones
    - Pruebas de PBX
    - Pruebas de Correo de Voz
    - Revisión del FAX
    - Pruebas del Módem

- Seguridad Inalámbrica
    - Redes Inalámbricas
    - Redes Bluetooth
    - Dispositivos de Entrada Inalámbricos
    - Dispositivos de Vigilancia Inalámbricos
    - RFID
    - Sistemas Infrarrojos
- Seguridad Física
    - Perímetro
    - Controles de Acceso
    - Alarmas
    - Ubicación
    - Entorno

Los canales y secciones que se encuentran en esta metodología se describen a continuación:

Tabla 1. Clases y Canales de OSSTMM
Fuente: Metodología OSSTMM

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Se enfoca en el elemento humano, donde la interacción puede ser física o sicológica
	Físico	Comprende cualquier prueba a objeto tangible, no necesariamente con medios electrónicos.
Seguridad del Espectro Electromagnético (SPECSEC)	Inalámbrico	Comprende las comunicaciones que se realizan mediante medios inalámbricos utilizando los espectros asignados a ellos.

Seguridad de las comunicaciones	Redes de Datos	Comprende a sistemas electrónicos y redes de datos que son interconectados mediante cables.
	Telecomunicaciones	Comprende comunicaciones análogas y digitales

También existe un documento de pruebas enfocadas únicamente a sitios web, de esta forma OSSTMM garantiza que se realicen pruebas esenciales en distintos equipos y servicios y de esta forma validar aspectos importantes de seguridad en una institución.

2.2.2. Metodología ISSAF

ISSAF (Information Systems Security Assessment Framework) es una metodología propuesta y diseñada por OISSG (Open Information Systems Security Group), similar a OSSTMM, es de distribución libre y al momento de la escritura del presente documento cuenta con tres guías que son:

- ISSAF versión 0.2.1 (Full release)
- ISSAF version 0.2.1 A (Non-Technical chapters)
- ISSAF version 0.2.1 B (Technical chapters)

Esta metodología se enfoca en la validación de los siguientes controles:

- Evaluar la política de seguridad implementada en la organización junto a sus procesos y así reportar faltas a su cumplimiento de acuerdo a estándares de tecnología, leyes locales y requerimientos regulatorios.
- Identificar y evaluar las dependencias del negocio en servicios de infraestructura proporcionados por TI.

- Llevar a cabo evaluaciones de vulnerabilidad y pruebas de penetración para resaltar las vulnerabilidades del sistema que podrían generar riesgos potenciales para los activos de información.
- Especificar los modelos de evaluación por los dominios de seguridad a:
    - Identificar configuraciones erróneas y solucionarlas.
    - Identificar los riesgos relacionados con las tecnologías y abordarlos.
    - Identificar los riesgos entre las personas y procesos de negocios y abordarlos.
    - Fortalecimiento de procesos y tecnologías existentes.
    - Proporcionar mejores prácticas y procedimientos para respaldar las iniciativas de continuidad del negocio.

2.2.3. Metodología OWASP

OWASP (Open Web Application Security Project), es una metodología para pruebas de seguridad en aplicaciones web, toda la documentación, herramientas e investigaciones realizadas son de libre acceso por lo cual OWASP ha sido muy bien aceptada por varios profesionales de seguridad, también ha sido adoptada por distintos fabricantes de equipos de seguridad en donde se hace referencia a protecciones del top 10 de vulnerabilidades web, también denominado OWASP TOP 10.

Este top 10 de vulnerabilidades, pretende mostrar las diez vulnerabilidades más relevantes en sitios web y que pueden poner en serio riesgo la seguridad de una institución en caso de ser aprovechada por un atacante.

Al momento de la realización del presente documento, la versión de OWASP Top 10 corresponde al año 2017, en donde existen algunos cambios en relación a su antecesora que fue publicada en el año 2013, sin embargo, se puede visualizar que la principal vulnerabilidad en sitios web es la inyección de código, por lo que las empresas deben tener especial cuidado en poder identificarlo y mitigarlo para evitar problemas de intrusiones o robo de información.

En la siguiente ilustración se puede apreciar las diferencias entre la versión de OWASP Top 10 de los años 2013 y 2017.

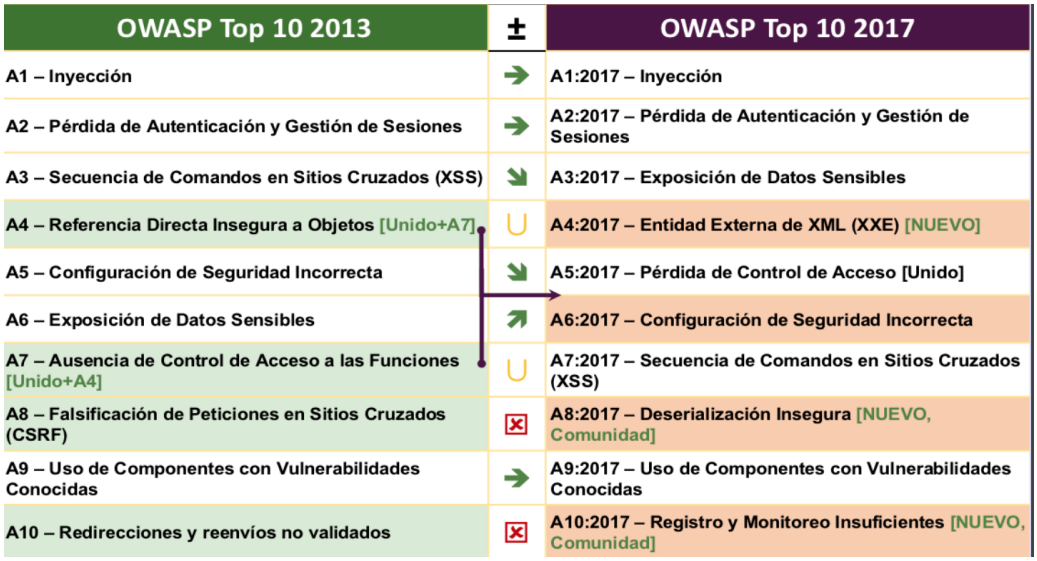


Figura 2. Diferencias entre OWASP Top10 2013 y 2017
Fuente*:* Sitio web de OWASP

Adicionalmente al OWASP Top 10, esta organización también tiene otros documentos relacionados a pruebas de seguridad como se muestran en las siguientes líneas:

- OWASP Application Security Verification Standard Project
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP AppSensor Project
- OWASP Testing Project

Generalmente, el documento más utilizado es OWASP Testing Project ya que contiene los pasos necesarios para validar las vulnerabilidades en aplicaciones web, iniciando desde lo más básico hasta técnicas complejas que permitan accesos no autorizados. Actualmente este documento se encuentra en la versión 4 e incluye una versión en español liberada por la Escuela Politécnica Nacional (EPN) del Ecuador. (Open Web Application Security Project, 2015)

2.2.4. Metodología PTES

Esta metodología cuyas siglas significan Penetration Testing Execution Standard, es una guía técnica que ayuda en el proceso de test de intrusión ya que define los pasos y herramientas requeridas en cada fase del ciclo de pruebas de vulnerabilidades.

Esta metodología presenta un lenguaje de fácil entendimiento, de tal forma que personal de mando gerencial pueda comprender las vulnerabilidades y los métodos de explotación llevadas a cabo por el equipo auditor, también presenta varios enlaces y herramientas recomendadas para las distintas fases lo cual la convierte en una metodología simple de comprender por personas técnicas y no técnicas.

2.2.5. Metodología NIST.

La NIST (National Insitute of Standards and Technology), es una entidad del gobierno de Estados encargada en publicar sus estándares nacionales.

Esta entidad ha publicado distintos documentos relacionados a seguridad informática entre los cuales se encuentra NIST SP 800-115 que es el documento que se encarga de guiar a un equipo auditor en la ejecución de pruebas de vulnerabilidad.

De acuerdo a lo descrito en la NIST 800-115, las pruebas ahí descritas pueden utilizarse para validar lo siguiente:

- Como el sistema tolera patrones de ataque del mundo real.
- Que tan sofisticado debe ser un ataque para comprometer con efectividad el sistema evaluado.
- Las medidas adicionales que se deben utilizar para mitigar las amenazas contra el sistema evaluado.
- Comprobar la habilidad del personal de defensa para responder apropiadamente a los ataques realizados.

Finalmente, esta guía se considerada como un documento que contiene las pautas de auditoría de manera muy general, por lo cual no se abordan de manera específica las técnicas y procedimientos que un atacante o analista de vulnerabilidades debe llevar a cabo contra los activos de información.

2.3. Controles de Seguridad de CIS

El Center for Internet Security (CIS) es una organización basada en Estados Unidos conformada por una comunidad de profesionales relacionados a seguridad informática y que incluyen otros actores clave en el ámbito de ciberseguridad, como entidades de gobierno, empresas de tecnología, entre otros.

Esta organización ha desarrollado un conjunto de 20 controles críticos de seguridad que se recomienda adoptar para conformar una protección más robusta para los activos de información de una empresa, de esta forma se espera que se sigan una serie de validaciones que faciliten la gestión de seguridad sobre los equipos e información que posee la Empresa.

Los controles están organizados en tres grupos en donde se analizan aspectos básicos empresariales, aspectos fundamentales de seguridad, y controles organizacionales de acuerdo a la siguiente ilustración.

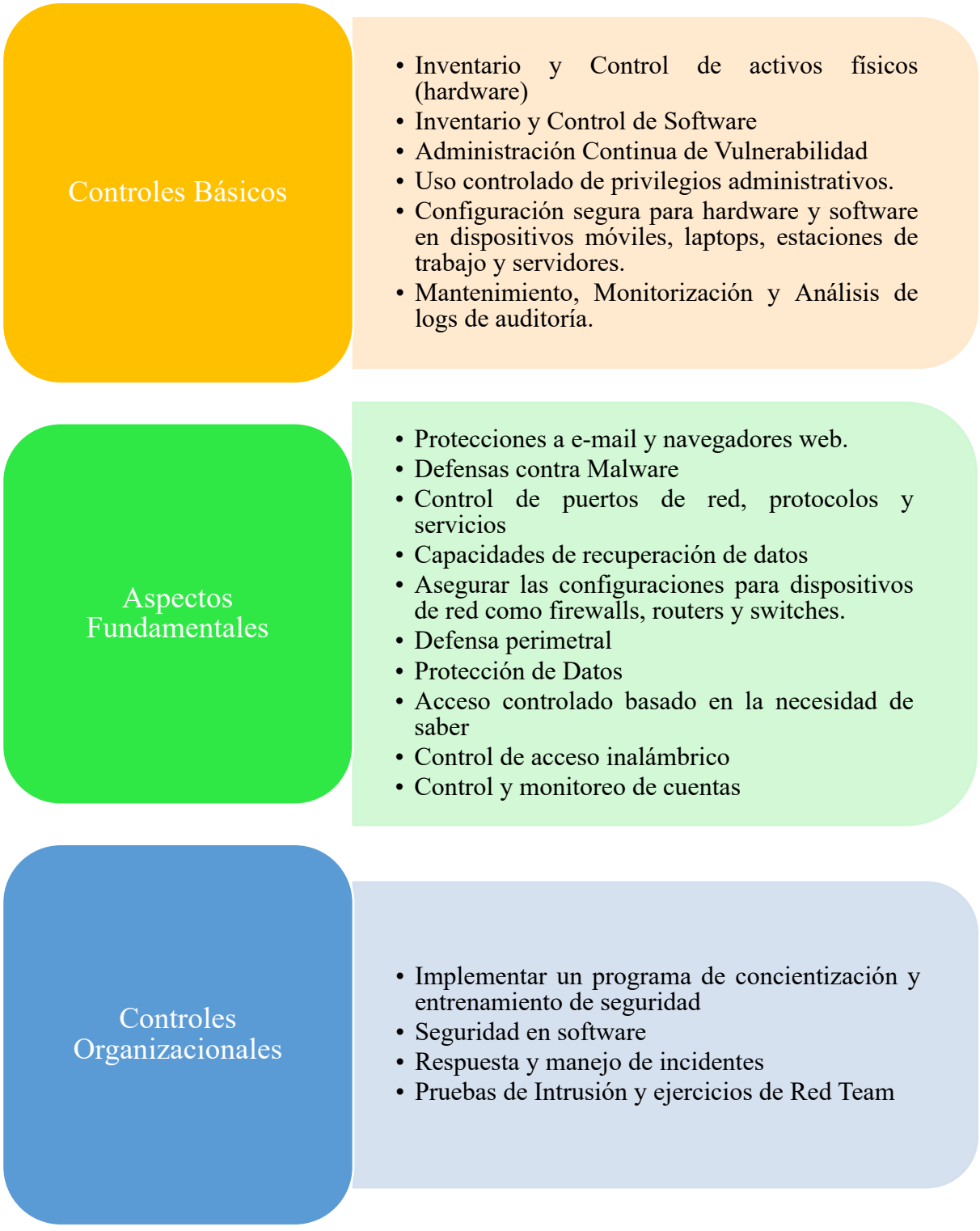


Figura 3. Controles de CIS

Fuente: Elaborada por el investigador

Estos controles no están enfocados únicamente a Centro de Datos ya que pueden ser adoptados en muchas instituciones con variados procesos organizacionales ya queya que, al partir desde la identificación de activos, involucra no sólo a personal técnico sino que el

campo de acción conlleva al compromiso institucional de todo los trabajadores de la Empresa. Finalmente, los controles de CIS facilitan la armonía con otras normas de seguridad como es ISO 27001, en donde se trabaja con plantillas y evaluaciones muy similares que ayudan en el proceso de validación por parte de entidades auditoras.

2.4. Modelos Internacionales de Hackeo Ético

En la actualidad, empresas internacionales dedicadas a la educación y certificación de profesionales han diseñado modelos que sirven de guía para profesionales de seguridad informática a realizar auditorías relacionadas a hackeo o pruebas de vulnerabilidades siguiendo ciertos pasos para obtener resultados fiables que puedan ser presentados en un informe final al cliente o contratista.

2.4.1. Modelo por CEH

Certified Ethical Hacker (CEH), es una certificación internacional elaborada por la empresa EC-Council y que ha ganado gran reconocimiento tanto local como a nivel mundial por ser un título que valida los conocimientos necesarios para realizar auditorías de seguridad relacionados a Hackeo Ético.

CEH propone un modelo de hackeo en donde se encuentran 5 fases principales como se muestra en la siguiente figura.

Figura 4. Modelo de hacking ético por CEH
Fuente: Elaborada por el investigador

En este modelo, el análisis de vulnerabilidades se encuentra en el proceso de Escaneo, en donde se sugieren distintas herramientas para este propósito.

2.4.2. Modelo por SANS

SANS Institute, es una entidad internacional que agrupa a varios profesionales relacionados al mundo de seguridad informática y que además ofrece cursos y certificaciones internacionales que en los últimos años han ganado alto prestigio por su complejidad y aplicabilidad en distintos escenarios.

SANS propone un modelo de pruebas de intrusión que se basa en el siguiente flujo

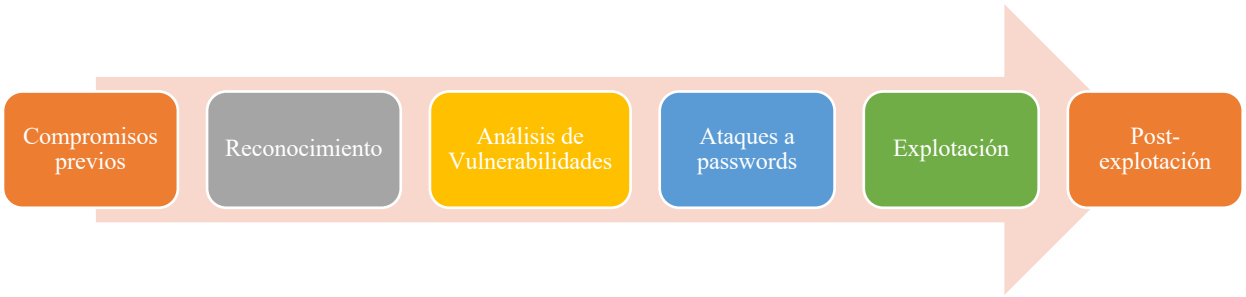


Figura 5. Modelo de hacking ético por SANS
Fuente: Elaborada por el investigador

2.5. Marco Legal en el Ecuador

En el Ecuador, los accesos no autorizados a sistemas informáticos están penalizados por la ley y la aplicación de las penas de privación de libertad están incluidas en el Código Orgánico Integral Penal (COIP).

De acuerdo a Carla Pérez en el artículo escrito en el portal web de la Policía Nacional, indica que los delitos informáticos que al momento son reconocidos en el Ecuador son: (Pérez, 2017)

- Pornografía infantil – 13 a 16 años de prisión.
- Violación del derecho a la intimidad – de uno a tres años de prisión

- Revelación ilegal de información de bases de datos – de uno a tres años de prisión
- Interceptación de comunicaciones – de tres a cinco años de prisión
- Pharming y Phishing – de tres a cinco años de prisión
- Fraude informático – de tres a cinco años de prisión
- Ataque a la integridad de sistemas informáticos – de tres a cinco años de prisión
- Delitos contra la información pública reservada legalmente – de tres a cinco años de prisión
- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones – de tres a cinco años de prisión.

En la estructura del COIP, la Sección Tercera corresponde a "Delitos contra la seguridad de los activos de los sistemas de información y comunicación" y los artículos incluidos son los siguientes:

- Artículo 229.- Revelación ilegal de base de datos.
- Artículo 230.- Interceptación ilegal de datos.
- Artículo 231.- Transferencia electrónica de activo patrimonial.
- Artículo 232.- Ataque a la integridad de sistemas informáticos.
- Artículo 233.- Delitos contra la información pública reservada legalmente.
- Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Por otro lado, la Superintendencia de Bancos, entidad que regula a las entidades financieras en el Ecuador en el año 2014 publicó la resolución 3066 en donde se exige a estas instituciones a realizar al menos un test de vulnerabilidades por año, esto se encuentra

descrito en el artículo 22, apartado 8 de dicho documento (Resolución JB-2014-3066, 2014) en el cual se indica lo siguiente:

> "*ARTÍCULO 22: Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente:*
>
> *22.8 – Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las instituciones deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas.*" (p. 13)

CAPÍTULO III

ANÁLISIS SITUACIONAL

3.1. Generalidades

Actualmente, la Empresa de Telecomunicaciones es líder en el servicio de conectividad de fibra óptica a nivel nacional, y en los últimos años ha logrado expandirse a otros países de la región procurando mantener los mismos estándares de calidad que lo han distinguido en el Ecuador.

La Empresa cuenta con presencia nacional (oficinas) en las principales ciudades de Ecuador, en donde la oficina matriz se encuentra en Guayaquil y la sucursal principal en Quito.

Internacionalmente, cuenta con oficinas en Colombia, Panamá y Guatemala, en donde se ofertan principalmente servicios de interconexión de fibra óptica y otros servicios gestionados.

Al momento la Empresa cuenta distintas líneas de negocio, que se ofertan en todos los lugares donde tiene representación, entre las que se encuentran:

- *Collaboration*, que se encarga de brindar servicios de comunicaciones mediante tecnología de video conferencia o voz sobre IP.
- *Network,* encargada de servicios para gestión de redes LAN.
- *Cloud,* donde se encuentran los servicios de web hosting, backup, IaaS[1], SaaS[2]
- *Connectivity,* servicio clásico de internet y datos.

[1] IaaS - Infrastructure as a service
[2] SaaS - Software as a service

3.2. El Segmento de Red

El Centro de Datos (Quito) de la Empresa de Telecomunicaciones es considerado uno de los más importantes a nivel nacional, en este lugar se han dispuesto no solo equipos para la operación de la Empresa, también en él se encuentran equipos que ofrecen servicios críticos a empresas de distinto giro de negocio.

Debido a la necesidad de colocar servicios en un centro alterno u ofrecer funcionalidades en la nube, la distribución de redes internas en el Centro de Datos ha sufrido considerables cambios a lo largo de los años que se encuentra en funcionamiento, es por ello que la administración de la Empresa ha identificado un segmento de red privado en donde están equipos que son utilizados para determinados servicios internos y en donde no se han ejecutado planes de gestión de vulnerabilidad continua para la identificación y solución de brechas de seguridad.

Dicho segmento de red corresponde a una implementación que fue realizada al inicio de las operaciones del Centro de Datos, por lo cual se estima que no tiene un sistema robusto de seguridades lógicas y físicas, mismas que pueden ser aprovechadas para ganar acceso a equipos relevantes de la Empresa o en su defecto para generar indisponibilidad en los servicios.

Este segmento de red, como fue comentado en el primer capítulo, mantiene servicios de correo electrónico, sitios web, y repositorios internos cuyos responsables de la gestión preventiva y correctiva son distintas áreas internas de la Empresa entre las que se pueden nombrar Networking, IT, Sistemas y Seguridad Informática.

Por la importancia de los servicios que se encuentran en el Centro de Datos, la divulgación de redes privadas o públicas no está permitido por la administración de la Empresa, por lo que la nomenclatura utilizada para la red dispuesta será 192.168.1.0/24, siendo de esta forma utilizada únicamente para fines didácticos en el presente documento, esto con la finalidad de mantener la confidencialidad de redes y direcciones IP de la Empresa.

Una representación gráfica del segmento evaluado se puede visualizar en la figura 6, en donde se encuentra configurado en la VLAN a y VLAN b del Centro de Datos. Cabe aclarar que los servidores configurados en VLAN b no poseen direccionamiento IP público configurado directamente en sus tarjetas de red, en su lugar se utiliza direccionamiento privado y para el acceso desde internet se ha realizado implementaciones de DNAT en el firewall perimetral.

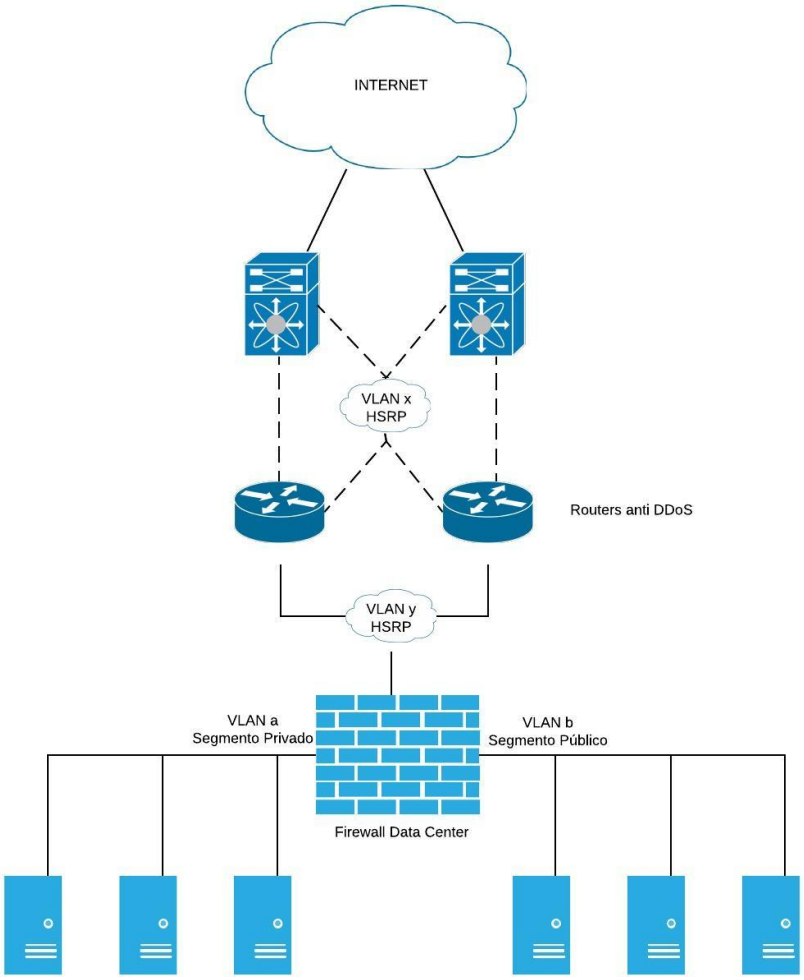


Figura 6. Diagrama del Segmento de Red
Fuente: Elaborada por el investigador

3.2.1. Activos de Información

De forma general, se puede mencionar que en el segmento de red se encuentran equipos que ofrecen servicios de correo electrónico, consolas de virtualización, portales de gestión documental, sitios web entre otros servicios que principalmente están configurados en equipos con sistema operativo Linux y una reducida cantidad con Windows.

Es importante conocer que para las soluciones de las debilidades o problemas identificados, la Empresa ha definido en sus políticas internas que los dueños o responsables de los activos sean los encargados de realizar estas remediaciones, siempre de la mano del área de seguridad informática quienes envían los reportes de vulnerabilidades y las mitigaciones correspondientes para defender los activos del segmento de red.

Finalmente, los activos de información deben estar bien identificados y ser mantenidos en un listado que permita conocer sus características principales como la dirección IP, sistema operativo y puertos habilitados, en la Empresa existe un sistema interno para la gestión de activos, donde las áreas involucradas son las responsables de actualizar el listado que es utilizado para distintos fines auditables.

Un ejemplo obtenido desde el sistema de registro de activos se puede observar en la tabla 2, en donde se muestran las principales características que ayudan a identificar a los activos del segmento de red.

Tabla 2. Registro de Activos por Área
Fuente: Elaborada por el investigador

Nombre de Host	**Dirección IP**	**Puertos**	**Sistema Operativo**	**Responsable**
correo1.empresa.net	192.168.1.101	tcp/25, tcp/80, tcp/110, tcp/135, tcp/143, tcp/443,	Linux	IT

		tcp/7071		
correo2.empresa.net	192.168.1.102	tcp/21, tcp/25, tcp/80, tcp/110, tcp/135, tcp/143, tcp/443, tcp/7071	Linux	IT
nfs.empresa.net	192.168.1.24	tcp/22, tcp/80, tcp/139, tcp/443, tcp/445	Windows	Networking
webhosting3.empresa.net	192.168.1.7	tcp/21, tcp/25, tcp/80, tcp/110, tcp/135, tcp/143, tcp/443	Windows	IT
dbzuio.empresa.net	192.168.1.31	tcp/22, tcp/80, tcp/443, tcp/3306	Linux	Sistemas
dbzuiobck.empresa.net	192.168.1.32	tcp/22, tcp/80, tcp/443, tcp/3306	Linux	Networking
intra.empresa.net	192.168.1.55	tcp/80, tcp/443	Linux	IT
av.empresa.net	192.168.1.200	tcp/139, tcp/445, tcp/3389	Windows	HelpDesk
portales.empresa.net	192.168.1.156	tcp/80, tcp/135, tcp/143, tcp/443	Linux	IT

3.3. Matriz de Riesgos para el Segmento Evaluado

Desde la proliferación de ataques informáticos y con las estadísticas mundiales de desastres naturales, las empresas han adquirido la suficiente madurez administrativa para reconocer potenciales peligros que puedan amenazar sus operaciones, por lo cual el personal

involucrado en evaluaciones de riesgo analiza, desarrolla y evalúa continuamente distintos escenarios que puedan afectar a la Empresa.

Para este apartado, se ha conformado una matriz de riesgos tecnológicos en donde se muestran las posibles amenazas que pondrían generar problemas relacionados a indisponibilidad de servicio, ataques informáticos, robo de credenciales y otras debilidades que puedan ser aprovechadas contra el Centro de Datos de Quito, tomando como puerta de acceso el segmento de red evaluado.

La matriz se encuentra agrupada por los distintos escenarios de riesgo, de tal forma que facilite la identificación de las amenazas y así poder dar el tratamiento adecuado.

De forma general, se puede decir que el riesgo es medido mediante la multiplicación de la probabilidad de ocurrencia por el impacto que ocasiona la amenaza si se materializa en los activos de la Empresa. Para la ponderación de la probabilidad de ocurrencia se ha determinado el uso de la siguiente nomenclatura:

- **B (Probabilidad Baja) -** El evento posiblemente ocurra en cualquier momento (poca probabilidad de ocurrencia)
- **M (Probabilidad Media) –** El evento probablemente ocurrirá en la mayor parte de las situaciones.
- **A (Probabilidad Alta) -** Existe una alta probabilidad que el evento ocurra

De igual forma, la nomenclatura utilizada para la ponderación del impacto se ha utilizado lo siguiente:

- **L (Impacto Bajo) -** Si el evento llega a presentarse, el impacto sería bajo en la red.
- **M (Impacto Medio) -** Si el evento se presenta, tendría medianas consecuencias en la red.

- **S (Impacto Alto) –** Si el evento llega a presentarse, las consecuencias serían serias poniendo en peligro la operación.

La siguiente tabla muestra la distribución de Probabilidad e Impacto en un mapa de calor.

Tabla 3. Mapa de Calor de Análisis de Riesgos

Fuente: Elaborada por el investigador

		Probabilidad		
		B (1)	**M (2)**	**A (3)**
Impacto	**L (1)**	BL 11%	ML 22%	AL 33%
	M (2)	BM 22%	MM 44%	AM 66%
	S (3)	BS 33%	MS 66%	AS 100%

Tabla 4. Análisis de Riesgo

Fuente: Elaborada por el investigador

N°	IDENTIFICACION DEL RIESGO		ANALISIS DEL RIESGO							
			PROBABILIDAD			IMPACTO			RESULTADO	CATEGORIA
	Escenario de Riesgo	Riesgo	A (3)	M (2)	B (1)	S (3)	M (2)	L (1)		
1	Pérdida de Energía Eléctrica en Data Center	Indisponibilidad de servicio	3			3			100%	AS
		Acceso no autorizado			1			1	11%	BL
		Corrupción de datos		2			2		44%	MM
		Exfiltración de datos			1			1	11%	BL
		Daño de equipos		2		3			67%	MS
		Robo de credenciales			1			1	11%	BL
		Instalación de puertas traseras			1			1	11%	BL
		Saltos entre VLANs			1			1	11%	BL
2	Hackeo de equipos por Identificación no oportuna de Vulnerabilidades	Indisponibilidad de servicio			1		2		22%	BM
		Acceso no autorizado	3			3			100%	AS
		Corrupción de datos		2			2		44%	MM
		Exfiltración de datos		2		3			67%	MS
		Daño de equipos			1			1	11%	BL
		Robo de credenciales		2		3			67%	MS
		Instalación de puertas traseras		2			2		44%	MM
		Saltos entre VLANs		2		3			67%	MS

3	Hackeo de Servidores y estaciones de trabajo (red interna)	Indisponibilidad de servicio		2			2		44%	MM
		Acceso no autorizado		2		3			67%	MS
		Corrupción de datos		2		3			67%	MS
		Exfiltración de datos		2		3			67%	MS
		Daño de equipos			1		2		22%	BM
		Robo de credenciales			1		2		22%	BM
		Instalación de puertas traseras		2		3			67%	MS
		Saltos entre VLANs			1			1	11%	BL
4	Indisponibilidad de bases de datos de aplicaciones internas	Indisponibilidad de servicio	3			3			100%	AS
		Acceso no autorizado			1			1	11%	BL
		Corrupción de datos		2		3			67%	MS
		Exfiltración de datos		2			2		44%	MM
		Daño de equipos			1			1	11%	BL
		Robo de credenciales		2		3			67%	MS
		Instalación de puertas traseras			1			1	11%	BL
		Saltos entre VLANs			1			1	11%	BL
5	Hackeo de servidores expuestos a Internet	Indisponibilidad de servicio		2			2		44%	MM
		Acceso no autorizado	3			3			100%	AS
		Corrupción de datos		2		3			67%	MS
		Exfiltración de datos	3			3			100%	AS
		Daño de equipos			1		2		22%	BM
		Robo de credenciales	3			3			100%	AS
		Instalación de puertas traseras	3			3			100%	AS
		Saltos entre VLANs		2		3			67%	MS

6	Hackeo de aplicaciones web desde internet	Indisponibilidad de servicio		2		3			67%	MS
		Acceso no autorizado		2		3			67%	MS
		Corrupción de datos			1		2		22%	BM
		Exfiltración de datos		2			2		44%	MM
		Daño de equipos			1			1	11%	BL
		Robo de credenciales		2		3			67%	MS
		Instalación de puertas traseras		2			2		44%	MM
		Saltos entre VLANs		2			2		44%	BM
7	Indisponibilidad de servicio por operadores de red no capacitados	Indisponibilidad de servicio		2		3			67%	MS
		Acceso no autorizado			1			1	11%	BL
		Corrupción de datos	3			3			100%	AS
		Exfiltración de datos			1		2		22%	BM
		Daño de equipos	3			3			100%	AS
		Robo de credenciales			1			1	11%	BL
		Instalación de puertas traseras			1			1	11%	BL
		Saltos entre VLANs			1			1	11%	BL

Como se puede observar, la matriz de riesgos muestra algunas debilidades que podrían elevar la posibilidad de intrusión al segmento de red. Si bien todos los resultados deben ser atendidos y mitigados, la necesidad de actuar frente a escenarios de riesgos catalogados como Altos (Rojos) y Medios (Amarillos) son de vital importancia ya corresponden a los problemas más serios que afectan la disponibilidad del segmento de red.

Como se puede observar en el siguiente gráfico, la tendencia de los riesgos de categoría Alta apunta principalmente a problemas relacionados a Indisponibilidad de Servicio, Accesos no Autorizados, Corrupción de Datos y Robo de credenciales.

Figura 7 - Riesgos Altos
Fuente: Elaborada por el investigador

Así mismo, los riesgos de categoría Media principalmente apuntan a tomar acciones relacionada a Indisponibilidad de servicio, Instalación de puertas trasera, corrupción y exfiltración de datos.

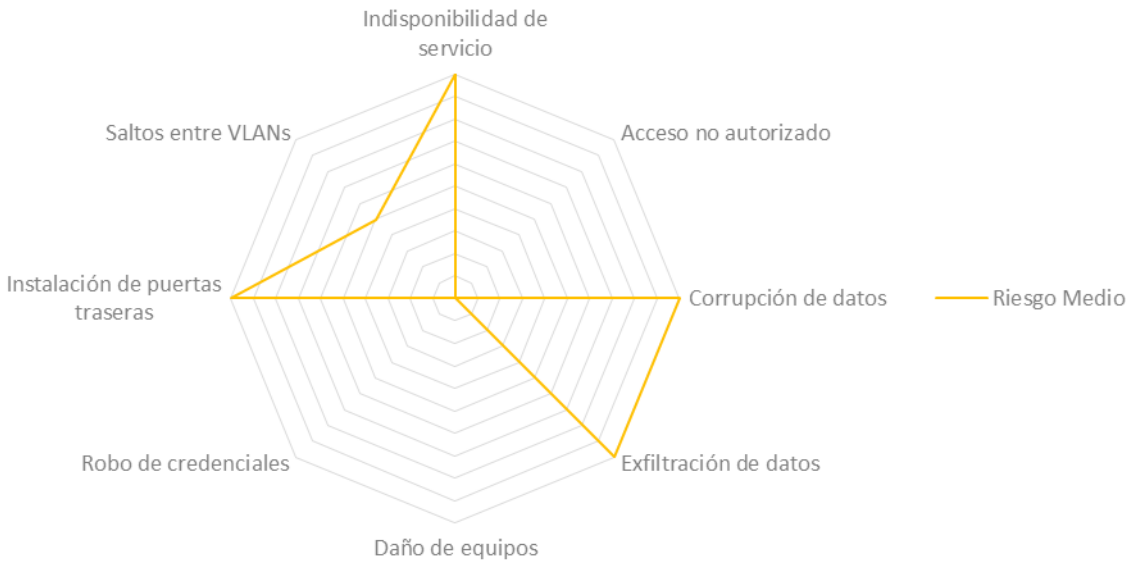


Figura 8 - Riesgos Medios

Fuente: Elaborada por el investigador

En relación al factor humano, es importante mantener campañas de capacitación interna sean estas técnicas y enfocadas a gestión interna, de esta forma se pueden minimizar las afectaciones hacia la infraestructura por parte de operadores que desconozcan no solo de las configuraciones sino también de los procesos que rigen al Centro de Datos. Las amenazas principales para este escenario son Indisponibilidad de Servicio, Corrupción de Datos y Daño de Equipos.

CAPÍTULO IV

PROPUESTA

La información relacionada a la evaluación de riesgos mostrada en el capítulo anterior, evidencian la necesidad de definir una estrategia que facilite el tratamiento de los mismos y así lograr disminuir la cantidad de vulnerabilidades que amenazan la disponibilidad, integridad y confiabilidad de los servicios que están en el segmento de red del Centro de Datos de Quito, por estos antecedentes, el marco de referencia propuesto debe permitir la minimización de brechas de seguridad en la red y consecuentemente la disminución del riesgo al identificar oportunamente debilidades que pongan en riesgo la continuidad de los servicios expuestos por el segmento de red evaluado.

4.1. Modelo de Referencia para el Segmento de Red

Como fue descrito en el capítulo anterior, la red 192.168.1.0/24 es uno de los primeros segmentos configurados en el Centro de Datos de Quito y en donde se encuentran distintos equipos que proveen de servicios importantes para la Empresa, los accesos no autorizados a los activos de esta red suponen un riesgo elevado ya que desde esta red se podría comprometer otros segmentos corporativos y si el atacante ejecuta tareas de escalamiento horizontal de privilegios podría posiblemente llegar a equipos utilizados por clientes, siendo esta una de las máximas preocupaciones para la Empresa.

Por estas razones, para el desarrollo del modelo de referencia se han utilizado conceptos y guías propuestas por las metodologías estudiadas en el Capítulo II, ya que son ampliamente utilizadas por empresas y profesionales relacionados a seguridad informática y que serán empleadas con la finalidad de analizar las vulnerabilidades del segmento de red y así mitigar sus riesgos asociados.

De forma gráfica, se puede resumir al marco de referencia propuesto en 6 grupos principales como se muestra a continuación:

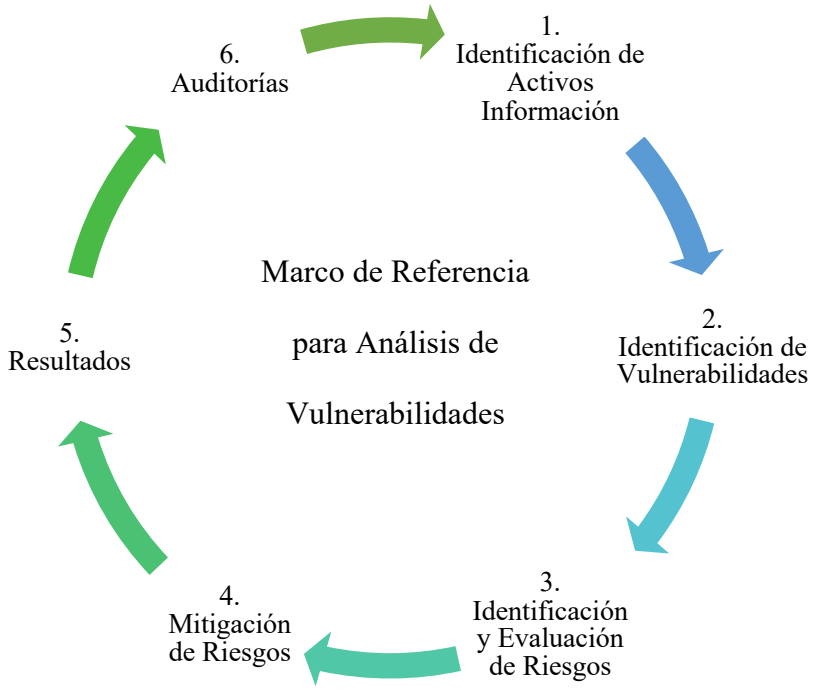


Figura 9. Propuesta de Marco de Referencia

Fuente: Elaborada por el investigador

4.1.1. Identificación de Activos de Información

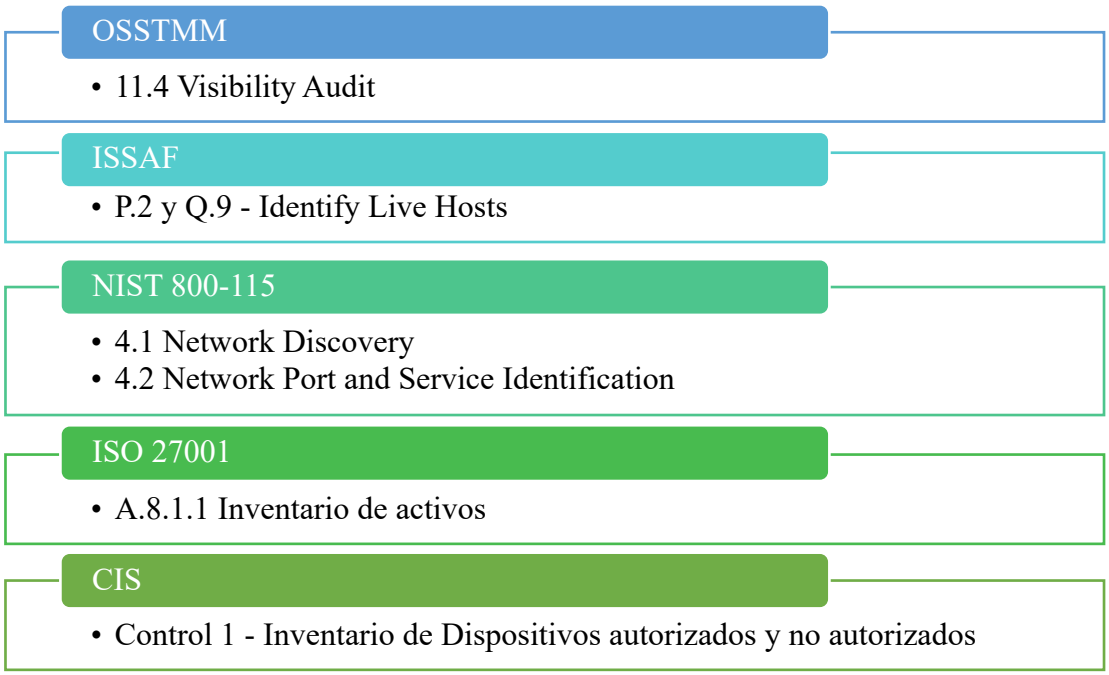
El primer paso para la definición del marco de referencia comprende la identificación de los activos que forman parte del análisis. En este apartado es importante diseñar un listado completo en donde se pueda apreciar características generales de los equipos.

De acuerdo a NIST (National Insitute of Standards and Technology, 2019), "Las organizaciones a menudo utilizan pruebas técnicas y no del todo técnicas para identificar los activos que se desean analizar. Por ejemplo, las empresas pueden mantener un inventario de activos u otras listas que formarán parte de la evaluación." (p.4-1).

Para efectuar descubrimientos automatizados de activos, se pueden ejecutar varias pruebas técnicas que ayudan en este propósito, las metodologías estudiadas proponen diferentes formas para la identificación de dispositivos como se muestra en la siguiente tabla.

Tabla 5. Método de Identificación de Activos

Fuente: Elaborada por el investigador



En general, todas las metodologías proponen actividades muy similares para la identificación de activos, por lo cual, en forma de resumen se puede decir que el modelo de identificación sería de la siguiente forma:

- Ejecutar identificación activa y pasiva.
- Ejecutar ping hacia toda la red.
- Ejecutar descubrimiento de red mediante el uso de la herramienta Nmap.
- Ejecutar enumeración de puertos comunes
- Identificación de sistema operativo.
- Listar hosts descubiertos.

Las herramientas esenciales para este paso son principalmente distribuidas por la comunidad de software libre y pueden ser descargadas desde sus portales oficiales.

4.1.2. Identificación de Vulnerabilidades

Después del descubrimiento de los activos existentes en el segmento de red, el segundo paso es la identificación de vulnerabilidades sobre estos equipos, para ello se utiliza un escáner automatizado y se configuran escaneos periódicos para validar la existencia de nuevas vulnerabilidades. El proceso de análisis de vulnerabilidades de acuerdo a CIS (CIS, 2018) afirma que:

> "*Las organizaciones que no buscan vulnerabilidades y abordan de manera proactiva las fallas detectadas se enfrentan una probabilidad significativa de que sus sistemas informáticos se vean comprometidos. Los defensores enfrentan desafíos particulares para escalar la remediación en toda una organización y priorizar las acciones con prioridades conflictivas y, en ocasiones, efectos secundarios inciertos.*" (p.17)

Por ello, se ha propuesto que estas validaciones se realicen siguiendo modelos internacionales que se encuentran en las metodologías previamente estudiadas. Estas actividades se muestran en la siguiente tabla.

Tabla 6. Análisis de Vulnerabilidades
Fuente: Elaborada por el investigador

ISSAF
• B.3 Vulnerability Assessment (Identification)
NIST 800-115
• 4.3 Vulnerability Scanning
PTES
• 3.1 Vulnerability Testing
CIS
• Control 3 - Gestión continua de vulnerabilidades

Las herramientas utilizadas para este tipo de proceso son muy variadas, pudiendo el auditor seleccionar entre pagadas o libres, sin embargo, es importante seleccionar un escáner que implemente evaluaciones de cumplimiento sean estas SCAP, SOX, PCI, entre otras y que las firmas sean actualizadas continuamente.

De acuerdo a ISSAF, el escáner seleccionado debe realizar las siguientes actividades (Information Systems Security Assessment Framework, 2006):

- Realizar escaneos UDP, ICMP y para todo el protocolo TCP (incluyendo escaneos mediante SYN y CONNECT).
- Alimentar al escáner con los resultados del descubrimiento de activos (herramienta de escaneo de puertos) considerando los puertos desde el 1-65535 TCP y UDP.
- No seleccionar plug-ins relacionados a Denegación de Servicio. (p.128)

4.1.2.1. Vulnerabilidades del segmento de red

De acuerdo a los resultados del escáner automatizado, las vulnerabilidades son categorizadas en 4 grupos que son: Críticas, Altas, Medias y Bajas, este tipo de agrupación está basado en la tercera versión del Common Vulnerability Scoring System (CVSS por sus siglas en inglés) y facilita el entendimiento del nivel de riesgo no solo a personal técnico sino, también está dirigido para un nivel gerencial, aportando con indicadores y porcentajes que son comúnmente utilizados por profesionales de alto mando dentro de las empresas.

Existe una última categoría y es la denominada Info, y aporta con información netamente informativa que puede ser de utilidad para el analista al momento de evaluar las vulnerabilidades descubiertas.

De acuerdo al subcontrol 3.1 propuesto por CIS (CIS, 2018), en donde se establece que los escaneos deben realizarse “automáticamente a todos los sistemas en la red de forma semanal o más frecuente para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.” (p.16), se colocó el segmento de red objeto de análisis en el escáner

automático, obteniendo resultados diarios de las vulnerabilidades encontradas. Ya que esta red no ha tenido el tratamiento correcto en relación a mitigación de brechas de seguridad, se puede observar la presencia de una cantidad considerable de vulnerabilidades de alto riesgo como se puede apreciar en las siguientes ilustraciones.

Vulnerabilidades de Severidad Crítica

Este tipo de vulnerabilidades son las más peligrosas para la seguridad de una Empresa, ya que pueden ser explotadas por atacantes con la finalidad de obtener accesos a los sistemas afectados. Es importante comentar que los ataques que se podrían ejecutar son de forma remota, es decir, el atacante podría obtener una sesión en el activo vulnerable desde un punto de red de la infraestructura de Data Center, o si el servicio es expuesto a internet podría ser atacado desde cualquier parte del mundo.

Sev	Name	Family	Count
CRITICAL	Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	CGI abuses	8
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ET…	Windows	1
CRITICAL	Unsupported Windows OS	Windows	1

Figura 10. Vulnerabilidades de Riesgo Crítico
Fuente**:** Elaborada por el investigador

Vulnerabilidades de Severidad Alta

Las vulnerabilidades de severidad alta, son problemas que podrían permitir a un atacante tomar control del sistema, sin embargo, la efectividad de lograrlo dependerá de otros factores como la existencia de códigos de explotación publicados en internet o mercados digitales, malas configuraciones realizadas en los activos, entre otros. Se incluyen en esta categoría vulnerabilidades que podrían causar la caída de servicios (denegación de servicio) al ser explotadas.

Sev	Name	Family	Count
HIGH	Oracle GlassFish Server URL normalization Denial of Service	CGI abuses	11
HIGH	SSL Version 2 and 3 Protocol Detection	Service detection	9
HIGH	JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE	Web Servers	8
HIGH	JBoss JMX Console Unrestricted Access	CGI abuses	8
HIGH	SNMP Agent Default Community Name (public)	SNMP	3

Figura 11. Vulnerabilidades de Riesgo Alto
Fuente: Elaborada por el investigador

Vulnerabilidades de Severidad Media

Estas vulnerabilidades permitirían a un atacante aprovechar descuidos en la configuración para acceder a información sensible u oculta que podría ayudarle a llevar a cabo ataques más severos. Este tipo de vulnerabilidades no contemplan accesos no autorizados de forma directa, sin embargo, son utilizadas para ataques consecuentes.

Sev	Name	Family	Count
MEDIUM	SSL Certificate Cannot Be Trusted	General	71
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	61
MEDIUM	SSL Self-Signed Certificate	General	59
MEDIUM	SSH Weak Algorithms Supported	Misc.	53
MEDIUM	SSL Certificate Validity - Duration	General	13
MEDIUM	Apache Server ETag Header Information Disclosure	Web Servers	11
MEDIUM	Oracle GlassFish Server Path Traversal	CGI abuses	11
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	9
MEDIUM	SSL Certificate with Wrong Hostname	General	9
MEDIUM	Terminal Services Encryption Level is Medium or Low	Misc.	9
MEDIUM	JBoss Enterprise Application Platform '/web-console' Authentication Bypass	Web Servers	8
MEDIUM	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	CGI abuses	8
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	8
MEDIUM	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncre…	CISCO	4

MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	8
MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	6
MEDIUM	mDNS Detection (Remote Network)	Service detection	6
MEDIUM	LDAP NULL BASE Search Access	Misc.	5
MEDIUM	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Misc.	5
MEDIUM	Apache Tomcat Default Files	Web Servers	4
MEDIUM	SMB Signing not required	Misc.	4
MEDIUM	SNMP 'GETBULK' Reflection DDoS	SNMP	3
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	2
MEDIUM	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1

Figura 12. Vulnerabilidades de Riesgo Medio

Fuente: Elaborada por el investigador

Vulnerabilidades de Severidad Baja

Haciendo uso de herramientas comunes, los intrusos pueden recolectar información acerca del activo remoto (puertos abiertos, servicios en ejecución, entre otros) que pueden utilizarse para encontrar otras vulnerabilidades. También se incluye en esta categoría información que podría resultar interesante para el administrador de red para determinar si un activo ha pasado por procesos de aseguramiento (hardening) previo a la salida a producción.

Sev	Name	Family	Count
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	59
LOW	SSH Weak MAC Algorithms Enabled	Misc.	54
LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	27
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	15
LOW	OpenSSL AES-NI Padding Oracle MitM Information Disclosure	General	10
LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	9
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	2
LOW	Web Server HTTP Header Internal IP Disclosure	Web Servers	1

Figura 13. Vulnerabilidades de Riesgo Bajo

Fuente: Elaborada por el investigador

Como se puede observar, el segmento de red objeto de análisis, mantiene múltiples vulnerabilidades, algunas de ellas de alto riesgo, que conforman una fuerte amenaza para la seguridad del Data Center si no son tratados oportunamente.

4.1.3. Identificación y Evaluación de Riesgo

El tercer paso del marco propuesto corresponde a la identificación y evaluación de riesgo, esto para tener una visión global de los posibles escenarios que puedan afectar la seguridad de la red y aplicado a los activos de información identificados en los procesos anteriores, es recomendable construir una matriz de riesgo en donde se pueda validar las dolencias actuales y así poder construir un plan de pruebas y mitigación. De acuerdo a ISO 27001, la cláusula 8.3 de esta norma indica que "La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información y la organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de información" (ISO/IEC, 2013, pág. 13).

También es muy importante identificar los riesgos asociados al factor humano de la Empresa, en donde técnicas de Ingeniería Social podrían debilitar cualquier control tecnológico implementado en el segmento de red y en el Data Center en general. ISSAF define a la Ingeniería Social como (Information Systems Security Assessment Framework, 2006) "el objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad de un sistema objetivo." (p.891)

La educación preventiva frente a este tipo de amenazas debe ser contínua para evitar fraudes o accesos no deseados a equipos privados por parte de usuarios distraidos que entreguen información a terceras personas.

De acuerdo a la norma ISO 27001, en la cláusula 7.2 de Competencia, indica los siguientes lineamientos que la Empresa debe cumplir (ISO/IEC, 2013)

> "*a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y*
>
> *b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;*

c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y

d) conservar la información documentada apropiada, como evidencia de la competencia." (p.10)

Todos estos procesos de evaluación fueron presentados en el capítulo anterior en donde se muestran los distintos escenarios de riesgo que pueden afectar directamente a la seguridad del segmento de red e indirectamente al Data Center de Quito.

4.1.4. Mitigación de Riesgos

El cuarto paso del marco propuesto constituye el plan de mitigación de los riesgos y vulnerabilidades que fueron categorizadas en el paso anterior, es aquí donde se utilizan las distintas metodologías y buenas prácticas internacionales que facilitan el tratamiento de lo identificado previamente.

En el capítulo anterior se expusieron distintos escenarios de riesgo en donde la seguridad del segmento de red del Centro de Datos se puede ver comprometida tanto por factores internos como por factores externos a la Empresa. En este apartado se exponen las distintas estrategias que pueden ayudar en tratamiento del riesgo y con ello también disminuir las vulnerabilidades que puedan tener los dispositivos conectados a esta red.

4.1.4.1. Pérdida de Energía Eléctrica en Data Center

La pérdida de energía en el Centro de Datos puede ocasionar problemas serios si no se tiene las medidas de seguridad adecuadas para este escenario de riesgo, ya que el Data Center de Quito cuenta con la certificación internacional TIER III, los riesgos que amenazan este escenario son minimizados por las directrices de esta calificación, sin embargo, no hay que

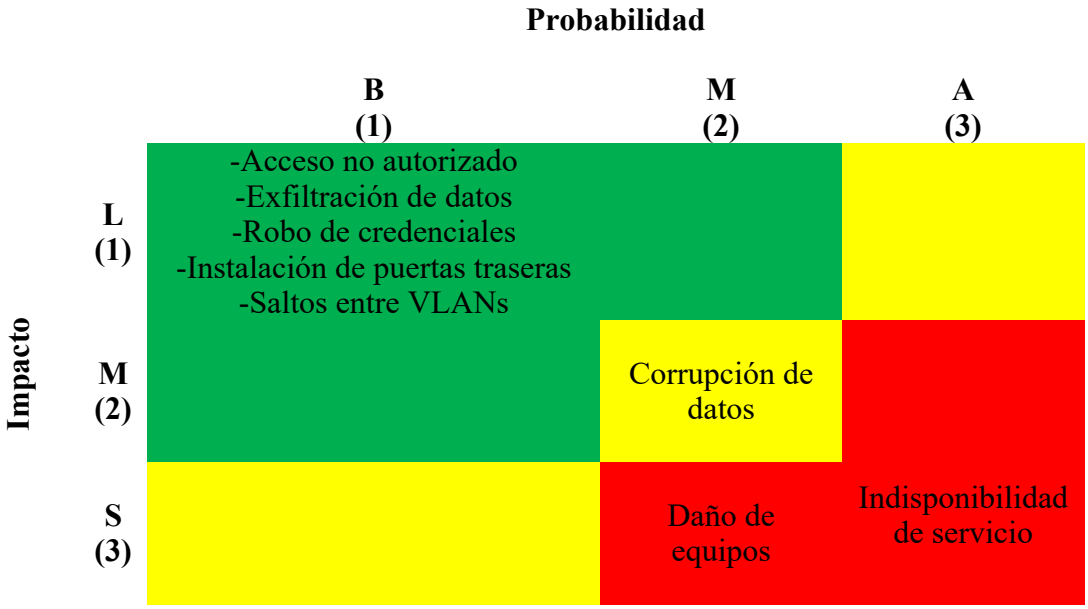
descuidar potenciales problemas que puedan surgir en relación a fallo humano que ponga en riesgo la continuidad del servicio del segmento de red.

Con estos antecedentes y de acuerdo a las directrices del Uptime Institute para evitar dificultades en este escenario se debe mantener lo siguiente:

- Sistemas de aire acondicionado y distribución de energía.
- UPS o generador eléctrico.
- Disponer de al menos un sistema de contingencia de cada componente de la infraestructura

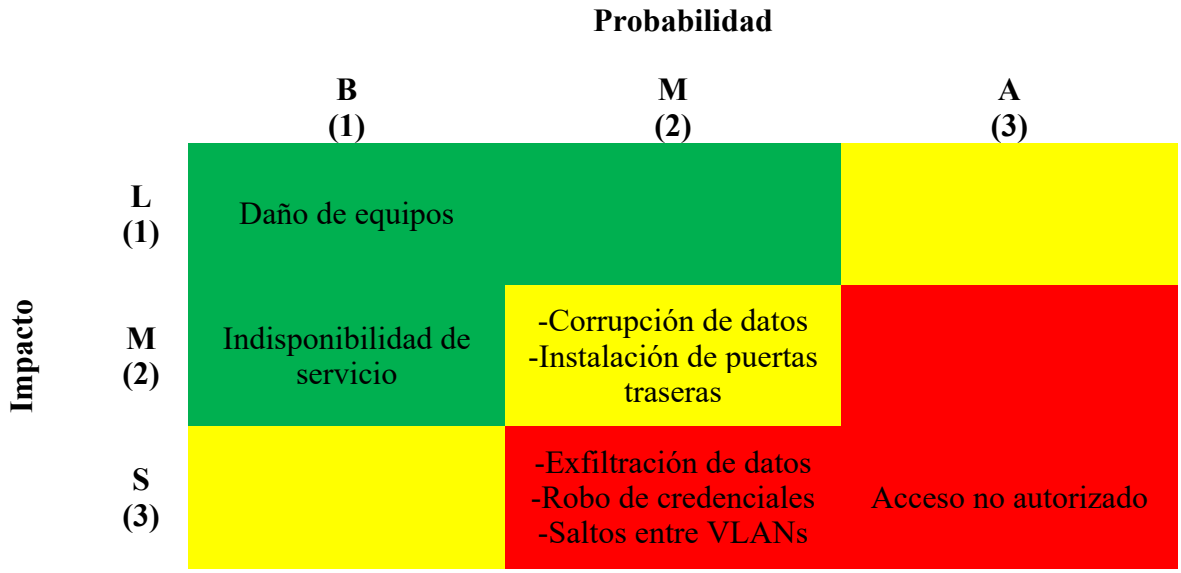
De esta forma se garantiza la continuidad en la operación de la red en caso de existir algún fallo relacionado al servicio eléctrico.

Tabla 7. Mapa de Calor Escenario 1
Fuente: Elaborada por el investigador



4.1.4.2. Hackeo de equipos por Identificación no oportuna de Vulnerabilidades

Tabla 8. Mapa de Calor Escenario 2
Fuente: Elaborada por el investigador



La anticipación a las posibles intrusiones que se puedan realizar por parte de atacantes es primordial en las labores de un Ingeniero de Seguridad, por lo cual la identificación y evaluación de brechas de seguridad debe ser ejecutada con alta regularidad y así reducir los riesgos de este escenario.

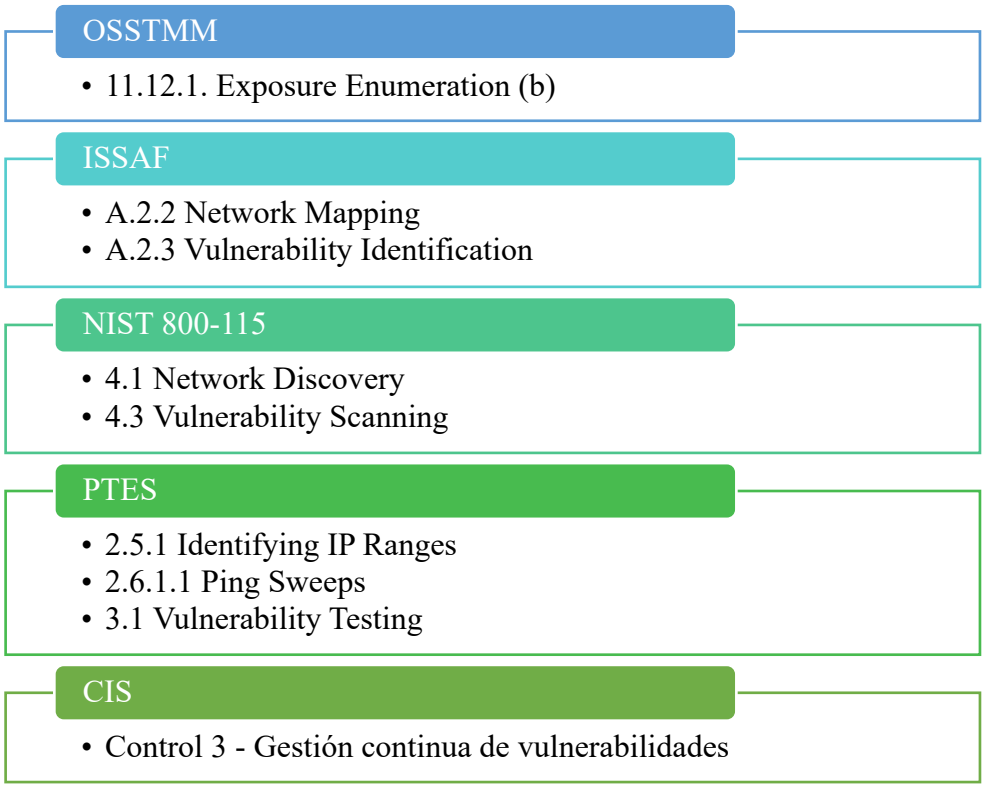
Existe un paso previo que debe realizarse antes de la ejecución de pruebas de vulnerabilidad y es la identificación de los activos de información, con un listado actualizado se puede priorizar los escaneos de redes y así optimizar tiempo en la solución de vulnerabilidades.

Con estos antecedentes, las tareas que se deben ejecutar para la mitigación de riesgos en este escenario son las que se muestran en la tabla 9.

Actualmente existen distintos fabricantes de herramientas de descubrimiento automatizado de vulnerabilidades, entre las más conocidas se encuentran Nessus, Nexpose, Qualys y OpenVas, este último es de libre distribución, sin embargo, cuenta con actualización tardía en relación a sus firmas de seguridad.

Tabla 9. Mitigaciones Metodológicas para Escenario 2

Fuente: Elaborada por el investigador



Las configuraciones esenciales que debe tener el escáner fueron presentadas en el apartado 4.1.2 del presente documento.

Para la solución de vulnerabilidades, el área de seguridad ha dispuesto un cuadro de tiempos de respuesta para las áreas dueñas de activos, misma que se encuentra documentada en los procesos internos del área de seguridad informática.

Tabla 10. Tiempos de Respuesta para Vulnerabilidades

Fuente: Elaborada por el investigador

Vulnerabilidad	**Tiempo de Solución (días)**	**Escalamiento a Gerencia si no existe respuesta (días)**
Crítica/Alta	3	4
Media	7	8
Baja	15	16

Para la mitigación de las vulnerabilidades descubiertas, cada área reportada ejecuta las actividades propuestas en la tabla 9 y en muchos casos acompañados por el proveedor del servicio adquirido, finalmente, se debe comentar al área de seguridad informática que las soluciones han sido aplicadas para que se ejecuten las validaciones respectivas y dar por solucionadas a las vulnerabilidades.

4.1.4.3. Hackeo de Servidores y estaciones de trabajo (red interna)

De forma similar al escenario anterior, el hardening es uno de los procesos importantes para evitar riesgos derivados de deficientes configuraciones de seguridad.

Tabla 11. Mapa de Calor Escenario 3
Fuente: Elaborada por el investigador

Impacto	Probabilidad: B (1)	Probabilidad: M (2)	Probabilidad: A (3)
L (1)	Saltos entre VLANs		
M (2)	-Daño de equipos -Robo de credenciales	Indisponibilidad de servicio	
S (3)		-Acceso no autorizado -Corrupción de datos -Exfiltración de datos -Instalación de puertas traseras	

Adicionalmente, las ejecuciones del escáner de vulnerabilidad son de gran utilidad al momento de identificar las falencias de los equipos que se encuentran en producción y que posiblemente no tuvieron un adecuado aseguramiento. De acuerdo a los resultados de vulnerabilidades para el segmento de red, se identificaron los siguientes problemas relacionados al escenario actual.

- Falta de aseguramiento de SMB (Eternalblue)

- Falta de aseguramiento de SSL
- Falta de aseguramiento de SSH (cifrados débiles)
- Falta de aseguramiento de Apache (Divulgación de Información)
- Falta de aseguramiento de protocolo SNMP (comunidades por defecto)
- Falta de aseguramiento de JBoss (Divulgación de Información / Instalación por defecto)
- Falta de aseguramiento de Apache Tomcat (Instalación por defecto)

Estas vulnerabilidades denotan descuido u olvido de las seguridades en los servidores y pueden ser mitigados con los controles propuestos a continuación:

Tabla 12. Mitigaciones Metodológicas para Escenario 3
Fuente: Elaborada por el investigador

OSSTMM	• 11.9.2 Common Configuration Errors • 11.9.3 Limitations Mapping
ISSAF	• P.5 Examine Common Protocols (Unix) • Q.15 Examine Common Protocols (Windows) • Q.16 Examining Windows Systems (Windows) • R Novell Netware Security Assessment
NIST	• 3.4 System Configuration Review
OWASP	• Test Network/Infrastructure Configuration (OTG-CONFIG-001)
CIS	• Control 5 - Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

En los documento elaborados por la entidad CIS, existen los denominados “CIS Benchmarks” (CIS, 2018), que son guías de aseguramiento para varias tecnologías entre las

que se encuentran servidores Microsoft, servidores Unix, equipos de usuario, entre otras tecnologías

También es posible obtener guías de aseguramiento en el repositorio de checklists de NIST (National Checklist Program Repository, 2019)

4.1.4.4. Indisponibilidad de bases de datos de aplicaciones internas

Las bases de datos internas pueden ser afectadas por distintos problemas en el segmento de red de un Centro de Datos e inclusive se pueden ver afectadas por los escenarios de riesgo enunciados previamente, sin embargo, existen vulnerabilidades específicas en distintos motores de bases de datos que pueden comprometer la seguridad de estos activos críticos de información.

Tabla 13. Mapa de Calor Escenario 4
Fuente: Elaborada por el investigador

Impacto \ Probabilidad	B (1)	M (2)	A (3)
L (1)	- Acceso no autorizado - Daño de equipos - Instalación de puertas traseras - Saltos entre VLANs		
M (2)		Exfiltración de datos	
S (3)		- Corrupción de datos - Robo de credenciales	Indisponibilidad de servicio

El tratamiento de riesgo para este escenario conlleva a aplicar guías de aseguramiento (hardening) que generalmente son distribuidas por los mismos fabricantes, o en su lugar se pueden utilizar los documentos propuestos por CIS Benchmarks (CIS Benchmarks, 2018).

Metodológicamente, los documentos descritos a continuación ayudarían a reducir los problemas de seguridad para estos servidores.

Tabla 14. Mitigaciones Metodológicas para Escenario 4
Fuente: Elaborada por el investigador

ISSAF
• Y.1 Microsoft Sql Server Security Assessment • Y.2 Oracle Security Assessment • Y.3 Database Services Countermeasures

Otro caso a tener en consideración, es la corrupción de datos o robo de credenciales desde una base de datos mediante técnicas de inyección de código en las aplicaciones web, es por ello, que se deben llevar a cabo auditorías periódicas de los sitios tanto públicos como privados para detectar problemas que puedan poner en alto riesgo la seguridad del segmento de red tomando en consideración la categorización de debilidades propuesto por OWASP.

Tabla 17 (cont.)

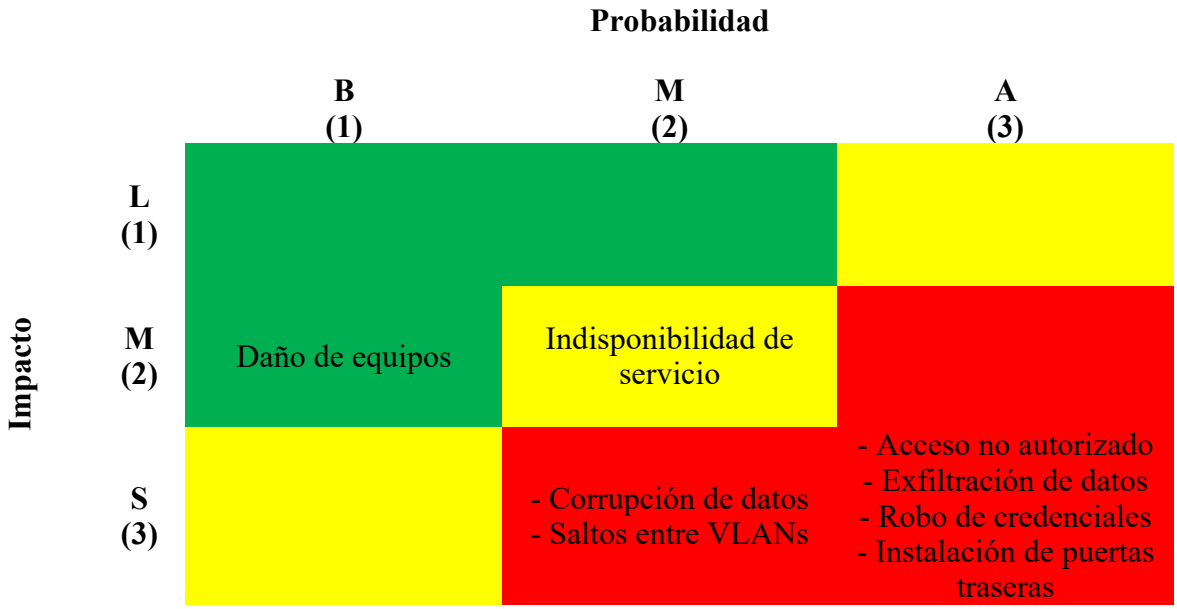
OWASP
• Identify application entry points (OTG-INFO-006) • Testing for SQL Injection (OTG-INPVAL-005) • Testing for ORM Injection (OTG-INPVAL-007) • Testing for XML Injection (OTG-INPVAL-008) • Testing for SSI Injection (OTG-INPVAL-009) • Testing for XPath Injection (OTG-INPVAL-010)

Finalmente, es importante contar con un inventario actualizado de los sitios web de la Empresa, para el caso de estudio se debe contar con el listado de portales configurados en el segmento de red, para posteriormente ejecutar un plan de auditoría que permita la identificación de vulnerabilidades de manera oportuna. El inventario de activos es un control de la norma ISO 27001, en donde se evalúa que “Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.” (ISO/IEC, 2013).

4.1.4.5. Hackeo de servidores expuestos a Internet

El segmento de red posee servidores con direccionamiento privado, sin embargo, en el firewall perimetral se han implementado configuraciones que permiten la publicación de ciertos servicios hacia internet, es así que la probabilidad de sufrir un ataque externo se incrementa considerablemente.

Tabla 15. Mapa de Calor Escenario 5
Fuente: Elaborada por el investigador



En la ejecución del reconocimiento de vulnerabilidades se debe prestar especial atención a vulnerabilidades categorizadas como Altas (naranja) y Críticas (rojas) ya que son estas las que podrían permitir la ejecución de códigos de explotación desde cualquier parte del mundo y así tener un acceso no deseado a la infraestructura, dichas vulnerabilidades en el segmento de red son:

- SSL Version 2 and 3 Protocol Detection
- Oracle GlassFish Server URL normalization Denial of Service
- JBoss JMX Console Unrestricted Access
- Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities

- JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE

Metodológicamente, estas vulnerabilidades pueden ser mitigadas utilizando las pruebas de seguridad ilustradas en la tabla 19.

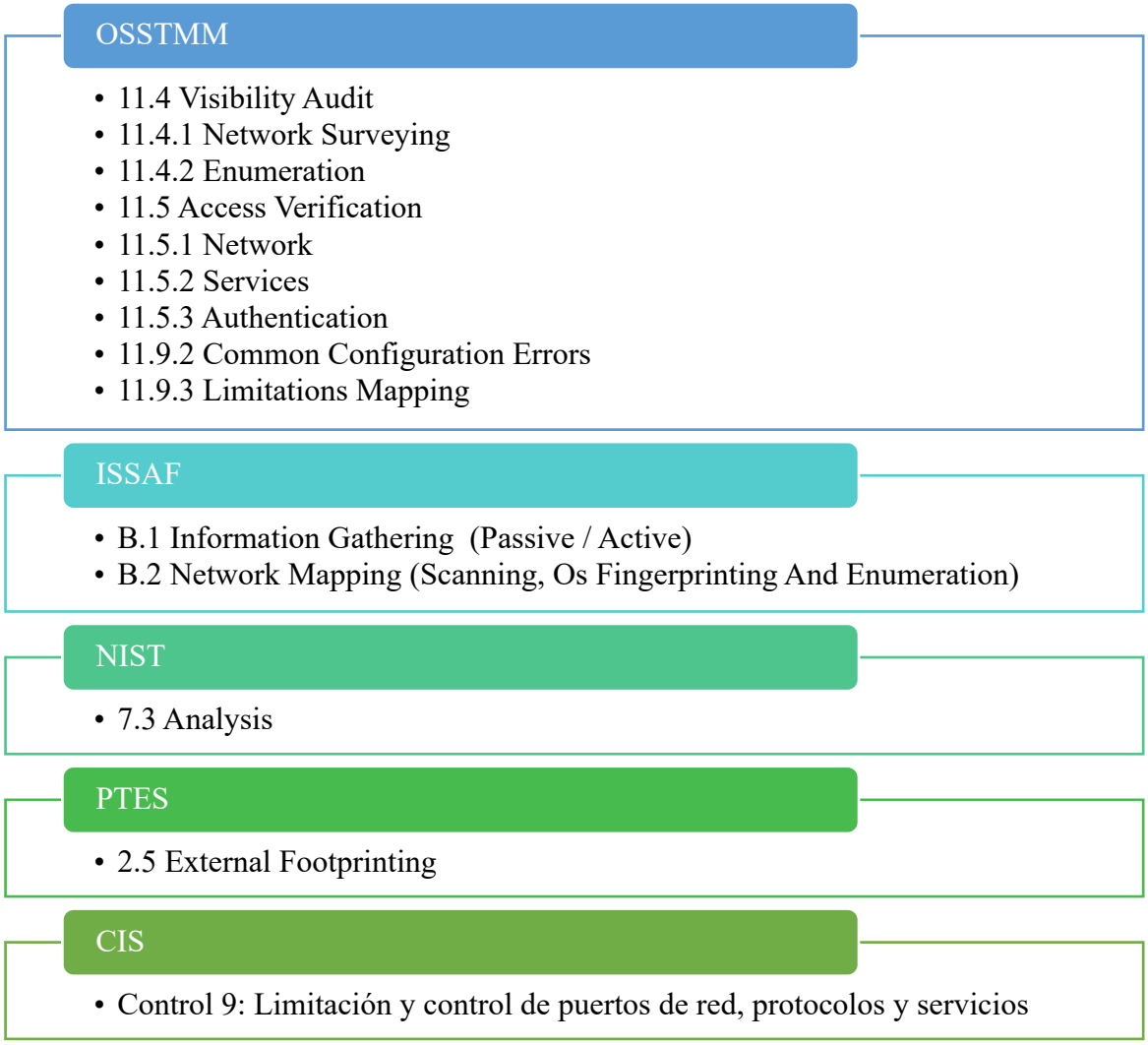
Las pruebas listadas son utilizadas para validar una posible explotación de las vulnerabilidades identificadas por el escáner. Al conocer las oportunidades que podría tener un atacante se pueden colocar controles adicionales como el aseguramiento (hardening) de servidores públicos, validación de reglas de firewall perimetral, configuración de Web Application Firewall (WAF) para los servidores que ofrecen acceso a sitios web y el afinamiento de políticas de detección de ataques de denegación de servicio.

Algunas herramientas que pueden ser de utilidad en la detección o explotación de las vulnerabilidades a modo de prueba de concepto, son:

- Nmap
- Shodan
- Whois
- Recon-ng
- Sn1per
- Metasploit Framework

Tabla 16. Mitigaciones Metodológicas para Escenario 5

Fuente: Elaborada por el investigador

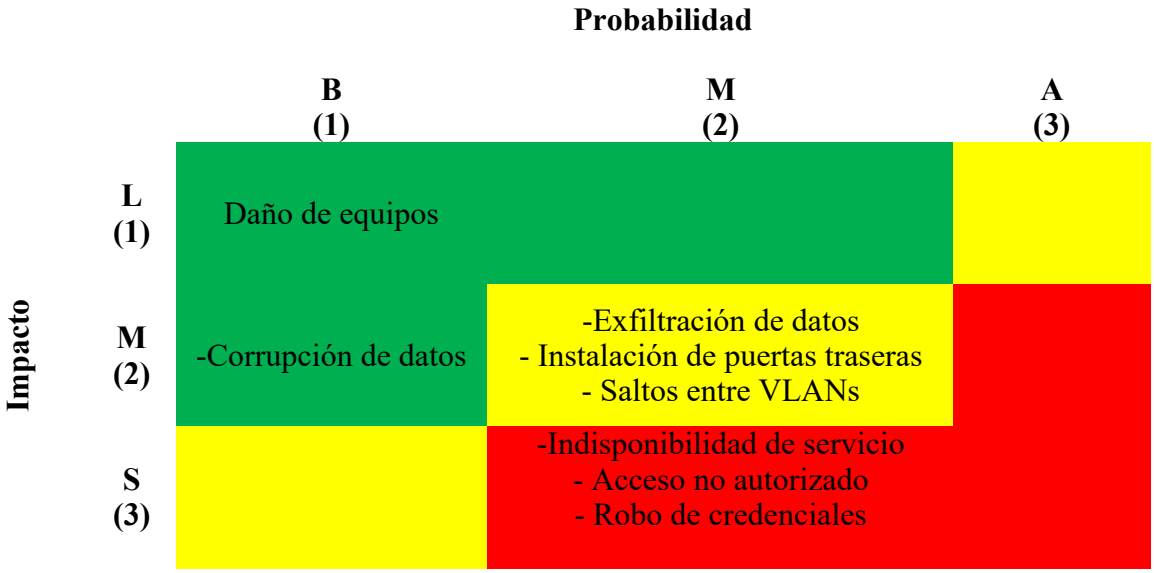


Para cumplir con estas propuestas de aseguramiento, el área de Seguridad Informática debe ejecutar las configuraciones necesarias en los equipos perimetrales y solicitar accesos provisionales a los servidores para realizar el hardening respectivo, sin embargo, la remediación en los servidores deben ser programadas por los dueños de estos activos.

4.1.4.6. Hackeo de aplicaciones web desde internet

Tabla 17. Mapa de Calor Escenario 6

Fuente: Elaborada por el investigador



Las aplicaciones web expuestas a internet constituyen un objetivo muy utilizado por los atacantes internacionales, esto debido a que en muchas ocasiones no se llevan a cabo revisiones de seguridad a nivel de código o se utilizan programas de terceros que contienen vulnerabilidades en su diseño o en sus complementos.

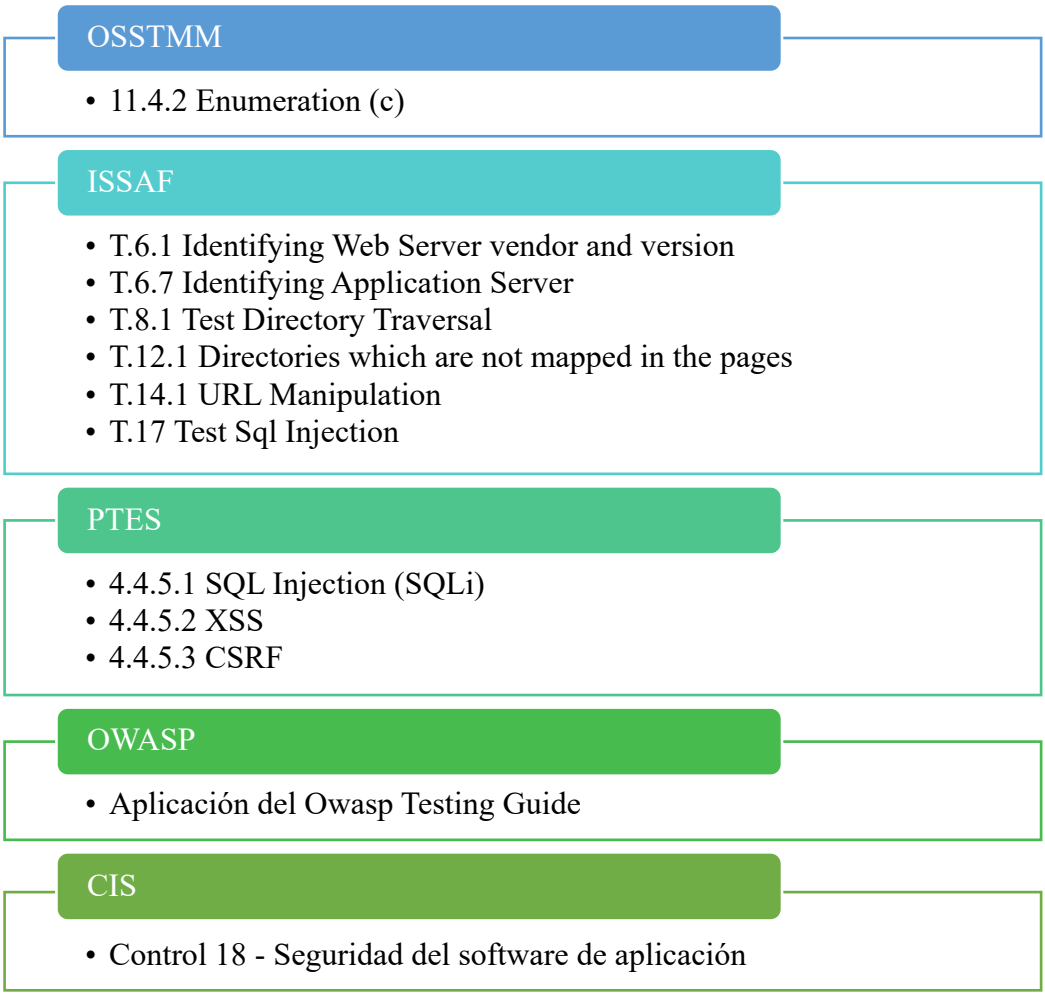
Para evaluar los problemas relacionados a sistemas web publicados en internet, es importante contar con un equipo VPS (Virtual Private Server) configurado en una red pública e independiente a la Empresa, actualmente existen servicios de arriendo de servidores en Estados Unidos, Canadá, Rusia y más países, con los que se pueden llevar a cabo validaciones más precisas simulando ataques provenientes desde internet.

Las técnicas de validación que se utilizan en este tipo de vulnerabilidades son similares a las realizadas para redes de datos privadas, por lo cual, si se tiene una intrusión aprovechando una vulnerabilidad de tipo web, el atacante podría obtener acceso al segmento de red evaluado y llevar a cabo escalamiento de privilegios para comprometer otros segmentos de red o robar información privilegiada de las bases de datos.

Para minimizar los riesgos en este tipo de escenario, es importante tomar en consideración las validaciones propuestas por OWASP para los servidores que tengan estos sitios expuestos, sin embargo, es importante mantener una política interna de revisión de código fuente para evitar colocar en producción software con múltiples vulnerabilidades desde el diseño.

Las validaciones que mitigan estos riesgos de acuerdo a las metodologías internacionales son las mostradas en la tabla 18.

Tabla 18. Mitigaciones Metodológicas para Escenario 6
Fuente: Elaborada por el investigador



Algunas herramientas que son útiles para detectar estos problemas o explotar las vulnerabilidades a modo de prueba de concepto son:

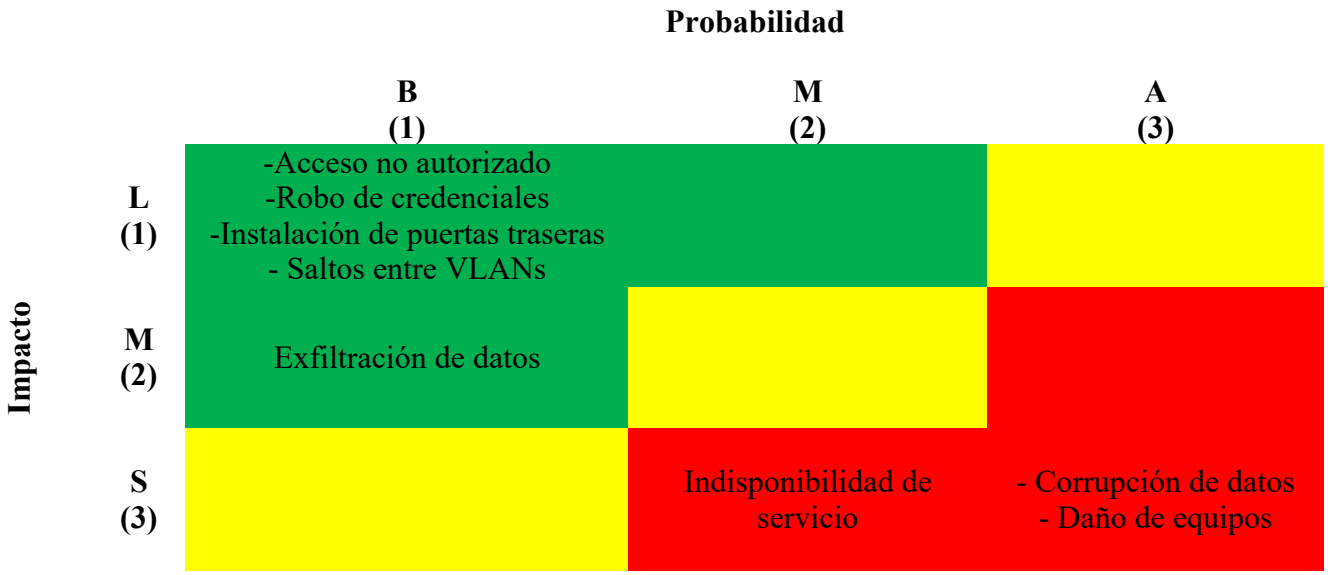
- Dirb

- OWASP ZAP
- Burpsuite
- SQLMap
- W3af
- Nikto

4.1.4.7. Indisponibilidad de servicio por operadores de red no capacitados

Tabla 19. Mapa de Calor Escenario 7

Fuente: Elaborada por el investigador



El desconocimiento de determinadas tareas en los equipos del Data Center puede generar serios problemas en la disponibilidad y continuidad de los servicios ofrecidos desde este lugar. Un administrador si no cuenta con la instrucción formal necesaria o desconoce acerca de la operación de las distintas plataformas que están configuradas de forma inconsciente podría generar una indisponibilidad de servicio o pérdida de información para el caso de réplicas de base de datos, por ello las tareas para mitigar este escenario riesgo de acuerdo a la metodologías OSSTMM deberán ser:

Tabla 20 - Mitigaciones Metodológicas para Escenario 7
Fuente: Elaborada por el investigador

OSSTMM
• 7.9.1 Education Mapping • 7.9.2 Policy Disruption • 7.9.3 Awareness Mapping

Adicionalmente, se debe mantener un plan de capacitación para las distintas áreas que dan servicio al Data Center, ya que al ser un área crítica dentro de la Empresa una falla humana podría ocasionar problemas no solo al segmento de red de estudio sino también a otras redes.

Los planes de capacitación junto con sus convenios internos deberán reposar en el área de Recursos Humanos, ya que son sustento auditable para otras normas que aplican al Data Center como lo es ISO 27001.

4.1.5. Resultados

El quinto paso del maro de referencia es utilizado para mostrar los resultados de la aplicabilidad de los procesos propuestos para el análisis de vulnerabilidades del segmento de red evaluado.

De forma global se puede mencionar que se obtuvieron resultados que ayudaron a disminuir el riesgo de una intrusión no controlada al segmento evaluado. Esto pudo ser validado mediante una nueva ejecución del escáner automático, en donde se verificó que las vulnerabilidades han disminuido, sin embargo se evidencia un remanente que si bien no es de alto riesgo, no debe ser descuidado para evitar problemas futuros.

En la siguiente figura se muestran los resultados del nuevo examen de vulnerabilidades contra los mismos activos del segmento de red.

Sev	Name	Family	Count
MEDIUM	SSH Weak Algorithms Supported	Misc.	53
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	9
MEDIUM	Terminal Services Encryption Level is Medium or Low	Misc.	9
MEDIUM	mDNS Detection (Remote Network)	Service detection	6
MEDIUM	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Misc.	5
MEDIUM	SMB Signing not required	Misc.	4
MEDIUM	SNMP 'GETBULK' Reflection DDoS	SNMP	3
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	2
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	59
LOW	SSH Weak MAC Algorithms Enabled	Misc.	54
LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	27
LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	9

Figura 14- Vulnerabilidades Aplicando Marco de Referencia
Fuente: Elaborada por el investigador

Si se realiza una comparativa entre lo identificado antes y después de la aplicabilidad del marco de referencia, se puede evidenciar que la reducción de vulnerabilidades es muy significante, ayudando a la protección de este segmento de red y al Data Center en general.

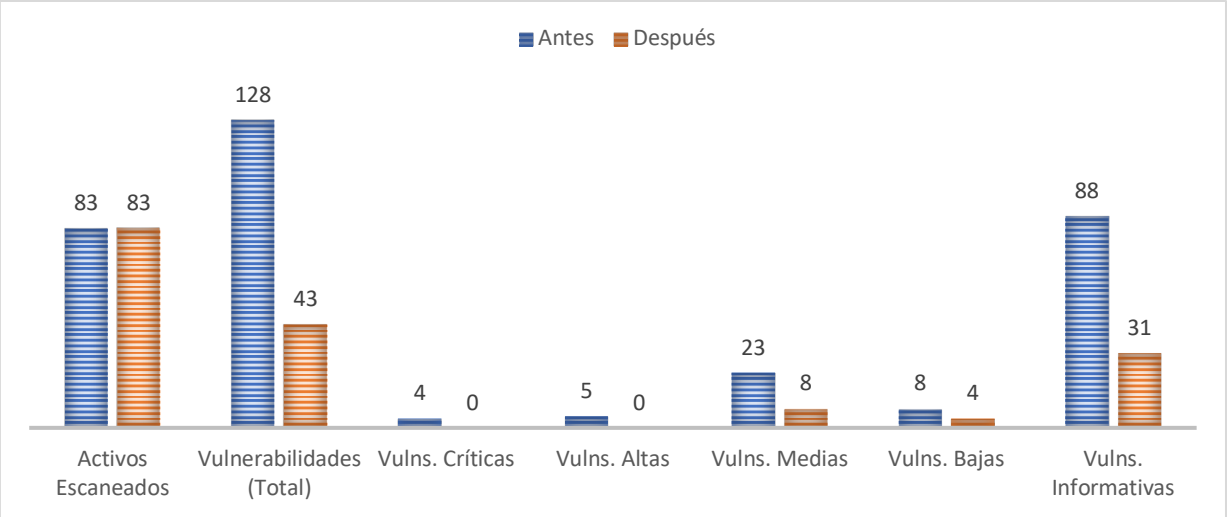


Figura 15 - Antes y Después de Marco de Referencia
Fuente: Elaborada por el investigador

De esta forma, se puede decir que el marco de referencia propuesto ha sido satisfactorio para la identificación y tratamiento de vulnerabilidades aplicadas al segmento de red del Data Center de Quito por lo que el área de seguridad informática podría proponer su aplicabilidad en otros segmentos de red.

4.1.6. Auditorías

Para cerrar el círculo de validaciones, es muy importante contar con auditorias de procesos internos en donde se pueda evidenciar el compromiso por parte de la alta gerencia hacia la seguridad de la información.

Es también importante contar con puntos de vista de validaciones de gobierno de tecnología y controles de TI para obtener una mejor imagen de los procesos relacionados al Data Center que podrían impactar en sus operaciones, sin embargo, este apartado debe ser ampliamente estudiado y validado en varias reuniones con las autoridades internas de la Empresa, en donde se lleven a cabo programas muy minuciosos de auditorías tanto internas como externas donde se contrata a un ente certificador para que exponga sus opiniones acerca de la gestión realizada en el Data Center.

Por estos motivos, la evaluación y resultados de auditorías efectuadas al marco de referencia constituyen el trabajo futuro que debe ser efectuado por la administración de la Empresa y así disponer de indicadores de calidad que fortalezcan a los procesos internos que pretenden asegurar contra factores maliciosos no solo a las redes del Data Center sino a todas las redes de la Empresa.

CAPÍTULO V

CONCLUSIONES Y TRABAJO FUTURO

5.1. Conclusiones

- Se pudo comprobar que, al aplicar el marco de referencia propuesto, se redujo la cantidad de alertas detectadas inicialmente por el escáner, logrando de esta manera una mejor administración en la detección, categorización y solución de vulnerabilidades de red. Estos resultados son parte del trabajo diario de un Ingeniero de Seguridad Informática y constituyen los datos de entrada que soportan el proceso de Gestión de Vulnerabilidad Técnica llevado a cabo en la Empresa de Telecomunicaciones.
- Se espera que el marco de referencia presentado en este estudio, pueda ser replicado en otras instituciones en donde se busque minimizar el impacto que ocasionaría una intrusión a la red corporativa, sin embargo, los escenarios y la evaluación de riesgo deben ser formulados en relación al estado actual de la red para obtener una visión precisa de los problemas que se pretende solucionar.
- La identificación de activos de información junto a sus responsables es una etapa crucial para el éxito de esta propuesta o cualquier metodología aplicable a la detección de vulnerabilidades, la interacción entre las áreas involucradas y el compromiso de Gerencias es muy importante en la ejecución de estos proyectos ya que de esta manera se conforman planes de acción y tiempos de solución más cortos para alertas críticas en los activos. El área de Seguridad Informática es la llamada a ser los guías de ejecución y quienes al finalizar los trabajos por parte de los dueños de los equipos validen si todo lo realizado está conforme a la normativa actual y los lineamientos propuestos en el marco de referencia.

5.2. Recomendaciones

- Para el éxito del modelo propuesto en otras empresas, es importante tener claramente identificados los escenarios de riesgo de los segmentos de red, de esta forma se puede proponer actividades que mitiguen vulnerabilidades en los activos internos, por ello para replicar este modelo en otras redes, es aconsejable conformar una matriz de riesgos para los activos críticos y de esta forma diseñar un plan de solución que minimicen la superficie de ataque hacia las redes de cada empresa.
- Es recomendable contar con un listado detallado de puertos y servicios que se encuentran en ejecución en los servidores de la red evaluada, esto facilitará la óptima configuración del escáner de vulnerabilidades evitando falsos positivos y permitiendo al equipo de seguridad informática accionar rápidamente contra las alertas de alto riesgo.
- Se aconseja no ejecutar la identificación de vulnerabilidades en horario laboral, ya que estas herramientas generan alto consumo de red pudiendo en determinado momento saturar a los equipos de networking y consecuentemente llegar a un estado involuntario de denegación de servicio.

5.3. Trabajo Futuro

- La propuesta del modelo de referencia incluye un módulo de auditoría, mismo que debe ser ejecutado en cada evaluación de seguridad para así estar alineados a los procesos de certificaciones internacionales que mantiene la Empresa.
- Idealmente, el proceso de auditoría conlleva varios pasos adicionales que podrían ser utilizados por profesionales expertos en el tema y de esta forma complementar este trabajo de investigación con evaluaciones de Gobierno de TI, Controles de TI entre otros. La validación de código fuente es un trabajo muy amplio y que debe ser incluido como complemento a las pruebas de seguridad de aplicaciones web o

aplicaciones de escritorio y así evitar colocar en producción software con múltiples vulnerabilidades.

- Adoptar el marco de referencia para otras redes de la Empresa y así evaluar la reducción de vulnerabilidades en los activos de información.
- Complementar el ciclo de detección de vulnerabilidades con un modelo referencia que tenga como enfoque principal la evaluación de seguridad interna de los activos, aplicando metodologías de hardening tanto para dispositivos de networking como para servidores y equipos de usuario final.

BIBLIOGRAFÍA

- Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria.
- Tori, C. (2008). *Hacking Etico.* Rosario, Argentina: Mastroianni Impresiones.
- Pacio Germán. (2014). *Data centers hoy.* Alfaomega Grupo Editor.
- Astudillo Karina. (2013). *Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos!* Createspace Independent Pub.
- TIA-942.org. (2014). *www.tia-942.org*. Obtenido de About_Data_Centers: http://www.tia-942.org/content/162/289/About_Data_Centers
- Real Academia Española. (2018). *Diccionario de la Lengua Española*. Obtenido de Diccionario de la Lengua Española: http://dle.rae.es/?id=JxkTJjl
- Patrick Engebretson. (2013). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy* (Vol. 2).
- Carla Pérez. (27 de Diciembre de 2017). *Policía Ecuador*. Obtenido de Delitos informáticos establecidos en el COIP y como prevenirlos: http://www.policiaecuador.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/
- Resolución JB-2014-3066. (2014). *Superintendencia de Bancos.* Obtenido de Resoluciones: http://oidprd.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2014/resol_JB-2014-3066.pdf
- Carvajal, M. S. (2013). Ethical Hacking: La Importancia de una intrusión controlada. *Revistas Bolivianas- Scientific Electronic Library Online*.

- Viteri, S. (2013). *Evaluación Técnica de la Seguridad Informática del Data Center de la Brigada de Fuerzas Especiales No. 9 Patria.* Obtenido de Repositorio Digital de la Universidad de las Fuerzas Armadas ESPE: https://repositorio.espe.edu.ec/bitstream/21000/6811/1/T-ESPE-047288.pdf
- Torres, H. (2010). *Diseño de la seguridad informática en la implementación de data center de la Universidad Nacional de Loj.* Obtenido de Repositorio Digital de la Universidad de Cuenca: http://dspace.ucuenca.edu.ec/handle/123456789/2535
- Trend Micro. (May de 2016). *Trend Micro*. Obtenido de https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ecuadorean-bank-loses-12m-via-swift
- El Comercio. (26 de Noviembre de 2012). *Webs gubernamentales del Ecuador fueron supuestamente hackeadas hoy*. Obtenido de http://www.elcomercio.com: http://www.elcomercio.com/actualidad/politica/webs-gubernamentales-del-ecuador-supuestamente.html
- El Telégrafo. (27 de Marzo de 2014). *La cuenta de Twitter del presidente Correa fue hackeada*. Obtenido de https://www.eltelegrafo.com.ec: https://www.eltelegrafo.com.ec/noticias/informacion/1/la-cuenta-del-presidente-correa-fue-hackeada
- AENOR UNE-ISO/IEC 27001. (2014). Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de Seguridad de la Información (SGSI), Requisitos. *UNE-ISO/IEC 27001*. Madrid, España: AENOR.
- ISECOM, & www.isecom.org. (s.f.). *www.isecom.org*. Obtenido de www.isecom.org.
- OWASP Open Web Application Security Project. (2015). *Guía de Pruebas 4.0 "Borrador".* Obtenido de DragonJar: https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml

- Project Management Institute, I. (2013). *Guía de los fundamentos para la dirección de proyectos (guía del PMBOK®) - 5a edición.*
- Open Information Systems Security Group. (2006). *Information Systems Security Assessment Framework (ISSAF)* (0.2.1 ed.). Obtenido de http://www.oissg.org/files/issaf0.2.1.pdf
- http://www.pentest-standard.org. (2014). *The Penetration Testing Execution Standard.* Obtenido de http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- National Institute of Standards and Technology (NIST). (2008). *Technical Guide to Information Security Testing and Assessment (800-115).* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- ISECOM, O. (2010). *Open Source Security Testing Methodology Manual - OSSTMM* (Tercera ed.). Obtenido de http://www.isecom.org/mirror/OSSTMM.3.pdf
- Pandey, Brijesh & Singh, Alok & Balani, Lovely. (2015). *ETHICAL HACKING (Tools, Techniques and Approaches).* Obtenido de https://www.researchgate.net/: https://www.researchgate.net/publication/271079090_ETHICAL_HACKING_Tools_Techniques_and_Approaches
- ISO/IEC. (2013). Norma Internacional ISO 27001.
- CISCO. (25 de Septiembre de 2018). *Guide to Harden Cisco IOS Devices*. Obtenido de Guide to Harden Cisco IOS Devices: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- Aruba Networks. (1 de Abril de 2018). *ArubaOS-Switch Hardening Guide for 16.04.* Obtenido de ArubaOS-Switch Hardening Guide for 16.04: https://community.arubanetworks.com/aruba/attachments/aruba/CampusSwitching/3080/2/ArubaOS-Switch%20Hardening%20Guide%20for%2016.04.pdf
- CIS. (2018). *CIS Benchmarks*. Obtenido de CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks/

- Fortinet. (2018). *Hardening your FortiGate*. Obtenido de Hardening your FortiGate: https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-hardening-52/intro.htm
- NIST. (2019). *National Checklist Program Repository*. Obtenido de National Checklist Program Repository: https://nvd.nist.gov/ncp/repository
- Open Web Application Security Project (OWASP). (3 de Agosto de 2015). *OWASP Testing Guide v4.* Obtenido de OWASP Testing Guide v4: https://www.owasp.org/images/1/19/OTGv4.pdf