UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE
Maestro en Seguridad y Gestión de Riesgos Informáticos

PROYECTO
Estrategias de defensa efectiva contra las amenazas a la seguridad cibernética

PRESENTADO POR
Leonardo Antonio Aguilera Torres
Miguel Angel Tejada Silva

ASESOR
Ivan Alvarado

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América
Abril 2020

Índice

1. Planteamiento del problema 4
   1.1. Descripción 4
   1.2. Objetivos 4
      1.2.1. Objetivo general 4
      1.2.2. Objetivo especifico 4
   1.1. Justificación 5
   1.2. Delimitación 5
2. Estado del arte 6
   2.1 Marcos de trabajo para la gestión y gobierno de TI 6
      2.1.1 ISO 27001:2013, Técnicas de seguridad - Sistemas de gestión de seguridad de la información - requerimientos 6
      2.1.2 ISO 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información 7
      2.1.3 COBIT 5, Un marco de negocio para el gobierno y la gestión de las TI de la empresa 10
      2.1.4 PCI DSS 13
   2.2 Metodología dinámica de gestión de riesgos 14
      2.2.1 Definición de las amenazas y vulnerabilidades dinámicas 16
      2.2.2 Principales amenazas y vulnerabilidad de TI para los sistemas de información 16
      2.2.3 Análisis de riesgo 18
      2.2.4 Evaluación de impacto a los objetivos de la organización 22
   2.3 Metodología para el monitoreo y evaluación de desempeño. 23
      2.3.1 Monitoreo de planes de implementación 24
      2.3.2 Establecer plan de auditoría 25
      2.3.3 Plan de investigación de nuevas amenazas 26
3. Metodología de investigación 29
   3.1 Tipo de investigación y alcance 29
   3.2 Unidades de análisis y variables 29
   3.3 Técnicas e Instrumentos 29
4. Resultados 30

4.1 Resultado nivel de madurez 30
4.2 Análisis de vulnerabilidad 32
4.3 Análisis de riesgo 35
5. Conclusiones y recomendaciones 38
5.1 Conclusiones 38
6.1 Recomendaciones 39
6. Anexos 40
7. Referencias 44

Índice de figuras

Figura 1 Principios COBIT 10
Figura 2 Gobierno y Gestión en COBIT 5 11
Figura 3 Catalizadores Corporativos 12
Figura 4 Áreas claves de gobierno y Gestión 12
Figura 5 Procesos de Gobierno de TI Empresarial 13
Figura 6 Matriz de riesgo cualitativa 21
Figura 7 Matriz de riegos cuantitativa 22
Figura 8 Gráfico de radar 32
Figura 9 Versión OpenVAS 33
Figura 10 Feed Status 33
Figura 11 Tarea de análisis 34
Figura 12 Resultado de análisis 34
Figura 13 Detalle de vulnerabilidad 35
Figura 14 Amenazas humanas 36

Índice de tablas

Tabla 1 Requerimientos PCI DSS 14
Tabla 2 Resultado evaluación de procesos 31

1. Planteamiento del problema

1.1. Descripción

El proyecto consiste en la formulación de un marco de trabajo para el diseño de estrategias de protección de activos informáticos corporativos de forma holística, basado en las mejores prácticas del gobierno de TI (Tecnología de la información) tal como COBIT 5 y marcos de trabajo para la gestión de TI (ISO 27001). Debido a la complejidad de las diferentes amenazas que las organizaciones enfrentan, es necesario definir estrategias y actividades recurrentes que permitan estar al día y así mitigar los riesgos asociados a las tecnologías de TI, esto basado en la experiencia profesional en el campo de trabajo soportado por una serie de certificaciones en el área de seguridad informática.

El crecimiento permanente y acelerado de las amenazas informáticas mantiene en constante investigación y desarrollo a muchas empresas líderes en el área de la industria de seguridad de las TI, para poder mitigar en cierta medida los ataques globales a todo activo que pueda considerarse de valor para las corporaciones y gobiernos que tengan algún nivel de integración con las TI con su infraestructura de producción y operación.

Hoy en día la mayoría de las empresas no están listas para enfrentar y asegurar sus activos TI a la velocidad y niveles mínimos requeridos, que permitan la continuidad del negocio en caso de ser blancos de un ciberataque.

1.2. Objetivos

1.2.1. Objetivo general

Proponer un marco de trabajo que permita a las empresas la evaluación, diseño y creación de estrategias de seguridad de las TIC, garantizando un buen nivel de protección en cuanto a la confiabilidad, integridad y disponibilidad de los datos y servicios para el desarrollo de las actividades primarias y secundarias relacionadas con la misión y visión de la empresa.

1.2.2. Objetivo especifico

- Analizar la madurez del gobierno de TI y su grado de alineación con los objetivos corporativos.
- Establecer una metodología dinámica adaptativa para la gestión de riesgos de las TI.
- Definir una metodología para el monitoreo y evaluación de desempeño de la seguridad de las TI.

1.1. Justificación

Hoy en día existen muchas organizaciones de todos tipos ya sea de gobierno, sector privado, etc., y de múltiples niveles que utilizan plataformas tecnológicas para poder alcanzar sus objetivos, todas estas plataformas poseen un riesgo asociado que podría impactar negativamente los objetivos corporativos.

No se pueden evitar las amenazas en un mundo digitalizado sin fronteras en el cual la tecnología apoya en gran medida a las metas de las organizaciones, no obstante, se pueden poner una serie de controles que permitan disminuir sistemáticamente el nivel de riesgo e impacto a los activos de una organización, priorizando acciones de mitigación en una adecuada medida y cantidad de recursos invertidos para ello.

Para poder establecer los controles de manera correcta es necesario seleccionar un marco de trabajo que se apegue a las necesidades y la naturaleza de la organización. Existe una amplia gama de marcos de trabajo ya establecidos y aprobados internacionalmente, pero no necesariamente todos se pueden apegar al lugar de trabajo donde se pretenden implementar, este trabajo de investigación será una guía que facilite a los líderes e implementadores el poder establecer un sistema de gestión de la seguridad de la información de una manera adecuada y basado en estándares internacionales.

La importancia de hacer énfasis en los diferentes marcos de trabajo y su implementación radica que no todas las organizaciones evolucionan al mismo ritmo, existen muchas empresas que son víctimas de ataques cibernéticos o robo de información debido a una mala gestión en los sistemas, lo cual puede conllevar a perdida de ganancias, clientes, multas hasta la banca rota. Con esta investigación se pretende hacer conciencia de tal importancia y servir como guía práctica para el desarrollo de plan de trabajo en la ciberseguridad.

1.2. Delimitación

La investigación será realizada en el período que corresponde al mes de agosto 2019 y enero 2020, lo que nos permitirá estudiar marcos de trabajos y estándares internacionales. Se establecerá un marco de trabajo el cual se podrá acoplar para cualquier tipo de organización la cual utilice sistemas de información para poder alcanzar sus objetivos corporativos.
Se hará mayor énfasis en reglamentaciones y regulaciones que se deben de implementar en El Salvador.

2. Estado del arte

2.1 Marcos de trabajo para la gestión y gobierno de TI

2.1.1 ISO 27001:2013, Técnicas de seguridad - Sistemas de gestión de seguridad de la información - requerimientos

ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) forman el sistema especializado para la estandarización universal. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. En el campo de la tecnología de la información, ISO e IEC ha establecido un comité técnico conjunto, ISO/IEC JTC 1. [1, p. ii]
La norma ISO 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) dentro del contexto de la organización, incluye requerimientos para la evaluación y tratamientos de riesgos de seguridad de la información de acuerdo con las necesidades de la organización.[1, p. 1]

La estructura de esta norma es de alto nivel y forma parte de la familia de estándares ISO 27000, la implementación se puede complementar entre las diferentes normas de la serie, por ejemplo: "Código de prácticas para gestión de la seguridad de la información" (ISO 27002), "Directrices de implementación" (ISO 27003), Gestión de riesgos de seguridad de la información (ISO 27005)

Requerimientos de la norma:

- CONTEXTO DE LA ORGANIZACIÓN
    - Comprensión de la organización y su contexto
    - Comprensión de las necesidades y expectativas de las partes interesadas
    - Determinar el alcance del sistema de gestión de seguridad de la información,
    - Sistema de gestión de seguridad de la información

- LIDERAZGO
    - Liderazgo y Compromiso
    - Política
    - Roles, responsabilidades y autoridades organizacionales

- PLANEACIÓN
    - Acciones para abordar riesgos y oportunidades

- Objetivos de seguridad de la información y planeación para lograrlos

- SOPORTE
  - Recursos
  - Competencia
  - Conciencia
  - Comunicación
  - Información documental

- OPERACIÓN
  - Planeación y control operacional
  - Evaluación del riesgo de seguridad de la información
  - Tratamiento del riesgo de seguridad de la información

- EVALUACIÓN DEL DESEMPEÑO
  - Monitoreo, medición, análisis y evaluación
  - Auditoría interna
  - Revisión de la Dirección

- MEJORA
  - No conformidad y acción correctiva

2.1.2 ISO 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información

Esta norma técnica está diseñada para organizaciones que utilizan como referencia para la selección de los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 o como un documento guía para las organizaciones implementando controles de seguridad de la información comúnmente aceptados. También tiene como propósito ser utilizada en el desarrollo de directrices de gestión de seguridad de la información específica para la industria y organización, considerando su ambiente especifico de riesgos de seguridad de información.[2, p. iv]

Requisitos de seguridad de la información

a) Evaluación de los riesgos, acá se identifican las amenazas, vulnerabilidad, probabilidad y el impacto potencial.
b) Requisitos legales.

c) Conjunto de principios, objetivos y requisitos de negocio para el manejo, procesamiento, almacenamiento, comunicación y archivado de información que una organización ha desarrollado para apoyar en sus operaciones.[2, p. v]

Selección de los controles

Los controles pueden ser seleccionados según los requisitos de seguridad de la organización, para poder satisfacer las necesidades y la aceptación de riesgo.
Los controles que indica esta norma se pueden considerar como guías en la gestión y pueden ser aplicables en la mayoría de las organizaciones.

Desarrollando las propias directrices

La norma se considera como un punto de partida para la implementación de controles, existirían escenarios donde no todos los controles son factibles, y se pueden ir agregando más controles que no mencionados según la conveniencia.

Consideraciones del ciclo de vida
Los sistemas de información tienen ciclos de vida dentro de los cuales son concebidos, especificados, diseñados, desarrollados, probados, implementados, usados mantenidos y finalmente retirados del servicio y desechados. La seguridad de la información debe ser considerada en todas las etapas.[2, p. iv]

Apartados de control y categorías de seguridad

La norma incluye 14 apartados de control de seguridad que contienen en conjunto un total de 35 categorías principales de seguridad y 114 controles.

1. Política de seguridad de la información
   1.1. Gestión de la dirección para la seguridad de la información
2. Organización de la seguridad de la información.
   2.1. Organización interna
   2.2. Dispositivos móviles y trabajo remoto
3. Seguridad de los recursos humanos
   3.1. Antes del empleo
   3.2. Durante el empleo
   3.3. Terminación y cambio del empleo
4. Gestión de activos
   4.1. Responsabilidad sobre los activos
   4.2. Clasificación de la información
   4.3. Manejo de medios
5. Control de acceso

5.1. Requerimiento del negocio para el control de acceso
5.2. Gestión del acceso de usuarios
5.3. Responsabilidades del usuario
5.4. Control de acceso a sistemas y aplicaciones

6. Criptografía
   6.1. Controles criptográficos
7. Seguridad física y ambiental
   7.1. Áreas seguras
   7.2. Equipo
8. Seguridad de las operaciones
   8.1. Procedimientos y responsabilidades operacionales
   8.2. Protección contra software malicioso
   8.3. Copias de seguridad
   8.4. Registro y monitoreo
   8.5. Control de software operacional
   8.6. Gestión de la vulnerabilidad técnica
   8.7. Consideraciones en la auditoria de sistemas de información
9. Seguridad de las comunicaciones
   9.1. Gestión de seguridad de red
   9.2. Transferencia de información
10. Adquisición, desarrollo y mantenimiento de sistemas
    10.1. Requisitos de seguridad de los sistemas de información.
    10.2. Seguridad en los procesos de desarrollo y soporte
    10.3. Datos de prueba
11. Relaciones con los proveedores
    11.1. Seguridad de la información en las relaciones con los proveedores.
    11.2. Gestión del servicio de entrega del proveedor.
12. Gestión de incidentes de seguridad de la información
    12.1. Gestión de incidentes de seguridad de la información y mejoras
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
    13.1. Continuidad de la seguridad de la información
    13.2. Redundancias
14. Cumplimento
    14.1. Cumplimiento con requerimientos legales y contractuales
    14.2. Revisiones de seguridad de la información

2.1.3 COBIT 5, Un marco de negocio para el gobierno y la gestión de las TI de la empresa

COBIT (Control Objectives for Information and related Technology) es un marco de trabajo holístico para el Gobiernos y Gestión de las tecnologías de información, desarrollado por ISACA (Information System Audit and Control Association).
ISACA es una asociación independiente global sin fines de lucro, comprometida en la adopción de las mejores prácticas en la industria de los sistemas de información. ISACA fue establecida en el año 1969 y tiene presencia en más de 188 países con más de 220 capítulos a nivel mundial.[3]

El marco COBIT 5 se construye sobre cinco claves para el gobierno y la gestión de las TI empresariales:[4, p. 14]

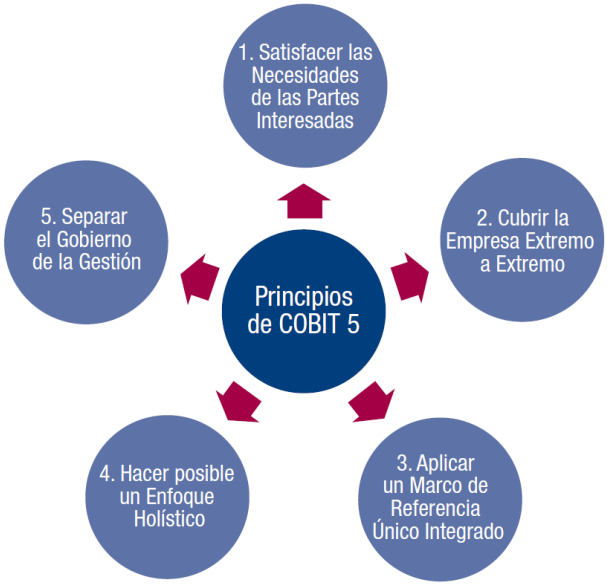

Figura 1 Principios COBIT

Principio 1: Satisfacer las necesidades de las partes interesadas
El deber ser de las organizaciones es para crear valor para sus accionistas, esto significa obtener beneficios mediante la optimización de los recursos y la optimización del riesgo, dichos beneficios se pueden materializar de diferentes maneras, ya sean beneficios financieros o servicios públicos de calidad, dependerá de la naturaleza de la organización.

Para poder cumplir con este principio COBIT menciona los siguientes tres puntos:

- Realización de beneficios.
- Optimización del riesgo
- Optimización de recursos.

Principio 2: Cubrir la empresa de extremo a extremo

COBIT integra el gobierno de TI con el gobierno corporativo, es decir que los objetivos de TI deben ir alineados los objetivos del negocio. Todos los servicios relevantes de TI ya sea internos o externos deben ir contemplados, así como los procesos del negocio. Se deberá de tener una visión integral y sistémica.
El enfoque de gobierno extremos-a-extremo es representado en la siguiente figura[4, p. 23]:

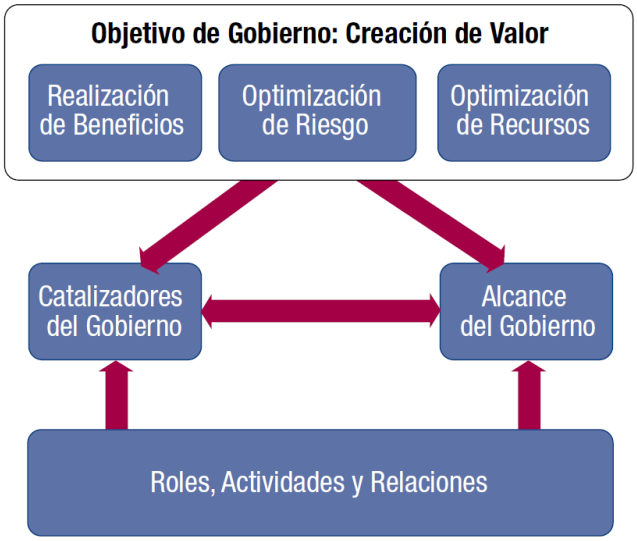

Figura 2 Gobierno y Gestión en COBIT 5

Principio 3: Aplicar un marco de referencia Único Integrado

Es un marco de referencia debido a que se alinea con otros estándares y marcos de referencia relevantes tales como ITIL (Information Technology Infrastructure Library), TOGAF (The Open Group Architecture Framework) y estándares ISO, COBIT es un marco único que sirve como una fuente integrada, guía en un lenguaje común y referencia de base de buenas prácticas.

Principio 4: Hacer posible un enfoque holístico

COBIT posee siete categorías catalizadoras que individual y colectivamente influyen como un todo, los catalizadores son guiados por metas y objetivos de alto nivel.

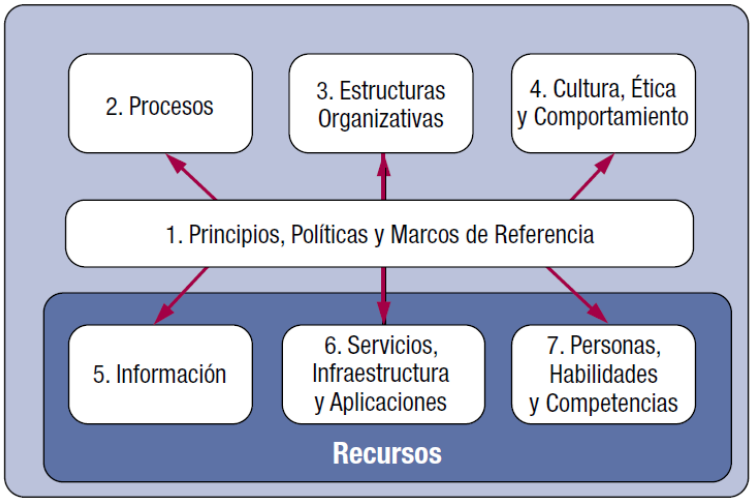

Figura 3 Catalizadores Corporativos

Principio 5: Separar el gobierno de la gestión

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.
La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.[4, p. 31]

El modelo de referencia de procesos COBIT no es prescriptivo, pero recomienda que las organizaciones implementen procesos de gobierno y gestión de manera que todas las áreas sean cubiertas, tal como se muestra en el siguiente diagrama:

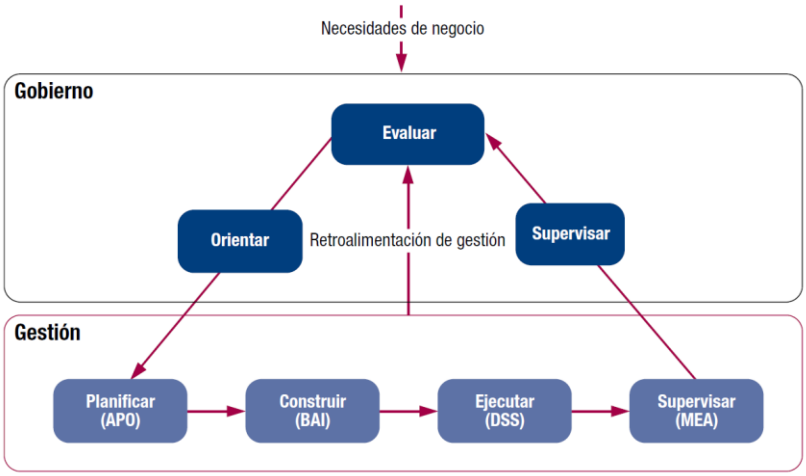

Figura 4 Áreas claves de gobierno y Gestión

Modelo de referencia de procesos

COBIT posee en total 37 procesos de gobierno y gestión que se describen en la siguiente figura, los detalles de cada se pueden consultar en la guía "COBIT 5: Procesos Catalizadores".[4, p. 33]

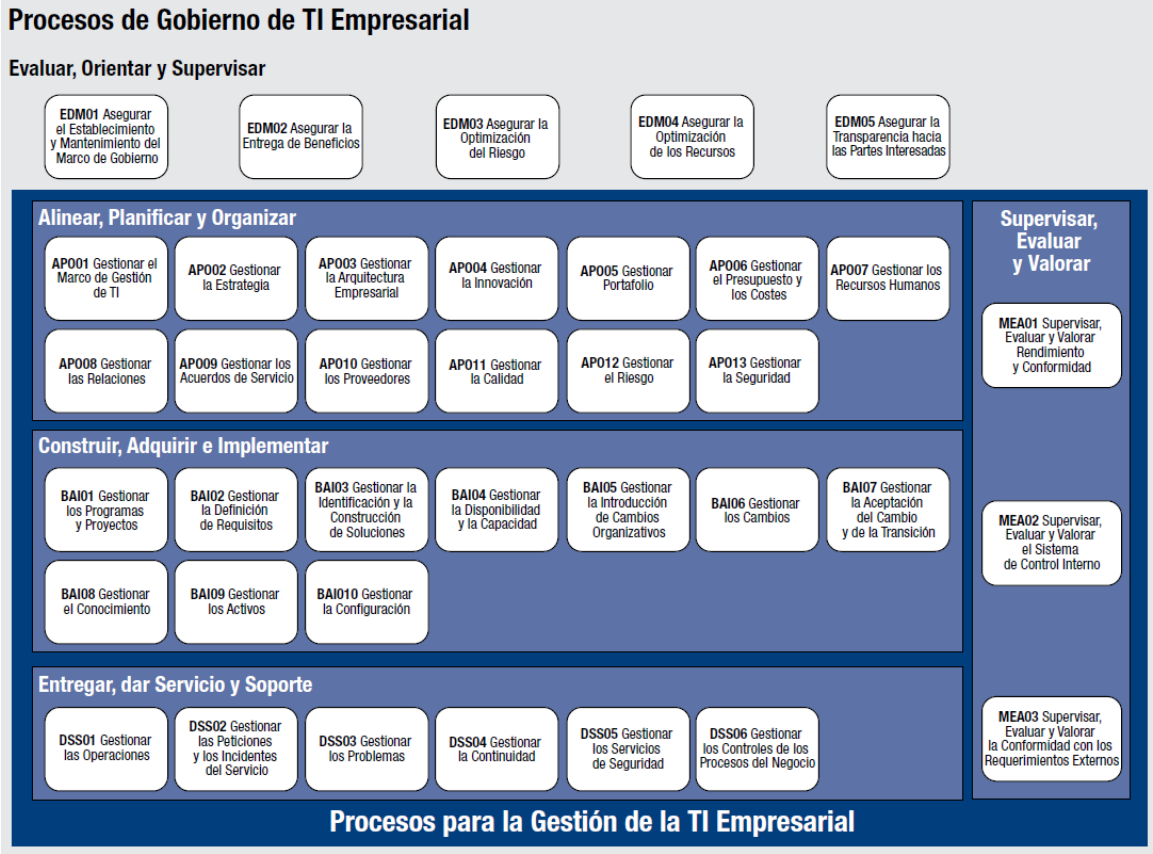

Figura 5 Procesos de Gobierno de TI Empresarial

2.1.4 PCI DSS

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) fue desarrollado para incentivar y mejorar la seguridad de los datos de los tarjetahabientes, y facilitar la adopción de medidas consistentes de seguridad a nivel global. PCI DSS provee una línea base de requerimientos técnicos y operacionales diseñado para proteger los datos de las cuentas, este estándar aplica a todas las entidades las cuales procesan pagos de tarjetas de crédito y todas aquellas que almacenan, procesan y transmiten datos de tarjetahabientes o datos sensibles de autenticación[5, p. 5].

A continuación, se describen las seis categorías y sus doce requerimientos de la versión 3.2.1:

Construir y mantener una red segura	1. Instalar y mantener las configuraciones de un firewall para proteger los datos. 2. No utilizar los parámetros de sistema y contraseña de por defecto de terceros,
Proteger la información del tarjetahabiente	3. Proteger los datos almacenados de los tarjetahabientes 4. Cifrar las transmisiones de redes abiertas y redes públicas.
Mantener un programa de gestión de vulnerabilidades	5. Proteger todos los sistemas en contra de software malicioso y actualizar antivirus. 6. Desarrollar y mantener sistemas de seguridad y aplicaciones.
Implementar fuertes medidas de controles de acceso	7. Restringir el acceso a los datos según los requerimientos del negocio. 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del tarjetahabiente.
Monitorear y probar las redes	10. Monitorear todo acceso a los recursos de red de los datos. 11. Probar con regularidad la seguridad de los procesos y sistemas.
Mantener una política de seguridad de la información	12. Mantener una política de seguridad de la información para todo el personal.

Tabla 1 Requerimientos PCI DSS

2.2 Metodología dinámica de gestión de riesgos

Antes de desarrollar el tema y para un mejor entendimiento es importante definir el significado de la palabra “metodología”. Según el diccionario de la real academia española viene de la palabra compuesta griego μέθοδος méthodos 'método' y -logía. Palabra femenina cuyo significado es:

1. Ciencia del método.

2. Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal.

Esto nos lleva la necesidad de referenciar que significa la palabra “método”. Según el diccionario de la real academia española* viene del vocablo latin, methŏdus y este del griego, μέθοδος méthodos. Cuyo significado en masculino significa:

1. Modo de decir o hacer con orden.
2. Modo de obrar o proceder, hábito o costumbre que cada uno tiene y observa.
3. Obra que enseña los elementos de una ciencia o arte.

Habiendo entonces definido la palabra metodología podemos reducirla para usos prácticos en la forma en que se debe realizar alguna tarea, trabajo, análisis, investigación, diseño o evaluación de cualquier índole.

Para el caso en particular de este apartado, se entenderá que es la forma ordenada de realizar los análisis, evaluación y gestión de riesgos los cuales cambian a medida surgen nuevos productos y tecnologías de la información siendo estos utilizados por empresas y organizaciones para el desarrollo de sus actividades y consecución de los objetivos organizacionales.

La metodología de gestión de riesgos no puede ser estática pues el uso de nuevas tecnologías de la información generan cambios en los procesos y actividades de las organizaciones tales como el desplazamiento de sistemas antiguos, los cuales deben de ser migrados por múltiples razones como lo son la eficiencia, capacidad, alcance e integración con otras herramientas tecnológicas más recientes, las cuales pueden estarse evaluando por una necesidad de su implementación debido a que el negocio necesita de esta tecnología o simplemente porque los objetivos organizacionales lo requieren. Cuando los sistemas de la información cambian su tecnología estos cambian su forma de interactuar con sistemas, procesos y personas generando así nuevas áreas de vulnerabilidades que deberán ser analizadas y evaluadas para definir el impacto que estas tendrán en los activos y objetivos de la organización. El no hacerlo sería una clara violación al espíritu de la misión y visión de la organización pues lo que esto traerá en consecuencia es la afectación directa en la consecución de los objetivos organizacionales lo cual hoy en día se conoce como “riesgo” organizacional.

Históricamente el ser humano tiene la tendencia a mejorar lo que hace, pero se basa en las experiencias pasadas que han funcionado y este le agrega algo o lo mejora de alguna forma. Es por ello que para definir el camino de la creación de una metodología dinámica de gestión de riesgos de las TIC’s nos basaremos y apoyaremos en los marcos de trabajos ampliamente aceptados, promulgados y respaldados por organismos internacionales a nivel global pues estos tienen un nivel de madurez avanzada durante décadas que permite sentar las bases sobre las cuales la dinámica de cada empresa decidirá que le es aplicable y en qué

grado o nivel de implementación y alcance los aplicará basados en su disponibilidad de recursos según decida el gobierno de IT de la organización.

2.2.1 Definición de las amenazas y vulnerabilidades dinámicas

Antes de entrar a definir la dinámica de las amenazas y vulnerabilidades relacionadas con la informática es importante definir cada una de ellas en el mismo contexto.

Amenaza: Es toda aquella que puede afectar los activos informáticos de una organización de forma negativa, es decir una amenaza consiste en una acción adversa sobre un activo realizada por una agente de amenaza.

Vulnerabilidades: Es toda aquella debilidad que posee un activo, la cual puede ser explotada por una amenaza.

Es de hacer notar que todo activo informático sea este un equipo físico ó sistema aplicativo posee intrínsecamente debilidades generales y propias, las generales pueden ser asociadas a su naturaleza de construcción, uso o aplicación; y las propias pueden ser asociadas a las características del diseño propiamente y forma de operación.

Las amenazas y vulnerabilidades no son estáticas si no por el contrario son del tipo variante y creciente en sus alcances y capacidades manteniendo los niveles de afectación pasados es decir de sus primeras versiones. Pero ¿cómo es que cambian a lo largo del tiempo? Esto es debido a que todo lo creado por el hombre es imperfecto y basado en ello que dichas creaciones son conceptualizadas, desarrolladas y creadas por un grupo de personas de una región y en un tiempo específico de la vida las cuales dependen de las experiencias y alcance que se hayan definido en dicha época. Por ello todo es relativo en el tiempo ya que lo que pudo haber sido la opción más segura en un tiempo puede que no lo sea en tiempos más modernos, como muestra de ello tenemos los sistemas criptográficos los cuales se están renovando a medida el poder de la computación aumenta pues la fortaleza de su seguridad reside en la complejidad de operaciones matemáticas que se deben hacer para descifrar la información.

2.2.2 Principales amenazas y vulnerabilidad de TI para los sistemas de información

Existen un sin fin de amenazas y vulnerabilidades para activos de información, el listado incluido tratara de ejemplificar los más importantes durante la última década hasta la fecha de realización del documento.

Las amenazas y vulnerabilidades de los activos informáticos no solo afectan la parte digital del tratamiento de los datos sino también la parte física de los mismos, teniendo en cuenta

desde la seguridad física, energética, ambiental hasta la parte operativa de la disponibilidad, integridad y confidencialidad de los datos.

Es importante mencionar que existen organizaciones especializadas en mantener un listado actualizado de las vulnerabilidades reportadas por todas las empresas de seguridad, de la comunidad de desarrolladores, especialistas y expertos en el ramo de las tecnologías de la información, vulnerabilidades y exposiciones comunes tal como cve.mitre.org

Estas pueden ser encontradas en Internet, colocando en un buscador palabras claves como "vulnerabilidades informáticas" de las cuales aparecen indexados miles de fuentes de información de todo tipo y nivel de complejidad en la presentación de dicha información, es un hecho de que existe una base de fuentes especializadas y constantes las cuales pueden dar una sólida base de investigación en el historial de las mismas. Entre ellos se puede contar con las empresas de antivirus, desarrolladores de sistemas operativos y aplicaciones, manufacturadores de equipos de informática en toda su amplia variedad, centros de respuesta ante amenazas informáticas, etc.

Amenazas y vulnerabilidad

Físicas:

- Ubicación geográfica de las instalaciones, amenazas asociadas a los factores ambientales del área.
- Descuido del control de acceso al perímetro del edificio, a los nodos de red, al centro de datos, a las terminales de la organización y demás sitios críticos a la organización.
- Descuido del control de ambiente en el centro de datos.
- Descuido del control de acceso a los equipos y sistemas informáticos.
- Descuido del control de Prevención, detección y supresión de incendios
- Descuido del control de la calidad de energía y respaldo.

Digitales:

- Descuido del control de actualización y parcheo de aplicaciones y sistema operativo.
- Descuido del control de endurecimiento de configuraciones de aplicaciones y sistema operativo
- Descuido del control de seguridad en equipos de red, aplicaciones y servidores.

- **Credenciales débiles**: Manejo de contraseñas cortas y no basadas en una política de seguridad apropiada.
- **Ingeniería Social**: Proceso fraudulento de intentar adquirir información sensible por medio de engaños al momento de una conversación telefónica o presencial,

incluyendo la investigación y reconocimiento tanto del área como de personal de la organización.

- **Phishing**, Proceso fraudulento de intentar adquirir información sensible por medio de engaños enviados por medio de correos electrónicos preparados con enlaces especializados para comprometer la seguridad del equipo por medio de malware.
- **Malware**, programa malicioso y perjudicial para una computadora y pueden ser virus del tipo troyanos, gusanos, spyware.
- **Zero-Days**, Son aquellas vulnerabilidades que no son conocidas y para las cuales no se tiene remediación disponible todavía.
- **Inyección SQL**, Normalmente asociado a una mala práctica de no filtrado de comandos de consultas en el código del programa.
- **Servicios Web**, falta de implementación de buenas prácticas desarrollo seguro servicios web.
- **Intercepción**, Hombre en el medio - "Man in the middle"
- **Ataque DDoS**, Ataques de denegación de servicios, normalmente desde el exterior.
- **Configuración de seguridad incorrecta** - Malas prácticas de TI, configuraciones por defecto de las diferentes tecnologías implementas para los sistemas en cuestión.

2.2.3 Análisis de riesgo

Antes de continuar con el análisis de riesgo es necesario definir "riesgo", el cual según el diccionario de la real academia española viene del vocablo latín, pericŭlum cuyo significado en masculino significa:

1. Riesgo o contingencia inminente de que suceda algún mal.
2. Lugar, paso, obstáculo o situación en que aumenta la inminencia del daño.

Lo que se traduce a la vida cotidiana en que "el riesgo es el potencial de pérdida incontrolada de algo de valor" lo cual nos lleva inmediatamente a pensar en ¿qué hacer con ese riesgo, es alto? ¿se puede quitar? ¿cómo reducir o mitigar ese riesgo, pero hasta qué nivel? Definitivamente si se pueden hacer muchas acciones para controlar y mitigar el riesgo asociado a los equipos informáticos sin olvidar que el riesgo no puede ser eliminado, pero debe ser gestionado. Una de las partes más importantes es definir el "apetito de riesgo de la empresa", el cual es el nivel de riesgo aceptado por la organización para operar o prestar un servicio que dependan de sistemas informáticos, pues por medio de sus operaciones crea valor, siendo necesario que la organización deberá de definir qué debe hacer con el riesgo, eligiendo si lo reducirá, aceptara, transferirá o evitara y es ahí particularmente donde los resultados de un análisis de riesgo le darán una visión holística importante del alcance e impacto de cada riesgo para la toma de decisiones que permitirá definir estratégicamente, técnicamente y operativamente cómo se tratara el riesgo.

Para determinar si un sistema o equipo informático es seguro o no, se debe de realizar un análisis de riesgo el cual nos va a dar información de a qué tipo de amenazas y vulnerabilidades se está expuesto al tenerlo y utilizarlo en diferentes escenarios tanto internos como externos. Para realizar un análisis de riesgo se pueden ocupar diferentes técnicas y herramientas incluidas en los diferentes marcos internacionales de seguridad informática, para luego darles seguimiento por medio de un "Sistema de Gestión de Seguridad Informática" el cual mantendrá un registro de los análisis e identificaciones de amenazas y vulnerabilidades al inicio y durante su ciclo de uso, permitiendo a éste el ser actualizado a medida nuevas tecnologías son agregas al entorno de la organización, la cual no solo necesariamente están relacionados con la parte informática si no con las estrategias y operaciones de la misma.

¿Para qué sirve un análisis de riesgo?
La evaluación de riesgos es para:

- Identificar los activos de una empresa.
- Asignar valores a los activos.
- Identificar las vulnerabilidades y amenazas de los activos.
- Calcular sus niveles de riesgo asociados.
- Estimar pérdidas y daños potenciales.
- Estima la probabilidad de un ataque.
- Proporcionar soluciones.

Elementos de evaluación de riesgos

- Alcance
- Descripción de los activos del área de evaluación, sistema, región, proceso
- Amenazas
- Vulnerabilidades
- Probabilidad
- Impacto
- Informe de evaluación de riesgos

¿Como se realiza un análisis de riesgo?
Un análisis de riesgo básico se puede realizar enumerando todas las posibles causas de amenazas y eventos no deseados al activo informático definido en el alcance del análisis, detallando las principales características de sus vulnerabilidades en función de sus componentes principales, definiendo posteriormente la probabilidad de ocurrencia para poder evaluar el nivel de impacto y afectación al mismo, sea esta de forma cuantitativa o cualitativa, permitiendo así incluir el detalle de las contra medidas para mitigar el nivel de riesgo analizado.

2.2.3.1 Guía de análisis de riesgo

1- Definir quienes estarán involucrados

Se recomienda si fuera posible escoger a personal calificado en tecnologías de la información, expertos en las áreas donde se encuentran los activos y al menos un representante de la alta dirección o delegado.

2- Definir el alcance del análisis

Es muy necesario dejar claro desde un inicio que activos serán incluidos en análisis de riesgo porque de lo contrario se puede tratar de abarcar más de lo que realmente es necesario o es posible en las primeras etapas, por lo que se recomienda enumerar los sistemas de forma general y luego ir detallando los por menores de cada sistema.

3- Identificar las amenazas y probabilidad

Es requerido definir un grupo básico general de amenazas y probabilidad de ocurrencia sobre cada activo informático como primera opción, luego puede detallarse un grupo más detallado con mayor nivel de atención.

No todas las amenazas les aplican a todos los activos informáticos y la probabilidad de ocurrencia varía en función del tipo de activo, definitivamente habrá amenazas comunes, pero también habrá amenazas muy propias de cada activo que no aplican a las demás debido a su tipo de función y operación.

4- Identificar las vulnerabilidades

Es muy importante que las debilidades del activo sean claramente conocidas y definidas tanto en operación como en reposo, ya que una vez identificadas será necesario el conocer e investigar qué nivel de explotación real tienen, pues de esa manera se podrá tener en cuenta si vale la pena o no tomarlas en cuenta para la inclusión en la matriz de riesgos la cual deberá de contar con su consecuente medida de mitigación.

5- Evaluación del riesgo

Los riesgos de los activos se evalúan en función de los objetivos definidos por las organizaciones y su personal clave.

Los riesgos de TI se pueden evaluar en una reunión con todas las partes interesadas para definir si se harán de forma cualitativa o cuantitativa.

Los principales tipos de evaluación de riesgos:

- **Cualitativo:** Basado en escenarios, Reputación. Se basa en obtener una impresión general de los riesgos para calificarlos. El proceso utiliza términos subjetivos como bajo, medio, alto y crítico.

- **Basado en escenarios:**
    - Desarrollar escenarios de riesgo
    - Reúna expertos de la compañía.
    - Trabaja a través de los escenarios
    - Clasifique la gravedad de las amenazas y calcule la probabilidad
    - Rango de efectividad de las contramedidas

Para calcular el valor de riesgo de un activo informático se puede utilizar la relación siguiente:

Riesgo = probabilidad x impacto

MATRIZ DE RIESGOS CUALITATIVA		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD DE OCURRENCIA	Baja	MEDIO	ALTO	CRÍTICO
	Media	BAJO	MEDIO	ALTO
	Alta	BAJO	BAJO	MEDIO

Figura 6 Matriz de riesgo cualitativa

- **Cuantitativo:** Está relacionado con dinero e impacto financiero.

Se requiere:

- Calcular la expectativa de pérdida única (SLE - Single Loss expectancy)
- Determinar la tasa anual de ocurrencia (ARO - Annual Rate of Occurrence)
- Calcular la expectativa de pérdida anual (ALE - Annual Loss Expectancy)

$$ALE = SLE \times ARO$$

Propósito de los valores de ALE

- Ayuda a clasificar los riesgos
- Los riesgos más dañinos deben abordarse primero
- Ayuda a determinar la cantidad para gastar en contramedidas
- La contramedida no debería costar más que el valor ALE
- Ayuda a crear un presupuesto de seguridad
- Ayuda a la gerencia a conocer la cantidad que debe presupuestarse para proteger los activos

- **Cuantitativos:** Asignan un valor numérico al riesgo. (por ejemplo, de 1 a 10 con su correspondiente designación de rangos) tomando en cuenta el costo monetario del impacto y asignando de un valor numérico a la probabilidad de ocurrencia (en porcentaje o basado en una escala numeral) se define un rango de asignación al producto de la probabilidad x el impacto.

Riesgo = probabilidad x impacto

De 1 a 4 = **Bajo**
De 5 a 6 = **Medio**
De 7 a 8 = **Alto**
De 9 y 10 = **Crítico**

MATRIZ DE RIESGOS CUANTITATIVA	IMPACTO			
PROBABILIDAD DE OCURRENCIA en %		< $5,000	> $5,000 < $10,000	> $10,000
	<=33%	MEDIO	ALTO	CRÍTICO
	>33% <66%	BAJO	MEDIO	ALTO
	>=66%	BAJO	BAJO	MEDIO

Figura 7 Matriz de riegos cuantitativa

6- Mitigar el riesgo

Una vez identificados los niveles de riesgo el siguiente paso es definir las medidas de mitigación las cuales sería el determinar los controles apropiados para aceptar, reducir, transferir o evitar la ocurrencia de riesgo o el nivel de impacto. (se puede complementar con el uso de una matriz de riesgo).

2.2.4 Evaluación de impacto a los objetivos de la organización

La evaluación del impacto a los objetivos de la organización están relacionados directamente con la eficacia y eficiencia de las medidas de mitigación de los riesgos informáticos, pues la misión y visión de la organización toma entre sus insumos todos los activos que la ayudaran a crear "valor" como resultado de sus operaciones basados en los objetivos planificados por la dirección de la organización, si los activos informáticos fallan en alguna medida, todos los procesos de la organización podrán ser afectados en diferentes niveles y proporciones según sea su nivel de integración y dependencia con los mismos.

2.2.4.1 Guía de evaluación de impactos establecidos

1- Priorizar por nivel de Impacto

De los resultados del análisis de riesgo, se toman todos los elementos incluidos en el análisis para priorizar de mayor a menor basado en el nivel de impacto obtenido.
La organización por medio de una mesa evaluadora deberá de ponerse de acuerdo para evaluar qué riesgos deben ser atendidos y controlados con la mayor prontitud pues estos podrán afectar las operaciones de la organización de manera seria y en algunas ocasiones de forma irremediable. Esta decidirá en qué medida los objetivos de la empresa pueden ser afectados.

2- Definir plan de mitigación

La mesa evaluadora deberá de definir y evaluar todas las opciones posibles para disminuir el nivel de impacto basado primordialmente en que es lo más importante para organización, entendiéndose como factores de importancia: Su imagen, su calidad de productos y servicios, su personal, sus instalaciones, etc.
Esta deberá de preparar y recomendar planes para cada uno de los casos permitiendo así tener una línea clara de acción en cada caso.

3- Seguimiento de resultados

Es necesario revisar periódicamente si los planes de mitigación son actuales y mantienen su efectividad al menos 1 vez por año. Es por ello que se deberán de revisar los análisis de riesgos y su consecuente nivel de impacto cada vez que un nuevo cambio a los sistemas es realizado, pues puede cambiar en gran o menor medida permitiendo así revaluar el impacto a los objetivos, los cuales podrían permitir una menor inversión en el plan de mitigación, aunque así mismo estos pueden incrementar basados en el aumento del nivel de riesgo.
Es importante detallar que el seguimiento incluye la revisión de los eventos e incidentes de seguridad informática pues de esa forma se puede confirmar si los planes y medidas de mitigación existen y si estas son suficientes o no.

4- Recomendaciones

La mesa evaluadora deberá de realizar sus recomendaciones a la dirección y todos los interesados dejando por escrito un resumen de incidentes y su correspondiente reporte de actividades para todos los diferentes niveles elegidos de impacto, asegurándose de que estas contengan nuevas y mejores formas de como para mitigar que un impacto no sobrepase el nivel de afectación preestablecido a los objetivos.

2.3 Metodología para el monitoreo y evaluación de desempeño.

Se puede contar con un amplio y minucioso análisis de riesgo para definir la mejor forma de mitigar las amenazas y vulnerabilidades de los activos informáticos. Pero se corre el riesgo de quedar estancado en obtener una imagen estática de las condiciones y sistemas

específicos en un periodo en particular lo cual no asegura que las medidas de mitigación continúan siendo eficaces.
Es por ello que es necesario darle continuidad a la gestión de riesgo por medio de un sistema de monitoreo y evaluación del desempeño de las contramedidas de mitigación.

La gestión de riesgos informáticos no es un sistema estático que ejecuta tareas y actividades específicas en determinados periodos predefinido. Si no que debe hacerlo permanentemente, siempre que exista un cambio de cualquier tipo en los sistemas informáticos incluidos aplicaciones e infraestructura.

La gestión de riesgos debe enfocarse en tener las mejores capacidades de monitoreo y evaluación que aseguren óptimas condiciones de detección temprana y de pérdida de capacidad en todos aquellos factores en los que se basa la confianza para definir si los sensores de detección están correctamente calibrados para su misión principal.

Se deberá realizar un grupo básico de pruebas que aseguren que los sensores de monitoreo están ajustados según los perfiles de respuesta esperados, lo que conlleva a medir y registrar los resultados de los mismo, permitiendo comparar el resultado del desempeño a lo largo del tiempo. Es importante mencionar que este grupo de pruebas bases deberá de estarse actualizando en función de las nuevas amenazas y vulnerabilidades que aparezcan, es decir el grupo de pruebas deberá de contemplar una evaluación de versionamiento y nuevas capacidades que deberán de ponerse a disposición en el abanico de contramedidas definidas.

2.3.1 Monitoreo de planes de implementación

Las organizaciones poseen una amplia cantidad de sistemas los cuales utilizan una diversidad de sensores para monitorear tanto sus operaciones del día a día como las condiciones de seguridad, siendo estos los normalmente olvidados o de menor prioridad pues aparentemente no representan una clara aportación a los objetivos de la organización. Por ello es de vital importancia el monitoreo de los parámetros de seguridad asociados a los activos informáticos, pues es de ahí que depende su estabilidad y capacidad para procesar todo el trabajo productivo, es por ello que se define a continuación un plan general básico de monitoreo:

Plan de monitoreo

1. **Alcance de monitoreo base**

Se deberán de incluir todos aquellos activos definidos en el análisis de riesgo general de la organización incluyendo todos aquellos sistemas auxiliares que dan soporte a los mismos.

2. **Parámetros del monitoreo base**

Se incluirán al menos los parámetros básicos requeridos para la operación óptima que permita el cumplimiento de los objetivos específicos designados particularmente al tipo de activo informático, tales como reportes de las consolas de antivirus, anti malwares, detección e intrusión, control y operación del tráfico interno y externo de red, de sistemas de autenticación e identidad, y de todos aquellos asociados a políticas de seguridad impuestas por la organización.

3- Monitoreo base

Deberá de incluir capacidades de monitoreo de parámetros en tiempo real, notificaciones automáticas bajo condiciones específicas preestablecidas, permitiendo así el modificar las condiciones del tipo y tiempo de confirmación para alarmas recibidas desde los equipos y sistemas las cuales serán enviadas a los administradores de los sistemas de operaciones y de seguridad, para que estos evalúen la condición y tomen acciones sobre estas.

4- Resultados del monitoreo base

Deberán ser revisados y analizados por personal idóneo, estos podrían incluir condiciones de la operación de la infraestructura informática, sin embargo para facilitar su revisión estos deberán de ser correlacionados con las alarmas y registro de acciones de los sensores de seguridad en dicha infraestructura informática, pues se deberá de dar seguimiento a los eventos e incidentes registrados hasta que quede claro y se tomen decisiones operativas y tácticas para dar por cerrado cada caso en particular.

5- Mejoras de monitoreo

Las capacidades actuales deberán ir cambiando a medida que los activos informáticos lo hagan. Una simple actualización del operativo o versionamiento de la aplicación podrá generar otras capacidades y vulnerabilidades al mismo activo informático y es por ello que se deberá confirmar si las capacidades actuales son suficientes para mantener cubierto el monitoreo de seguridad y operaciones con el fin de asegurar la pronta detección y respuesta a eventos e incidentes de seguridad informática.

2.3.2 Establecer plan de auditoría

Es de vital importancia el tener claramente definidos el alcance y capacidad de los equipos y sistemas de monitoreo utilizados para la seguridad informática, pues de esa forma se podrá realizar una revisión de las capacidades y resultados de cumplimiento de los mismos.

Plan de auditoría del sistema de monitoreo

1- Alcance de la auditoría

Deberá de incluir todos aquellos sistemas, sean estos aplicativos, equipos físicos y bases de datos definidos, concebidos y utilizados para darle el adecuado registro de los eventos e incidentes de seguridad asociados a los procesos e infraestructura informática.

2- Parámetros auditables

Serán todos aquellos que permitan definir el grado de afectación o de riesgo informático de todos los activos informáticos de la organización. Permitiéndole enumerar y ponderar el nivel de importancia que tendría el mismo para el aseguramiento y el cumplimiento de las políticas de seguridad informáticas definidas por la organización.

3- Proceso de auditoría

Se deberán de revisar y confirmar el cumplimiento de todos parámetros auditables predefinidos, permitiendo así el ponderar el nivel de cobertura y cumplimiento específico para cada parámetro asociado a cada activo informático de la organización. Esta deberá de ser realizada por personal idóneo al área de informática.

4- Reporte de auditoría

Deberá de contener los hallazgos y recomendaciones pertinentes que permitan a los departamentos de seguridad y operaciones el solventar y mejorar el nivel de aseguramiento y respuesta ante los eventos e incidentes informáticos asociados a cada activo informático de la organización.

5- Recomendaciones de auditoría

Las recomendaciones deberán ir acompañadas del respectivo costo para poder así informar a la dirección de la organización, permitiéndole así decidir las respectivas autorizaciones y definiendo el curso de aplicación de dichos recomendables.
Las recomendaciones deberán de incluir el contexto y posibles escenarios de afectación a ser evaluados junto con su análisis de riesgo individual, lo cual permitirá conocer de forma específica la condición de seguridad actual y futura permitiendo así el evaluar de mejor forma y a la vez el tomar una mejor decisión sobre las inversiones o rumbos para mitigar los posibles riesgos informáticos para cada activo informático.

2.3.3 Plan de investigación de nuevas amenazas

Es definitivamente requerido el invertir tiempo y recursos para poder contar con la más actualizada información disponible, por lo que toda organización preocupada por el mejoramiento de las capacidades de sus sistemas de detección, reacción y monitoreo de amenazas, necesita participar en conferencias, campamentos técnicos y pruebas de concepto de todas aquellas nuevas aplicaciones y equipos que permitan dicho

mejoramiento.

Existen anualmente una gran cantidad de conferencia internacionales las cuales cuentan con una adecuada cobertura de proveedores los cuales demuestran y explican todas las novedades desarrolladas las cuales integran hoy en día no solo las capacidades de monitoreo, sino que junto con la automatización de procesos y la inteligencia artificial definir la respuesta del sistema cuando una particular condición insegura es detectada.

Como referencia de estas conferencias se puede mencionar:

- https://www.ciscolive.com/us.html
- https://www.gartner.com/en/conferences/calendar
- https://www.cybertechisrael.com/program
- https://www.isaca.org/training-and-events/conferences
- https://www.oracle.com/openworld/
- https://www.vmworld.com/en/us/index.html
- https://www.ieee-security.org/TC/SP2020/index.html
- https://www.sans.org/cyber-security-summit/
- https://www.rsaconference.com/
- https://www.defcon.org
- https://www.blackhat.com/
- https://www.ibm.com/events/think/
- https://events.microsoft.com
- https://www.hpe.com/us/en/discover.html
- https://www.exploit-db.com/
- https://gbhackers.com/
- https://www.georgia.org/industries/technology/cybersecurity
- https://www.youtube.com/watch?v=-2XpDe6QBQQ&feature=youtu.be

Varios de los sitios web arriba mencionados transmiten en tiempo real gran parte de los eventos, y otras lo comparten posteriormente por medio del acceso a su biblioteca de videos a demanda. Por lo cual no necesariamente es imprescindible el viajar y participar en el evento para tener acceso a una gran cantidad de información relacionada con la seguridad informática.

Plan de investigación del sistema de monitoreo

1- Alcance de la investigación

La cobertura deberá de incluir las diferentes capas del procesamiento de datos en la infraestructura informática (Nodos de procesamiento, de bases de datos, de redes, de aplicativos, de almacenamiento, etc.).

2- **Parámetros de la investigación**

Todos aquellos que se consideren técnicamente útiles para medir con el menor impacto de las capacidades productivas. Se recomienda hacer una correlación entre los procesos operativos y los incidentes de seguridad para definir nuevas métricas específicas de impacto al proceso productivo (Indicador clave de rendimiento).

3- **Investigación base**

Revisar específicamente cada área de mejora basado en los activos informáticos disponibles.

Existen hoy en día en Internet una cantidad suficiente de empresas que se encargan de ofrecer servicios y productos para la gestionar vulnerabilidades de seguridad, el aprovisionamiento, la configuración, el parcheo aplicado a servidores físicos, virtuales y en la nube.

Permitiendo automatizar parte de la seguridad informática.

4- Reporte de investigación

Deberá de incluir las áreas y puntos investigados, con su propuesta de mejora comparado con lo que se tiene o no se tiene actualmente disponible en los sistemas de la empresa. Se deberá de incluir el valor mínimo teórico calculado del **ROSI** (Return of Security Investment por sus siglas en inglés) lo que se traduciría como la tasa de retorno por la inversión en seguridad lo cual significa el tiempo necesario para recuperar la inversión hecha al implementar alguna medida asociada a la seguridad de los activos informáticos.

5- Recomendaciones futuras de investigación

Definitivamente se deberá de contar con un mapa de ruta que permita priorizar y asegurar la continuidad de la mejora en los sistemas de seguridad informática aplicables a la organización, es por ello que se deberá destacar todo punto válido actual y futuro al entorno o escenarios que la organización podría incluir para el aseguramiento del cumplimiento de los objetivos organizacionales.

3. Metodología de investigación

En el presente capítulo se definirá la metodología planteada para realizar la investigación.

3.1 Tipo de investigación y alcance

La investigación es clasificada de tipo “aplicada”, ya que se analizan los diferentes marcos de trabajo y estándares internacionales, dicha investigación servirá de ayuda en la creación de una guía de trabajo o referencia para poder establecer las estrategias de defensa sobre las diferentes amenazas informáticas.
Además, tendrá un enfoque de tipo cualitativo, debido a que se estará realizando un diagnóstico del estado actual de una organización que hace uso de la tecnología para alcanzar sus objetivos corporativos, descripción y análisis de políticas actúales, procesos de negocio, análisis de riesgo de sus activos informáticos, y las recomendaciones necesarias para poder mitigar riesgos.

3.2 Unidades de análisis y variables

A continuación, se definen los objetos de estudios y las variables que serán investigadas y de los cuales se obtendrá información.

Unidades de análisis, estas comprenderán las organizaciones, políticas, procesos, procedimientos y activos informáticos. Es indispensable tener un enfoque holístico a la organización y sus procesos para el diagnóstico y establecer su propia metodología hecha a la medida para mitigación de riesgos.

Las variables serán el nivel de madurez que la organización tiene en sus procesos según los estándares internaciones y buenas prácticas en la gestión de los activos informáticos y sistemas de información.

Se podrán definir variables cuantitativas tales como el nivel de riesgo y los posibles impactos que puede tener en los objetivos de la organización, cantidad de vulnerabilidades presentes en los diferentes activos informáticos.

3.3 Técnicas e Instrumentos

Los instrumentos utilizados en esta investigación serán cuestionarios hechos al personal clave de las organizaciones, tales como departamento de recursos humanos, directores de operaciones, gerentes de tecnología, jefaturas de informática, control interno, etc. El organigrama y puestos de trabajo dependerá de cada organizaron y los roles de trabajo se pueden distribuir según necesidad.

Se hará una auditoria a los procesos principales del negocio donde los activos informáticos sean clave para poder alcanzar el objetivo de dicho proceso, es por eso la importancia de establecer el alcance de la auditoria.

Se utilizarán herramientas informáticas especializadas en realizar análisis de vulnerabilidades a los activos informáticos, estas herramientas deben de estar actualizadas para poder acabar las diferentes amenazas que se tienen a la fecha presente.

Se establecerá el nivel de riesgo según metodología aceptada, y sus respectivas recomendaciones.

4. Resultados

4.1 Resultado nivel de madurez

Tal como se menciona la norma ISO 27001 en sus requerimientos, primero se debe de conocer el contexto de la organización, objetivos estratégicos, necesidades del negocio y demás.
El marco de trabajo COBIT ayuda en hacer un mapeo de objetivos versus procesos COBIT, todo esto basado en el "Balanced Scorecard" [4, p. 17].

En el capítulo 2 Figura 5 se puede encontrar la descripción de todos los de los procesos catalizadores agrupados en áreas claves tales como Planificar, Construir, Ejecutar y Supervisar.

En esta ocasión se evaluará una mediana empresa, la cual se encarga de venta de artículos de primera necesidad por medio de internet. Para tal ejercicio se asume que ya se conoce el contexto de la organización y se han elegido los procesos COBIT a evaluar los cuales van de la mano con los activos de la organización y el aseguramiento de los sistemas de información.
Cada proceso COBIT posee objetivos y criterios los cuales deberán ser evaluados por los diferentes tipos de auditores, todos las evidencias y resultados deberán ser adecuadamente documentados.
En los anexos se definen a detalle todos los criterios de cada proceso y las herramientas de cuantificación de los resultados.

En la siguiente tabla se observa resultado de dichas evaluaciones a los procesos:

Definición de niveles:

N - 0 % - 15 % → No alcanzado
P - 15 % - 50 % → Parcialmente alcanzado
L - 50 % - 85 % → Ampliamente alcanzado
F - 85 % - 100 % → Totalmente alcanzo

Process ID	Process Name	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Processes for Governance of Enterprise IT - Evaluate, Direct and Monitor							
EDM01	Ensure Governance Framework Setting and Maintenance		F	F	L		
EDM03	Ensure Risk Optimization		F	L			
Align, Plan and Organize							
APO01	Manage the IT Management Framework		F	F	L		
APO07	Manage Human Resources		F	L			
APO10	Manage Suppliers		F	L			
APO12	Manage Risk		F	L			
APO13	Manage Security		F	F	L		
Build, Acquire and Implement							
BAI04	Manage Availability and Capacity		F	F	F	L	
BAI06	Manage Changes		F	F	L		
BAI08	Manage Knowledge		F	F	L		
BAI09	Manage Assets		F	F	L		
BAI10	Manage Configuration		F	L			
Deliver, Service and Support							
DSS04	Manage Continuity		L				
DSS05	Manage Security Services		F	F	F	L	
Monitor, Evaluate and Assess							
MEA02	Monitor, Evaluate and Assess the System of Internal Control		F	L			
MEA03	Monitor, Evaluate and Assess Compliance with External Requirements		F	L			

Tabla 2 Resultado evaluación de procesos

El mismo resultado se puede representar en grafico de tipo radar, esto permite identificar gráficamente los procesos más débiles y poder definir planes de remediación y reevaluación.
Por ejemplo, se puede identificar el proceso de gestión de continuidad y gestión del riesgo poseen valores muy bajos, si no se corrige a tiempo esto puede causar un efecto adverso a los objetivos corporativos.
Todos estos resultados deberán ser presentados al comité ejecutivo para poder priorizar y poder brindar recursos en los planes de remediación.

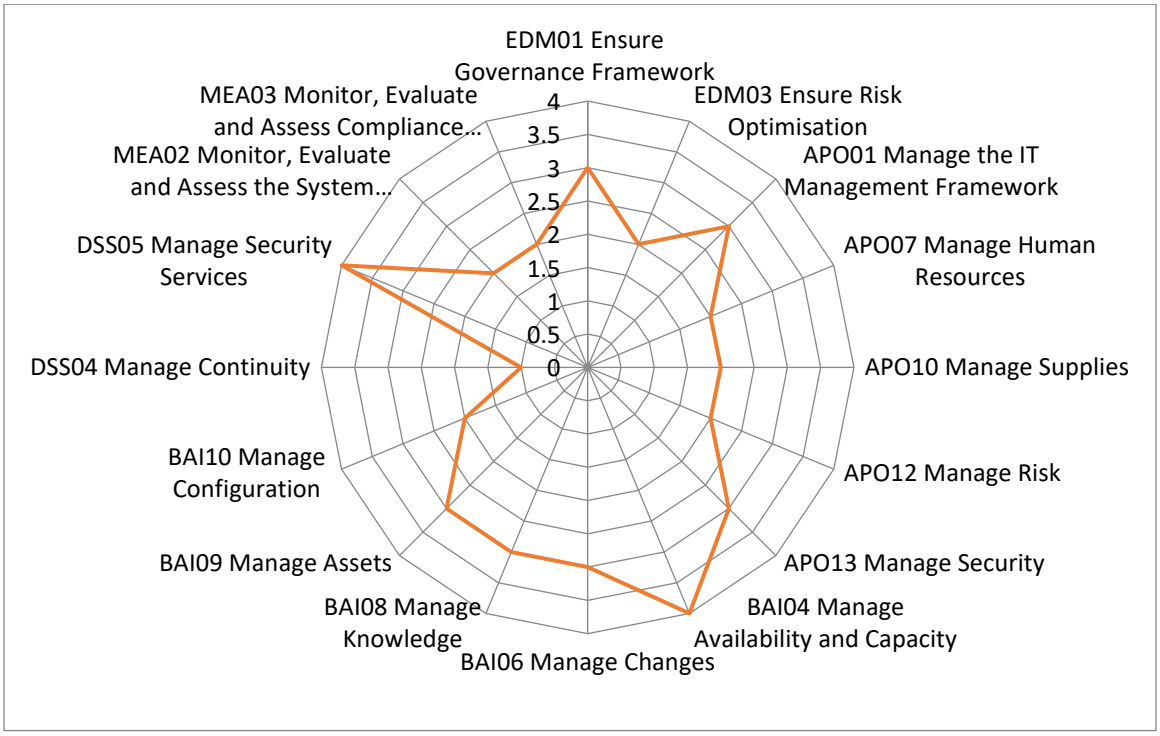

Figura 8 Gráfico de radar

4.2 Análisis de vulnerabilidad

En el capítulo 2, sección 2.2.3 se define el análisis de riesgo, y enlista los pasos necesarios para tal análisis, un paso fundamental es identificar todos aquellos activos informáticos críticos o indispensables para la continuidad del negocio.
En este apartado se detalla el proceso de identificación de las vulnerabilidades.

Siguiendo con el ejemplo de la mediana empresa que se dedica a la venta de artículos de primera necesidad por Internet, se ha identificado como activo critico el servidor de base de datos, el cual corre sobre sistema operativo Oracle Linux Server 7.7 y se tiene la base de datos Oracle 19.3.

Existe una gran diversidad de herramientas para la identificación de vulnerabilidades, las herramientas pueden ser especializadas en las diversas capas, tales como elementos de red, sistemas operativos, bases de datos, servidores web y aplicaciones. La selección de esta estará determinada según necesidad y capacidad de inversión.

Para esta pequeña empresa se ha seleccionado la solución OpenVAS “Open Vulnerability Assessment Scanner”[6] la cual se apega al presupuesto de la organización.

Se utilizará la siguiente versión:

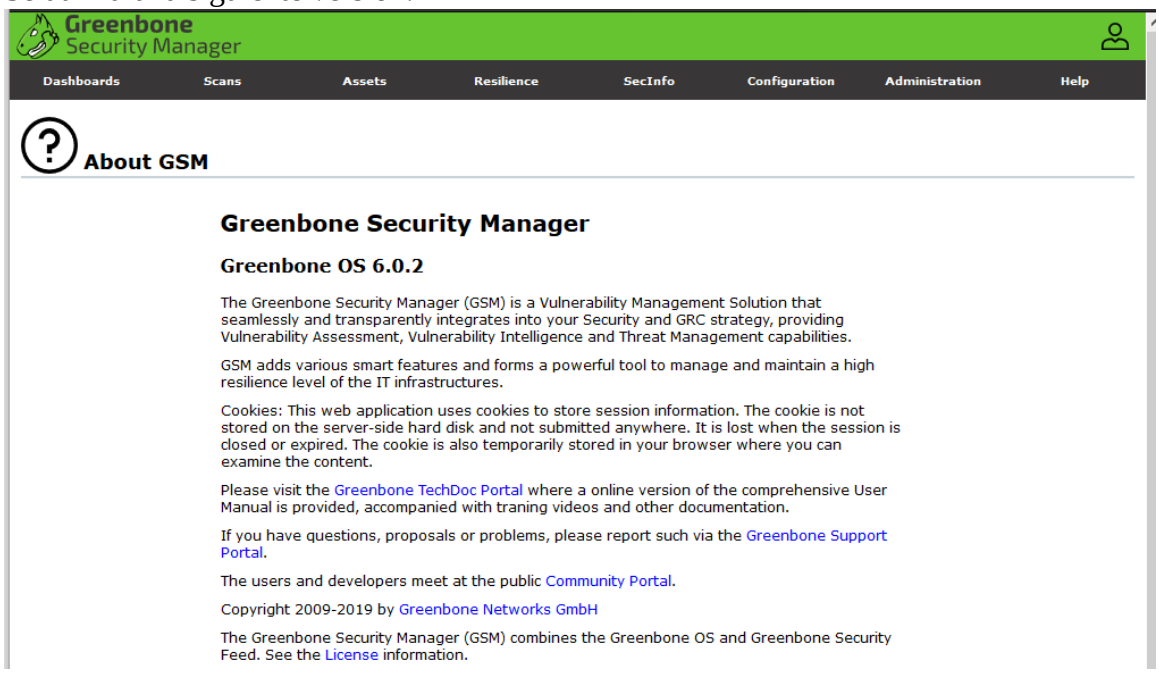

Figura 9 Versión OpenVAS

Y posee la última versión a la fecha de los “feed” los cuales son las bases de datos de las vulnerabilidades conocidas a la fecha. Es importante mencionar que se debe de realizar los escaneos con regularidad y tener actualizados los feed a la última versión.

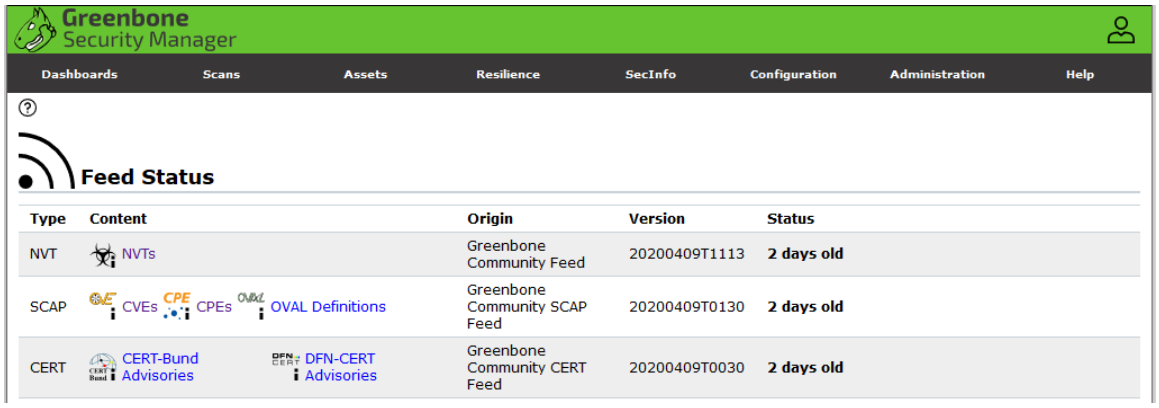

Figura 10 Feed Status

Creación de tarea para análisis:

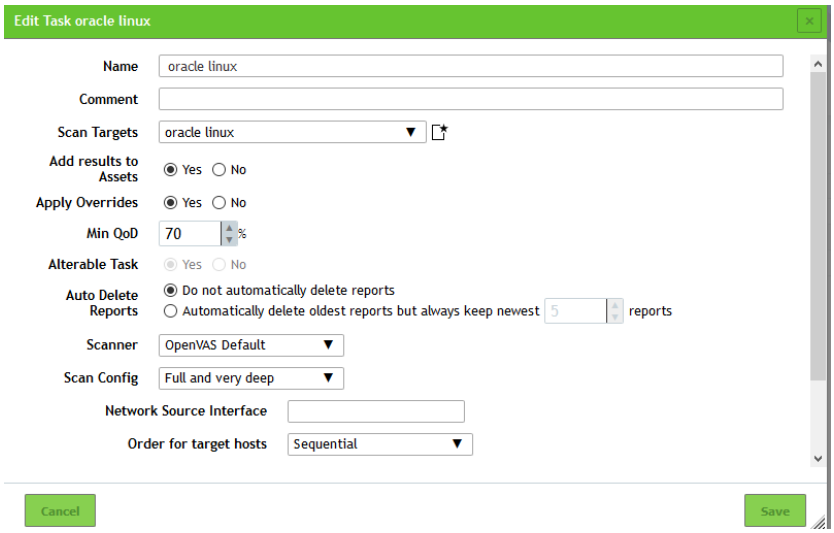

Figura 11 Tarea de análisis

Como resultado tenemos el siguiente reporte, se encontraron 4 vulnerabilidades críticas y 41 de tipo medio.

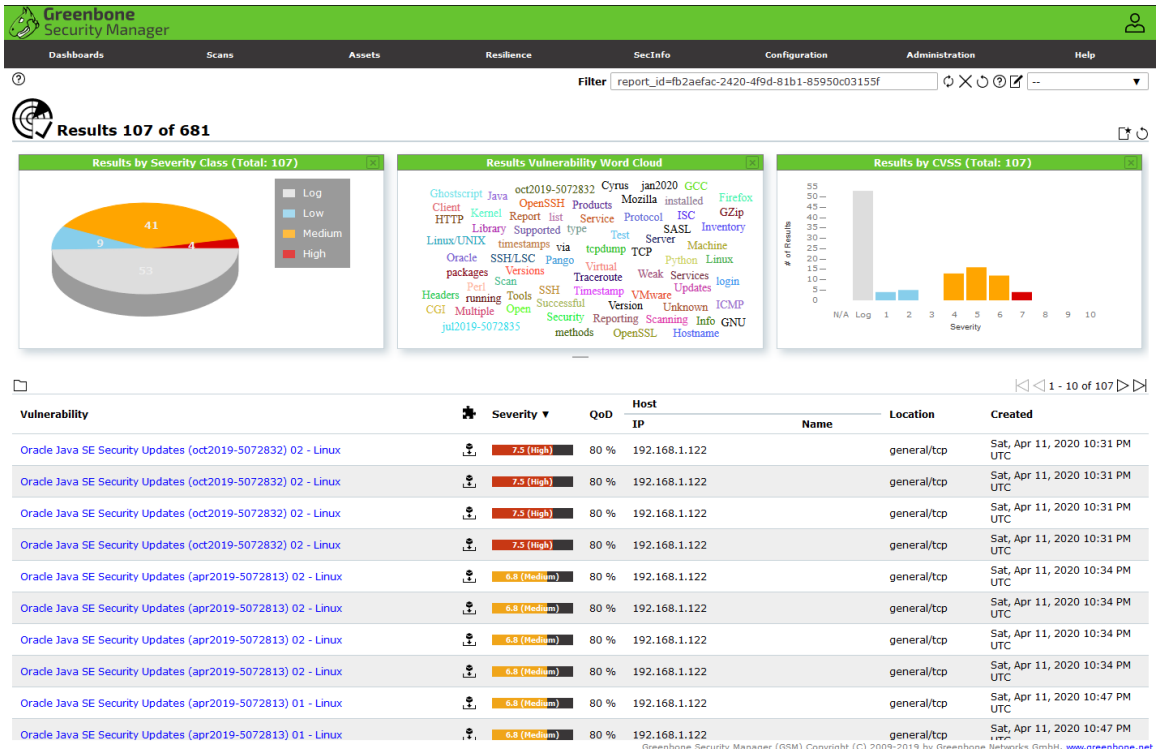

Figura 12 Resultado de análisis

En la siguiente pantalla se puede observar a detalle la vulnerabilidad critica, para este ejemplo en específico se muestra que es necesario parchar la aplicación JAVA, y también los enlaces de las referencias y documentación. Si los sistemas son desarrollados utilizando lenguaje de programación JAVA, se debe parchar para mitigar los riesgos asociados.

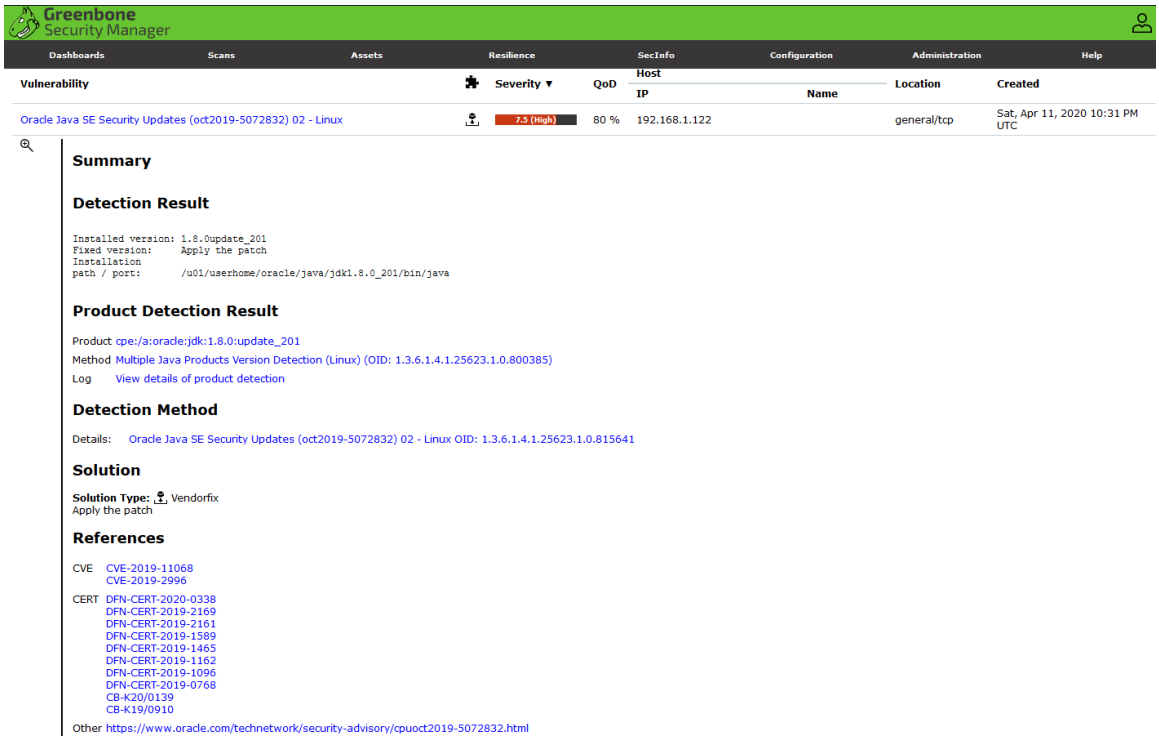

Figura 13 Detalle de vulnerabilidad

4.3 Análisis de riesgo

Siguiendo la guía definida en la sección 2.2.3 se hará un ejercicio de análisis de riesgo para una vulnerabilidad en específico, es muy importante en escenarios reales que este análisis sea de la manera más exhaustivo posible identificando todos los activos esenciales, tomando en cuenta todas las amenazas y vulnerabilidades posibles.

Alance: serán los activos que permiten dar el servicio de venta de artículos por internet:

- Servidor web
- Servidor de aplicación
- Servidor de base de datos

La cantidad de activos y / o elementos dependerá de cada organización y la identificación estará a cargo del equipo expertos de IT desarrolladores, arquitectos, administradores, etc.

Amenazas: Existe una diversidad de amenazas, para esto se puede basar en las diferentes guías de análisis de riesgo para tecnologías, acá se cita un diagrama de amenazas de tipo humanas, disponible en Octave Allegro una guía de evaluación de riesgo para sistemas de información.[7, p. 50]
Se puede tener internas o externas a la organización, si se materializan se puede tener divulgación, modificación, destrucción de información o interrupción de servicios.

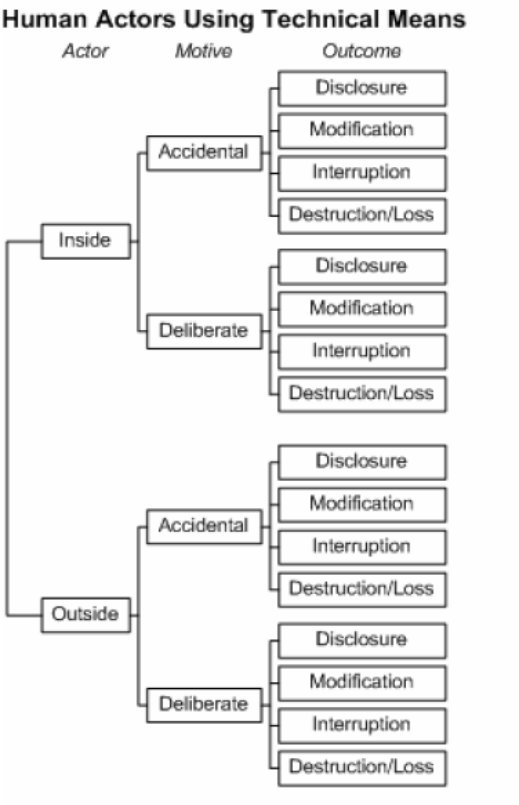

Figura 14 Amenazas humanas

Vulnerabilidades: En el apartado anterior 4.2 se identificaron las vulnerabilidades críticas a los sistemas según la solución de OpenVAS, estas están relacionadas a la versión de Java.

Para poder determinar probabilidad e impacto se deberá de analizar la documentación de la vulnerabilidad, en este ejemplo tenemos el siguiente ID CVE-2019-11068 y podemos hacer la consulta en el sitio "National Vulnerability Database"[8] .

En la descripción tenemos:
"libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit access even upon receiving a -1 error code.

xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded."[8]

Lo que indica que es un problema de control de acceso por medio de una URL modificada, la probabilidad es alta, ya que es una vulnerabilidad conocida y los servidores están expuestos a Internet, además de usar lenguaje de programación Java para los sistemas de información.

Evaluación de riesgo: Con el insumo anterior se puede crear la matriz de riesgo

Riesgo: Vulnerar control de acceso de sistema de venta en línea.

Probabilidad: Alta, debido a que está expuesto a internet con software vulnerable.
Impacto: Alto, debido al sistema de venta en línea.

Matriz de riesgos cuantitativa	IMPACTO			
PROBABLIDAD DE OCURRENCIA		BAJO	MEDIO	ALTO
	BAJA	MEDIO	ALTO	CRITICO
	MEDIA	BAJO	MEDIO	ALTO
	ALTA	BAJO	BAJO	MEDIO

Mitigar riesgo: Aplicar parche de seguridad.

5. Conclusiones y recomendaciones

5.1 Conclusiones

- Con base al objetivo 1, el cual procuraba el analizar la madurez del gobierno de TI (COBIT 5) y su grado de alineación con los objetivos corporativos, se concluye que: Se puede observar que basado en el nivel de madurez desarrollado por una institución en cuanto a sus procesos internos, existe una relación interdependiente respecto al uso de sistemas informáticos para el procesamiento de datos en áreas operativas y financieras las cuales están inversamente relacionadas, es decir que el nivel de exposición a un mayor de riesgo se da cuanto su nivel de madurez en cuanto a procesos de seguridad informática es menor, incluyéndose aquellos procesos de auditoria y seguimiento a eventos específicos de carácter de comportamiento humano los cuales requieren un nivel especializado de detección y reacción automáticos lo cual hoy en día se centraliza en grupos de seguridad informáticos permanentes los cuales pueden ser cubiertos y desarrollados de forma interna en la empresa como servicios externos. En revisión del nivel de actualidad y aplicación de las políticas asociadas con todos los procesos que la institución requiere para desarrollar con efectividad y eficiencia sus objetivos primarios y secundarios.

- En atención al objetivo 2, el cual busca establecer una metodología dinámica adaptativa para la gestión de riesgos de las TI, se concluye que: Después de todo lo desarrollado y mencionado en el presente trabajo está claro que el nivel de riesgo a los activos de una institución está asociados al contexto de la misma, lo cual define de forma primaria el rubro de operación y riesgos asociados a su actividad diaria. Es de hacer notar que dependiendo del tipo de procesos, actividades, servicios y tecnologías utilizadas aumentan el área de riesgo a ser tomada en cuenta en el análisis de riesgo (ISO 27001), siendo lo más importante las actividades de documentar, actualizar e informar sobre las vulnerabilidades y la forma en que se mitigaran para obtener el respaldo de la alta dirección.

- En referencia al objetivo 3, que define el diseño de una metodología para el monitoreo y evaluación del desempeño de la seguridad de las TI, se concluye que: En relación a lo expuesto referente a desarrollar nuevas formas de monitoreo y evaluación del desempeño de la seguridad de las TI de una forma innovadora aplicable al contexto de la empresa utilizando los últimos adelantos en el campo de la seguridad informática que permitirán correlacionar de forma automática los procesos dinámicos en la empresa, por lo cual se genera esta actividad de nivel primordial debido a que se está viviendo de forma simultánea una serie de eventos disruptivos que afectan a todo tipo de institución sean estas gubernamentales y privadas afectando en una gran cantidad de ámbitos comerciales por lo cual las técnicas y medidas previas actuales podrían no ser las más adecuadas para darle el seguimiento apropiado de los resultados de las mismas; por lo tanto es de suma importancia el dedicar tiempo y recursos para definir el nivel de actualización

requeridos de tal forma que sean las más apropiadas que aseguren el nivel de mitigación esperado para cada uno de los activos de la empresa.

6.1 Recomendaciones

- Implementar en las instituciones públicas y privadas programas destinados a dar a conocer, actualizar y motivar a las jefaturas y demás personal a ser parte permanente del liderazgo que impulse y soporte los diferentes sistemas de seguridad de la información basándose en la concepción de que todo lo relacionado con la informática tiene un alto nivel de cambio en su ciclo de vida.

- Desarrollar proyectos de mejora en la cultura de seguridad informática los cuales permitan un mejor nivel de participación de todos los colaboradores para que los directivos y jefaturas puedan revisar los diferentes puntos de vista de todos los interesados permitiéndose así el reforzamiento de las actuales medidas implementadas pero basadas en la experiencia propia de los usuarios expertos.

- El que la alta gerencia o directivos de la institución soporten los procesos de auditoria e implementación segura de equipamiento tecnológico, para confirmar el cumplimiento del diseño, implementación, ejecución y desarrollo de las buenas prácticas asociadas a todos los procesos del negocio los cuales estén directamente relacionados con los objetivos de esta.

6. Anexos

Ejemplo de herramienta de evaluación de procesos COBIT, tomado de ISACA.[3]

EDM01	Ensure Governance Framework Setting and Maintenance							
	Purpose	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.						
	Assess whether the following outcomes are achieved.	**Criteria**	**Criteria Are Met Y/N**	**Comment**	Not achieved (0-15%)	Partially Achieved (15% - 50%)	Largely Achieved (50% - 85%)	Fully Achieved (85-100%)
Level 0 Incomplete	**The process is not implemented, or fails to achieve its process purpose.**	At this level, there is little or no evidence of any achievement of the process purpose.						
Level 1 Performed	**PA 1.1 The implemented process achieves its process purpose.**	The following process outcomes are being achieved:	**Overall rating for the process**					
		EDM01-O1 Strategic decision-making model for IT is effective and aligned with the enterprise's internal and external environment and stakeholder requirements.						
		EDM01-O2 The governance system for IT is embedded in the enterprise.						
		EDM01-O2 Assurance is obtained that the governance system for IT is operating effectively.						
Level 2 Managed	**PA 2.1 Performance Management - A measure of the extent to which the performance of the process is managed.**	As a result of full achievement of this attribute: a) Objectives for the performance of the process are identified. b) Performance of the process is planned and monitored. c) Performance of the process is adjusted to meet plans. d) Responsibilities and authorities for performing the process are defined, assigned and communicated. e) Resources and information necessary for performing the process are identified, made available, allocated and used. f) Interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.						
	PA 2.2 Work Product Managem	As a result of full achievement of this attribute:						

	ent - A measure of the extent to which the work products produced by the process are appropriately managed. The work products (or outputs from the process) are defined and controlled.	a) Requirements for the work products of the process are defined. b) Requirements for documentation and control of the work products are defined. c) Work products are appropriately identified, documented, and controlled. d) Work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.						
Level 3 Established	**PA 3.1 Process Definition - A measure of the extent to which a standard process is maintained to support the deployment of the defined process.**	As a result of full achievement of this attribute: a) A standard process, including appropriate tailoring guidelines, is defined that describes the fundamental elements that must be incorporated into a defined process. b) The sequence and interaction of the standard process with other processes is determined. c) Required competencies and roles for performing a process are identified as part of the standard process. d) Required infrastructure and work environment for performing a process are identified as part of the standard process. e) Suitable methods for monitoring the effectiveness and suitability of the process are determined.						
	PA 3.2 Process Deployment - A measure of the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes.	As a result of full achievement of this attribute: a) A defined process is deployed based upon an appropriately selected and/or tailored standard process. b) Required roles, responsibilities and authorities for performing the defined process are assigned and communicated. c) Personnel performing the defined process are competent on the basis of appropriate education, training, and experience. d) Required resources and information necessary for performing the defined process are made available, allocated and used.						

		e) Required infrastructure and work environment for performing the defined process are made available, managed and maintained.						
		f) Appropriate data are collected and analysed as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the process, and to evaluate where continuous improvement of the process can be made.						
Level 4 Predictable	**PA 4.1 Process Measurement - A measure of the extent to which measurement results are used to ensure that performance of the process supports the achievement of relevant process performance objectives in support of defined business goals.**	As a result of full achievement of this attribute: a) Process information needs in support of relevant defined business goals are established. b) Process measurement objectives are derived from process information needs. c) Quantitative objectives for process performance in support of relevant business goals are established. d) Measures and frequency of measurement are identified and defined in line with process measurement objectives and quantitative objectives for process performance. e) Results of measurement are collected, analysed and reported in order to monitor the extent to which the quantitative objectives for process performance are met. f) Measurement results are used to characterise process performance.						
	PA 4.2 Process Control - A measure of the extent to which the process is quantitatively managed to produce a process that is stable, capable and predictable within defined limits.	As a result of full achievement of this attribute: a) Analysis and control techniques are determined and applied where applicable. b) Control limits of variation are established for normal process performance. c) Measurement data are analysed for special causes of variation. d) Corrective actions are taken to address special causes of variation. e) Control limits are re-established (as necessary) following corrective action.						
Level 5 Optimizing.	**PA 5.1 Process innovation - A measure of the extent to which changes to the**	As a result of full achievement of this attribute: a) Pprocess improvement objectives for the process are defined that support the relevant business goals.						

	process are identified from analysis of common causes of variation in performance, and from investigations of innovative approaches to the definition and deployment of the process.	b) Appropriate data are analysed to identify common causes of variations in process performance. c) Appropriate data are analysed to identify opportunities for best practice and innovation. d) Improvement opportunities derived from new technologies and process concepts are identified. e) An implementation strategy is established to achieve the process improvement objectives.						
	PA 5.2 Process optimisation - A measure of the extent to which changes to the definition, management and performance of the process result in effective impact that achieves the relevant process improvement objectives.	As a result of full achievement of this attribute: a) Impact of all proposed changes is assessed against the objectives of the defined process and standard process. b) Implementation of all agreed changes is managed to ensure that any disruption to the process performance is understood and acted upon. c) Based on actual performance, effectiveness of process change is evaluated against the defined product requirements and process objectives to determine whether results are due to common or special causes.						

7. Referencias

[1] *Técnicas de seguridad - Sistemas de gestión de seguridad de la información - requerimientos*, ISO 27001:2013. 2014.

[2] *Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información*, ISO 27002:2013. 2014.

[3] "About ISACA." https://www.isaca.org/about-isaca/Pages/default.aspx (accessed Jan. 12, 2020).

[4] *Un Marco de Negocio para el Gobierno y la Gestión de las s TI de la Empresa*, COBIT 5. ISACA: Estados Unidos IL, 2012.

[5] *Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures* , PCI DSS V32, 2018.

[6] "OpenVAS - OpenVAS - Open Vulnerability Assessment Scanner." https://www.openvas.org/ (accessed Apr. 11, 2020).

[7] Caralli, Richard., Stevens, James., Young, Lisa., & Wilson, William. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (CMU/SEI-2007-TR-012). Retrieved May 30, 2020, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

[8] "NVD - CVE-2019-11068." https://nvd.nist.gov/vuln/detail/CVE-2019-11068#vulnCurrentDescriptionTitle (accessed Apr. 12, 2020).