UNIVERSIDAD INTERNACIONAL DE LA RIOJA

**Universidad Internacional de La Rioja**
**Máster universitario en Seguridad Informática**

# Metodología para el análisis de vulnerabilidades del SO y la Red.

**Trabajo Fin de Máster**

**Presentado por:** Ortega Ramírez, Adrián

**Director/a:** Del Barrio García, Alberto

Ciudad: Cali - Colombia
Fecha: 17 de Enero de 2017

## Resumen

Con el presente trabajo se propone una metodología para el análisis de vulnerabilidades a nivel de sistema operativo y red interna de pequeñas y medianas organizaciones. La metodología involucra cuatro fases: Relacionamiento con la gerencia y las personas, Planeación, políticas y controles de seguridad y aseguramiento del sistema operativo y red interna de la organización; cada fase contiene una serie de actividades y recomendaciones enfocadas a la detección de posibles brechas de seguridad de la información que puedan presentarse en los elementos ya mencionados. Como parte del trabajo experimental se muestran los resultados obtenidos del análisis de vulnerabilidades realizado en una empresa del sector público juntamente con posibles acciones de solución que permitan mitigar los riesgos detectados. Los resultados permitieron concluir que las pequeñas y medianas empresas pueden buscar estrategias que les permitan asegurar la información que manejan a un bajo costo teniendo en cuenta los recursos que están disponibles.

**Palabras Clave:** Vulnerabilidad, Sistema Operativo, Políticas, Seguridad, Análisis.

## Abstract

This work proposes a methodology for vulnerability analysis at the operating system level and internal network of small and medium organizations. The methodology involves four phases: Relationship with management and people, Planning, policies and controls of security and assurance of the operating system and internal network of the organization; Each phase contains a series of activities and recommendations focused on the detection of possible security breaches of information that may occur in the elements already mentioned. As part of the experimental work, the results obtained from the vulnerability analysis carried out in a public sector company are presented together with possible solutions actions that allow mitigating the detected risks. The results allowed to conclude that the small and medium companies can look for strategies that allow them to assure the information that they manage to a low cost taking into account the resources that are available.

**Keywords:** Vulnerability, Operating System, Policies, Security, Analysis.

# Contenido

# Lista de Ilustraciones

# Lista de Tablas

# INTRODUCCIÓN

Hoy en día la información se considera el activo más importante y valioso de una empresa sin importar el sector o la actividad económica a la cual se dedica. Es por esto que dichas empresas deben buscar garantizar en tanto sea posible la integridad, disponibilidad y confidencialidad de la información que manejan; lo anterior se logra definiendo prácticas, estrategias, normas o metodologías que permitan la protección de la información, la prevención ante eventuales ataques y planes de acción en caso de que los riesgos identificados se materialicen. Lograr que una empresa cumpla con todo lo anteriormente mencionado requiere organización, tiempo y por supuesto una inversión económica dado que se requieren herramientas tecnológicas, implementación de procesos y políticas y a nivel general un gran conjunto de actividades y prácticas que solamente las organizaciones con suficiente capital podrían implementar.

Es precisamente el factor económico lo que detiene a muchas empresas PYMES para establecer un área de seguridad de la información o al menos para implementar el uso de herramientas que les permitan identificar y analizar las vulnerabilidades en la información como un factor vital para la detección y prevención de ataques y amenazas. Es aquí donde nace la necesidad de buscar una estrategia o metodología que permita a las pequeñas y medianas empresas mejorar el aseguramiento de la información que manejan a un bajo costo que este dentro del presupuesto y los alcances de la organización.

En consecuencia, con el presente trabajo se pretende proponer un conjunto de buenas prácticas y recomendaciones de herramientas a manera de metodología para que las pequeñas y medianas empresas puedan realizar análisis de vulnerabilidades con un costo que este dentro del alcance de cada empresa sin perder la calidad y la garantía del aseguramiento de la información; con esto, la organización tendrá una herramienta que le permita mejorar las prácticas en cuestión de seguridad de la información y con dicha experiencia, la maduración de los procesos internos y de la misma metodología la cual podrá ser adaptada y ajustada teniendo en cuenta las necesidades particulares del que hacer y del funcionamiento de la empresa. La metodología a proponer se apoya en estándares internacionales tales como la ISO/IEC 27001 y en metodologías que hoy ya existen y que han sido resultado de investigaciones en empresas de pequeña y mediana escala por lo que esta propuesta también puede aplicarse en empresas del sector público.

## 1.1 Objetivos

### 1.1.1 Objetivo General

Realizar una propuesta de metodología para analizar vulnerabilidades a nivel de sistema operativo y red interna en empresas Pymes y del sector público.

### 1.1.2 Objetivo General

- Determinar las políticas y lineamientos que se deben tener en cuenta para realizar un análisis de vulnerabilidades, teniendo en cuenta la norma ISO 27001:2005 en una organización.
- Realizar un análisis de vulnerabilidades a nivel de la red interna y sistema operativo del departamento de Tecnología de la empresa EMCALI E.I.C.E.
- Categorizar las vulnerabilidades encontradas en el análisis aplicado y establecer posibles alternativas de solución que busquen mitigar dichos hallazgos.
- Establecer un conjunto de buenas prácticas y recomendaciones a manera de propuesta de metodología para la realización de análisis de vulnerabilidades en empresas pequeñas, medianas y del sector público.

# 2. MARCO TEÓRICO

La información es uno de los activos más importantes hoy en día en cualquier tipo de organización y precisamente en orden de la importancia que ésta representa se debe buscar garantizar, en tanto sea posible, la integridad, disponibilidad y confidencialidad de la misma. En respuesta a lo anterior, entes internacionales como la Organización Internacional de Normalización (ISO) ha establecido un conjunto de normas, parámetros y buenas prácticas que buscan propender la calidad y la gestión de la calidad de bienes o servicios, entre ellos, la información y su seguridad.

## 2.1 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

La Norma ISO 27001 especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) que a su vez es un conjunto de prácticas, reglamentos y buenas prácticas que permiten gestionar el acceso y manipulación a la información sin importar cuál sea el medio en el que ésta se encuentra y por ende, al tener control en la manipulación, se podrá identificar y gestionar de una manera más eficiente las vulnerabilidades y riesgos globales a los cuales la información de una organización está expuesta.

La importancia de implementar un SGSI en una organización radica principalmente en que al ser la información uno de los activos más importantes de una empresa, la manipulación y uso que se haga de ella puede representar un factor determinante en el éxito o el fracaso del negocio y aun de la sostenibilidad del mismo. Dentro de los beneficios que existen de implementar un SGSI en las organizaciones cabe resaltar los siguientes:

- Permite garantizar la continuidad y disponibilidad del negocio.
- Permite conocer en detalle el que hacer de la organización como empresa, su funcionamiento y el establecimiento de planes de acción ante posibles incidentes como parte de la gestión de mejora continua del negocio.
- Cumplimiento de las normas, leyes y legislaciones en términos de protección de datos y de seguridad de la información en general.
- Brinda a los clientes de la organización confiabilidad y tranquilidad de estar vinculados a una empresa que garantiza la protección y buen manejo de su información personal.

- Mejor aprovechamiento de los recursos y disminución en los costes causados por incidentes gracias a las acciones preventivas, minimización de ocurrencia de incidentes y planes de contingencia establecidos en caso que un riesgo previamente identificado y categorizado se materialice.
- Ordenamiento del negocio teniendo en cuenta que el SGSI permite la distribución de roles, funciones y asignaciones de manera organizada y sincronizada al interior de la organización.

De acuerdo a la norma técnica colombiana **NTC-ISO/IEC 27001**, la norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. En la Figura 1, se muestra cada fase del modelo con su respectiva descripción:

**Ilustración 1. Modelo de Procesos Planear, Hacer, Verificar y Actuar - PHVA**

| | |
|---|---|
| Planificar (establecer el SGSI) | Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización. |
| Hacer (implementar y operar el SGSI) | Implementar y operar la política, los controles, procesos y procedimientos del SGSI. |
| Verificar (hacer seguimiento y revisar el SGSI) | Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión. |
| Actuar (mantener y mejorar el SGSI) | Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI. |

Fuente: NTC-ISO/IEC 27001

De acuerdo al cuadro anterior, la fase de 'Hacer' implica implementar y operar políticas, controles, procesos, procedimientos y estrategias que permitan el aseguramiento de la información que maneja una organización y de los sistemas que trabajan y manipulan dicha información. En consecuencia, el análisis de vulnerabilidades se considera un procedimiento de suma importancia en la fase 'Hacer' dentro del ejercicio de la ejecución e implementación de un sistema de gestión de la seguridad de la información en una organización.

## 2.2 ANALISIS DE VULNERABILIDADES

El análisis de vulnerabilidades es un procedimiento que se realiza con el fin de incrementar la seguridad y garantizar que la información que se maneja y manipula al interior de una empresa esté protegida ante cualquier eventualidad que pueda interrumpir o alterar el correcto funcionamiento de la organización. El realizar análisis de vulnerabilidades como

procedimiento preventivo permite identificar no conformidades potenciales y sus causas, evaluar la necesidad de acciones para impedir que las no conformidades ocurran, determinar e implementar la acción preventiva necesaria, registrar los resultados de la acción tomada y revisar la acción preventiva tomada. Por lo anterior, se recomienda que la organización identifique los cambios en los riesgos teniendo en cuenta las vulnerabilidades y brechas en seguridad identificadas e identificar los requisitos en cuanto acciones preventivas, concentrando la atención en los riesgos que han cambiado significativamente. (NTC-ISO-IEC 27001, Sección 8.3 Acciones preventivas).

De acuerdo a Garzón, Ratkovich y Vergara (2005), es de suma importancia que se identifiquen y mitiguen los riesgos a los que se encuentra expuesta pero aunque se logren identificar dichas vulnerabilidades y riesgos, es recomendable que la organización esté preparada para superar cualquier eventualidad que interrumpa las actividades habituales mediante procedimientos tales como la sincronización y fijación del tiempo de equipos y dispositivos, auditorías internas, computación forense, entre otros procedimientos. Teniendo en cuenta lo anterior, solamente empresas con suficiente capital estarían en la capacidad de implementar una solución de seguridad que contemple todo el aseguramiento necesario incluyendo tantos frentes como sea posible; por tal motivo, se hace necesario el establecimiento de un paso a paso o metodología de seguridad apropiada para las empresas y organizaciones pequeñas que no cuentan con los suficientes recursos pero que requieren implementar mecanismos de seguridad de la información que manejan.

### 2.2.1 Vulnerabilidades De Un Sistema Informático

En un sistema informático lo que se quiere proteger son sus activos, es decir, los recursos que forman parte del sistema. Estos activos se pueden agrupar así:

- **Hardware:** elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVD, entre otros).
- **Software:** elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos:** comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red. [1]

Los anteriores grupos, se consideran los más delicados y críticos dado que si los datos que están almacenados en el hardware y que son procesados por las aplicaciones software

sufren algún tipo de ataque, podría incurrirse en daños que pueden ser irreparables y por ende la organización se vería afectada en gran manera y el encontrar la solución podría ser una tarea compleja teniendo en cuenta que son 3 factores claves comprometidos: Hardware, software e información.

A nivel del sistema operativo, las vulnerabilidades pueden deberse a:

- Errores del programa: Un error en el código de un programa puede permitir que un virus informático acceda al dispositivo.
- Funciones intencionadas: Formas legítimas y documentadas en las se permite el acceso de las aplicaciones al sistema. [2]

Si se sabe que existen vulnerabilidades, es decir, se tiene conocimiento con antelación de las brechas de seguridad existentes en un sistema operativo o una aplicación (tanto si dichas vulnerabilidades son intencionadas como si no), la probabilidad de poder mitigar ese riesgo o de contenerlo es más alta precisamente por el factor de prevención.

Claramente una vulnerabilidad es un estado de riesgo en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente [3]:

- ❖ Permitir que un atacante ejecute comandos como otro usuario
- ❖ Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- ❖ Permitir a un atacante hacerse pasar por otra entidad
- ❖ Permitir a un atacante realizar una negación de servicio

### 2.2.2 Vulnerabilidades a nivel de Red

Una red de ordenadores funciona como un sistema en el que a la vez que se van introduciendo novedades que mejoran su rendimiento, van apareciendo debilidades que necesitan de otras mejoras que puedan corregir dichos puntos débiles.

De esta forma se puede entrever que una red proporciona un marco ideal para proferir ataques de manera justificada o injustificada. Solo basta con tener en cuenta que lo que se mueve dentro de una red no es más que información, y, ya sea esta sensible o no, está expuesta a la posibilidad de que se quiera manipular en cualquiera de sus formas. En consecuencia, los ataques más relevantes que una red puede sufrir son:

- Suplantación de identidad: Una persona o entidad suplanta a otra con fines delictivos. En este sentido, puede haber personas que se hacen pasar por otras para acceder a un recurso de la red al que por defecto no tendrían acceso, hasta otros casos en los que dichas personas se dan a conocer como otra que no son de cara al exterior.
- Divulgación del contenido: Se produce cuando una persona o entidad se entromete en el destino final de un mensaje o de parte de su contenido de forma que puede hacer uso de la información interceptada de forma fraudulenta.
- Modificación de mensajes: Consiste en modificar el contenido de un mensaje sin que sea posible detectarlo de forma que el destinatario actúe en consecuencia a lo que ese mensaje contiene.
- Denegación del servicio: Se consigue de manera ilícita que una persona o entidad no pueda operar de forma normal impidiéndole el acceso a determinados servicios como podría ser, por ejemplo, el correo electrónico.

Los ataques descritos anteriormente pueden ser llevados a cabo mediante diferentes mecanismos que pueden provenir de factores internos o externos a la organización y no necesariamente. Por lo anterior, es de gran importancia dividir responsabilidades para evitar ataques internos en una red. Si una persona es la única encargada de la seguridad de una organización, tendrá en su poder información suficiente para manipular todo el sistema sin que pueda ser detectado por los demás. [4].

Las vulnerabilidades en un sistema, sea una red, sistema operativo, aplicación web, aplicación de escritorio, etc., tienen un comportamiento que las caracteriza desde el momento en que son detectadas hasta el momento en que son mitigadas o tratadas. El análisis de vulnerabilidades permite identificar, cuantificar y clasificar vulnerabilidades comunes y conocidas de una red, aplicación o infraestructura, por lo general de manera automática y no invasiva [5], es decir, no se explotan las potenciales vulnerabilidades que puedan encontrarse por lo que puede considerarse una estrategia más segura y aceptable por la organización dado que no se estaría atacando (de manera controlada) los sistemas productivos de la compañía en busca de amenazas o brechas de seguridad. Precisamente una de las principales diferencias entre el análisis de vulnerabilidades y las pruebas de penetración es que la prueba de penetración involucra realizar de una manera controlada un ataque a un sistema determinado; es por eso que muchas compañías prefieren realizar como primera instancia una evaluación de las vulnerabilidades ya que lo que se evaluaría son los sistemas que están en ambientes productivos los cuales no se desean poner en riesgo de alguna interrupción o fallo por causa de los ataques controlados que pueden involucrar códigos maliciosos, inyección de SQL, malware, etc. En la Ilustración 2 se muestra el ciclo de vida de las vulnerabilidades y las características de cada etapa:

**Ilustración 2. Ciclo de Vida de una Vulnerabilidad**


Fuente: Herramientas de Vulnerability Assessment y Gestión de Incidencias. Recuperado de: https://seguridadetica.wordpress.com/

## 2.3 CONTEXTO EMCALI – ANTECEDENTES Y SITUACION ACTUAL

### 2.3.1 ¿Quién es EMCALI?

Empresas Municipales de Cali o EMCALI es la empresa prestadora de servicios públicos (energía, acueducto, alcantarillado y telecomunicaciones) que presta sus servicios de electricidad y telecomunicaciones a los municipios de Cali, Yumbo y Puerto Tejada, y de acueducto y alcantarillado en el casco urbano de Cali y Yumbo. Empezó labores en 1931 siendo propiedad del municipio de Santiago de Cali.
Emcali apunta a ser una empresa pública ágil, competitiva y orientada al cliente, que nos permita convertirnos y mantenernos como la mejor alternativa en el mercado colombiano y modelo empresarial en América Latina. [6]

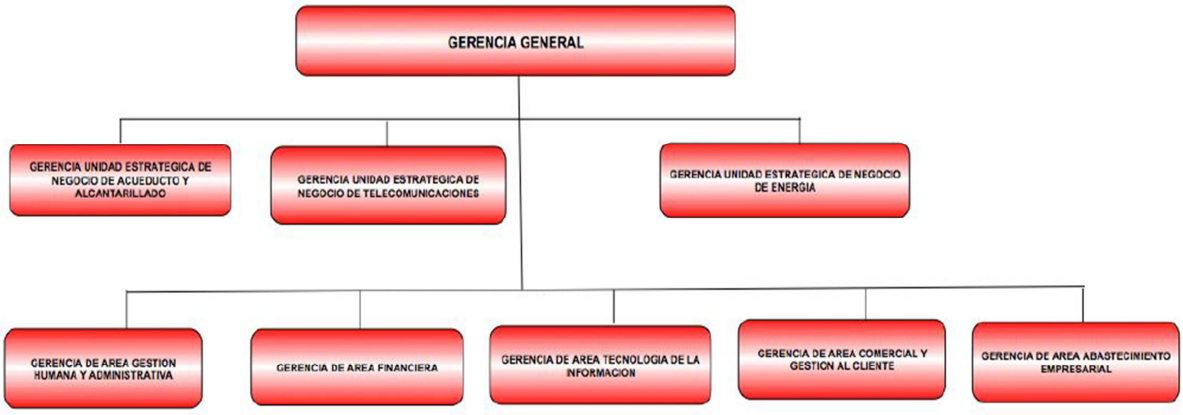
### 2.3.2 ¿Qué es lo que mueve a EMCALI?

La misión de Emcali como empresa prestadora de servicios públicos es contribuir con desarrollo de la ciudad de Santiago de Cali y su comunidad, brindando la prestación de servicios públicos fundamentales para el diario vivir de la ciudad, garantizando rentabilidad económica y social.

### 2.3.3 Gerencia de Tecnología de Información de Emcali

La empresa Emcali se encuentra estructurada por tres patrones estratégicos o gerencias, las cuales se encargan de liderar el modelo de negocio según sea la unidad del portafolio de servicios de la empresa. Estas tres unidades se encuentran soportadas por gerencias de apoyo, las cuales cumplen la labor de segmentar la estructura empresarial de las mismas. En la Ilustración 3, se presenta el organigrama general de la empresa Emcali:

**Ilustración 3. Organigrama General de EMCALI**

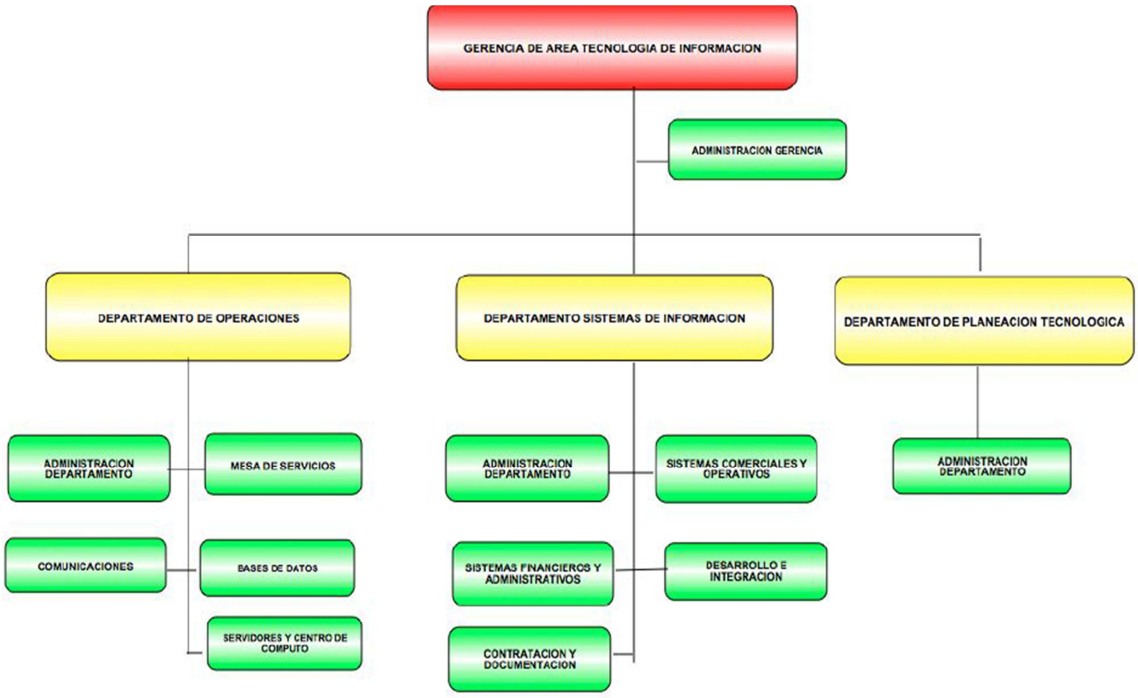



Fuente: EMCALI E.I.C.E. Estructura Organizacional[1]

La gerencia de Tecnología de la información se encarga de gestionar y administrar el departamento de informática, en ella se encuentran empleados de alta calificación para dirigir y controlar procesos de administración de la plataforma utilizada por la empresa, además de comprobar los accesos a la información de toda la empresa. Dentro de esta gerencia se encuentran otros departamentos los cuales dan apoyo para el buen manejo de la infraestructura e información (física como lógica). Como lo muestra la Ilustración 4, se pueden observar las subdivisiones de la gerencia de tecnología de la información.

[1] Morales, Madelayne. 2016. FCAPS Caso aplicado: EMCALI. Proyecto de Curso -Sistemas Gerenciales de Ingeniería. Pontificia Universidad Javeriana. Cali.

**Ilustración 4. Gerencia de Área de Tecnología de la Información**




Fuente: EMCALI E.I.C.E. Estructura Gerencia TI[2]

La gerencia de tecnología de la información (GTI) durante el periodo de 2008-2012 opto por implementar nuevas prácticas y estrategias de negocio que se aplicaron tanto a las unidades de negocio como las gerencias de apoyo para lograr así la integridad, disponibilidad y confidencialidad de la información.

Esta gerencia ha definido un objetivo estratégico alineado con el plan estratégico 2013-2017, en el cual contribuirá en el alcance de la meta definida por la organización que está basada en agregar valor a los servicios ofrecidos por TI optimizando los procesos de negocio. Por eso el cumplimiento de este objetivo incluirá la aplicación de distintas actividades de complemento que son:

- Medir, analizar, mejorar y controlar la implementación de tecnología de información.
- Madurar el sistema de gestión para una mejor prestación de los servicios de TI.
- Fortalecer la disponibilidad, integridad y confidencialidad de los servicios de TI.

[2] Morales, Madelayne. 2016. FCAPS Caso aplicado: EMCALI. Proyecto de Curso -Sistemas Gerenciales de Ingeniería. Pontificia Universidad Javeriana. Cali.

- Diseñar e implementar una arquitectura empresarial con la cual se estructuren la estrategia, procesos, metodologías y componentes (recursos, información y Tecnologías de la Información) desde perspectivas diferentes.
- Diseñar y crear nuevos negocios.

Con la implementación de estas actividades el área GTI garantiza el cumplimiento de su misión y visión, las cuales se describen a continuación.

### 2.3.4 Misión del área GTI

La gerencia de tecnología de información tiene como misión proveer y administrar recursos y servicios de tecnología de información y comunicaciones de óptima calidad a EMCALI EICE ESP y organizaciones externas, que contribuyan al cumplimiento de sus metas y objetivos institucionales, soportados en una excelente atención al cliente, utilizando buenas prácticas y aplicando estándares internacionales para así dar cumplimiento de la normativa legal del modelo estándar de control interno y sistema de Gestión de Calidad.

### 2.3.5 Visión GTI

La gerencia GTI tiene como objetivo para el año 2017 consolidarse como una importante ventaja competitiva para EMCALI-EICE-ESP, sus unidades estratégicas de negocio y socios estratégicos, con una excelente oferta y prestación de servicios, apoyada en buenas prácticas y soluciones tecnológicas innovadoras e integrales, que contribuyan a la gestión y desarrollo de la empresa.

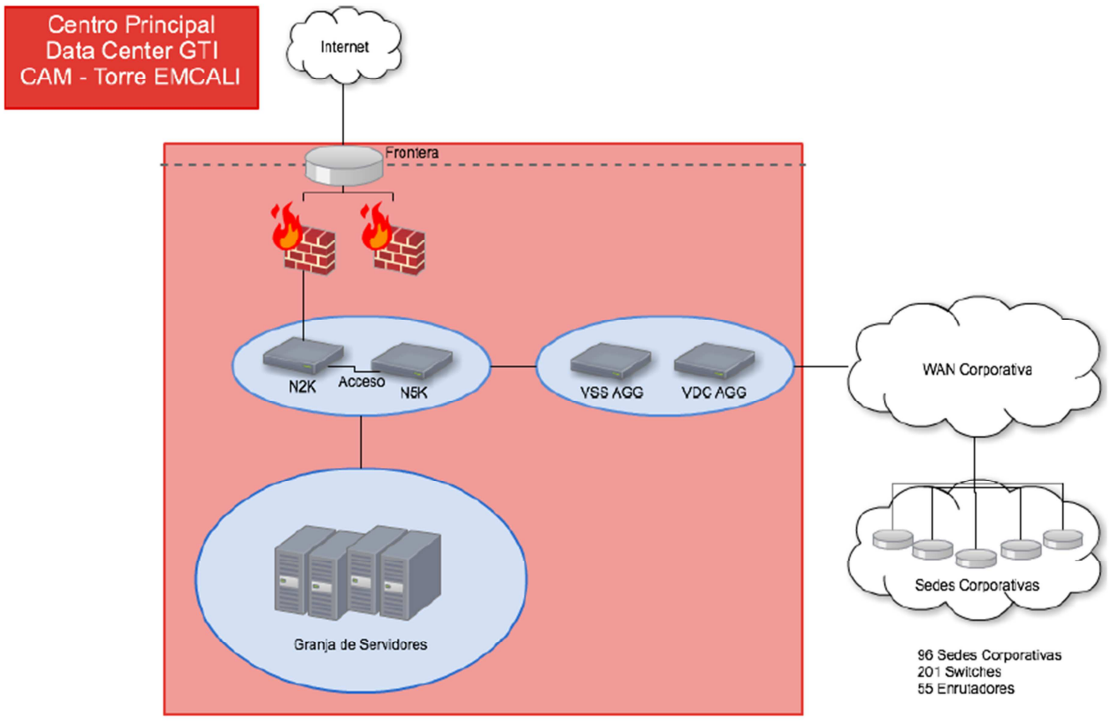
El departamento de GTI ha contribuido al mejoramiento de la plataforma tecnológica de la empresa para soportar la actividad del negocio y brindar un mejor servicio a la ciudadanía de Santiago de Cali. Es por ello que desde hace 15 años se están implementando avances importantes en el departamento los cuales han servido de apoyo para el proceso de maduración de la empresa en cuanto a la prestación del servicio y atención al cliente.

### 2.3.6 Infraestructura Tecnológica de EMCALI - EICE-ESP (Topología, Tecnologías y Servicios)

Emcali cuenta con 96 sedes corporativas distribuidas en la ciudad de Cali, Puerto Tejada, Yumbo y Jamundí. Esta distribución permite a la empresa crear una topología tipo estrella que permite a las estaciones estar conectadas directamente a un punto central y todas las comunicaciones se hacen a través de ese punto (conmutador, repetidor o concentrador). Esta comunicación entre sedes utiliza la tecnología de fibra óptica la cual es una herramienta para transmitir información sin interrupciones, su proveedor de servicios de

redes es EMCALI Telecomunicaciones y se administran alrededor de 400 dispositivos en la red como lo muestra la Ilustración 5:

**Ilustración 5. Diagrama General de la Red Administrativa de EMCALI**




Fuente: FCAPS Caso aplicado: EMCALI. Proyecto de Curso -Sistemas Gerenciales de Ingeniería. Pontificia Universidad Javeriana. Cali.

Para el soporte de la estructura que maneja EMCALI se implementan varios servicios de gran importancia para todas las unidades estratégicas de negocio. A continuación, se mencionan los servicios más importantes implementados en la arquitectura de la empresa:

- Software Open Smart Flex es un sistema modular y pre-configurado con un motor de facturación robusto, un efectivo módulo de servicio al cliente, un sistema de gestión de servicios ágil y un millar de funciones para manejar las necesidades del cliente.

- Telefonía IP es una tecnología que permite integrar en una misma red las comunicaciones de voz y datos. Esta tecnología proporciona ventajas como lo son la simplificación de la estructura de comunicaciones en la empresa, la integración de las diferentes sedes y trabajadores móviles de la organización en un sistema unificado de telefonía, la movilidad y el acceso a funcionabilidades avanzadas.

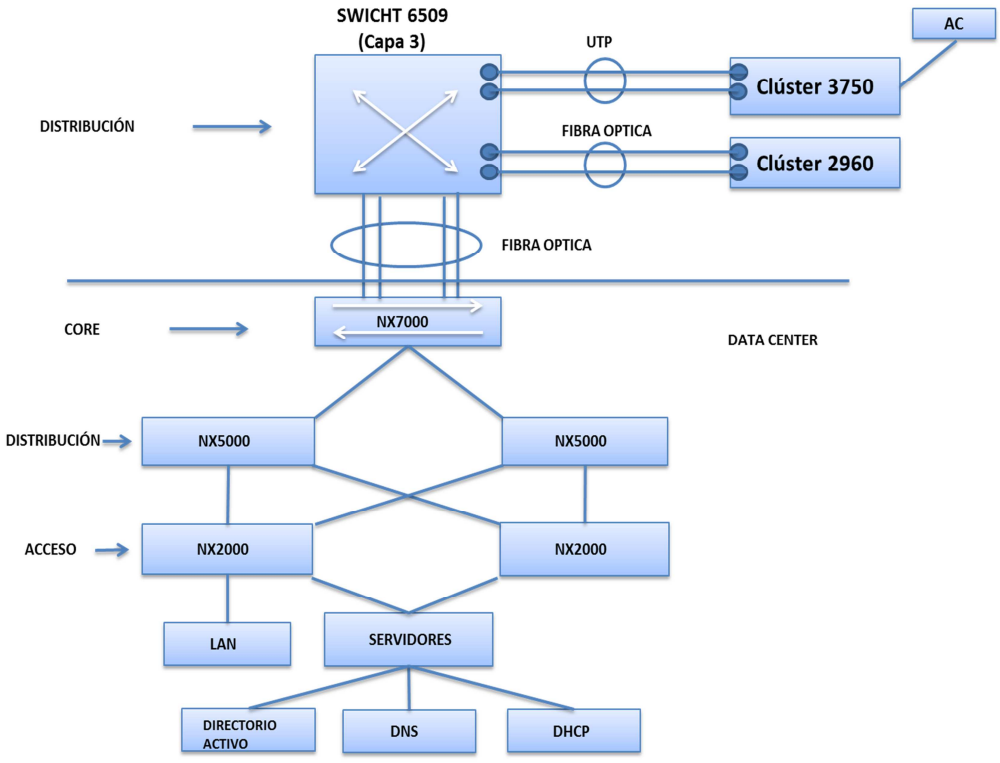
- Contac Center servicio fundamental para la empresa EMCALI el cual le permite tener un contacto más directo con el cliente y asegurar la fidelidad de este respecto a los productos y servicios que se les ofrecen a los usuarios que se surten de los servicios prestados por la empresa.

- Portal Web el portal web de EMCALI es fundamental para prestar un servicio oportuno y eficaz para los usuarios por ende este servicio permite planificar correctamente una presencia en internet incluye el ocuparse de manera intensa de la oferta de productos y servicios, tus clientes pueden ver los productos de Emcali, pueden registrar solicitudes o PQRs para la atención de sus peticiones.

- VPN (virtual private network) le permite a los funcionarios de EMCALI conectarse desde varios puntos de manera segura, además de facilitar el acceso remoto a una red local de la empresa así se encuentre en otra sede.

En la Ilustración 6 que se muestra a continuación, se visualiza el diagrama de red de la gerencia de tecnología de EMCALI:

**Ilustración 6. Diagrama de Red de GTI – EMCALI**




Fuente: Elaboración Propia

### 2.3.7 Gestión De La Seguridad En Emcali

Para el aseguramiento remoto de los equipos de trabajo de la empresa se usan dos herramientas:

- Kaspersky: Antivirus instalado en todas las terminales de trabajo de la empresa como PCs y equipos portátiles. Esta herramienta licenciada permite la protección de los equipos de trabajo contra Malware y en general cualquier amenaza en la red de la empresa.

- Aranda: esta herramienta se encuentra instalada en todos los terminales de computo PCs y Laptops de la red corporativa que permite la detección de intrusos basado en reglas, control de dispositivos móviles y removibles de almacenamiento, minimizar perdida de datos y tiempos de recuperación; rápida, fácil y eficiente migración de hardware, protección multicapa contra robo de datos y el acceso no autorizado a sus archivos.

Haciendo referencia a los servidores donde se encuentra la información de la empresa se cuenta con dos servidores (Protocolo AAA) que garantizan y realizan la autenticación, autorización y registro de los usuarios que acceden a la red interna y para el acceso de los servicios se cuenta con el Directorio Activo o autenticación propia de la aplicación.

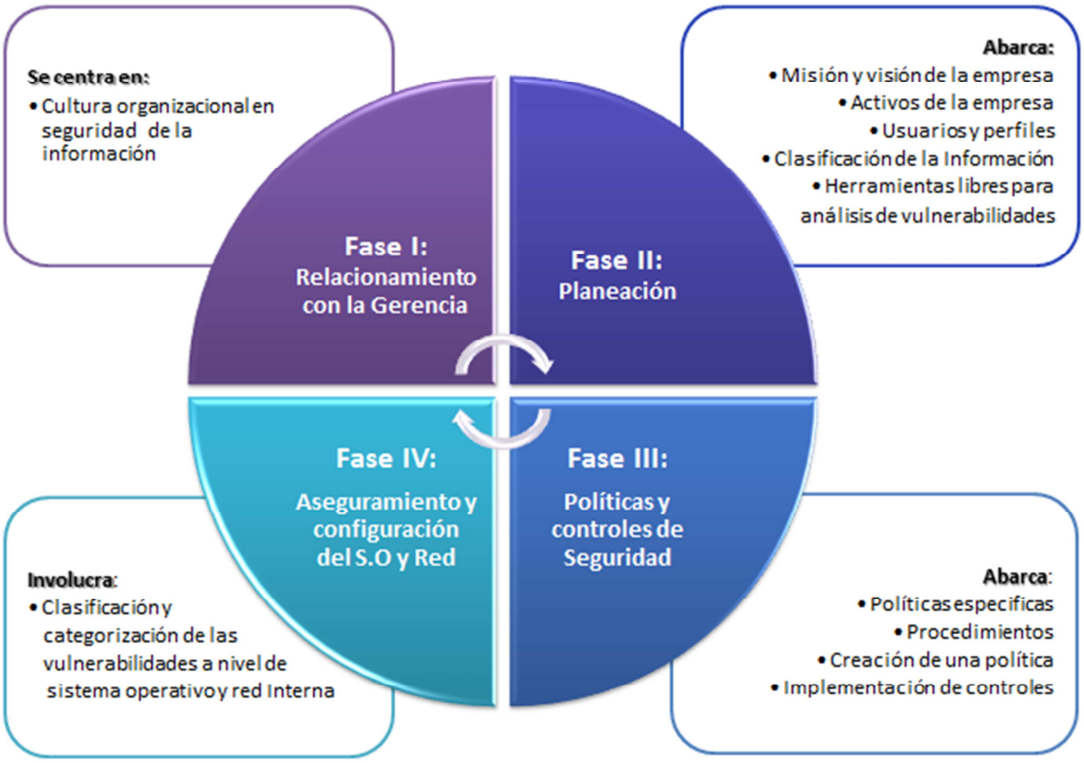
Para la seguridad perimetral de la red corporativa de EMCALI se cuenta con dos AS con funcionalidades de IPS (Firewalls Cisco ASA 5500) los cuales proporcionan la visibilidad de red que los administradores necesitan, además proveen protección superior contra amenazas y malware avanzado. Hasta el momento estas herramientas han funcionado de manera correcta, pero como proyecto de mejora y debido al crecimiento del servicio del portal Web de EMCALI se cambiarán por Firewalls de nueva generación, la implementación de una solución W.A.F (web Application Firewall) y una solución Anti DDos que permita un mejor control y seguridad para servicios Web y servicios en la nube.

# 3. METODOLOGÍA PARA EL ANÁLISIS DE VULNERABILIDADES EN SISTEMA OPERATIVO Y RED EN PEQUEÑAS Y MEDIANAS EMPRESAS

La metodología que se propone para el análisis de vulnerabilidades a nivel del sistema operativo y la red interna de organizaciones pequeñas y medianas se basa específicamente en la fase HACER del modelo de procesos PHVA (Planear, Hacer, Verificar y Actuar) de la Norma ISO 27001 y toma algunos elementos expuestos en la metodología estructurada por Garzón, Ratkovich y Vergara (2005) cuyos resultados se consignaron en el artículo *"Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala"*. [7].

Teniendo en cuenta que el factor económico es uno de los principales elementos que frena a muchas empresas PYMES para establecer un área de seguridad de la información, una alternativa de solución es la implementación de controles, procedimientos y procesos que permitan a la organización identificar y analizar las vulnerabilidades y riesgos que pueden atacar su información sin que esto represente una inversión monetaria que se desborde del alcance financiero de la empresa y de esta forma dicha organización aunque se encuentre madurando y creciendo en sus procesos y aseguramiento de la información no estaría del todo desprotegida. En la Ilustración 7, se presentan las fases que componen esta propuesta metodológica:

**Ilustración 7. Fases de la Metodología Propuesta**




Fuente: Elaboración Propia

## 3.1 FASE I: Relacionamiento con la Gerencia y las personas.

### 3.1.1 Cultura Organizacional en seguridad de la Información.

Típicamente las empresas están organizadas por departamentos o unidades de negocio que cumplen una función específica y es precisamente ese trabajo conjunto el que tiene como objetivo alcanzar las metas definidas por toda la organización. Es precisamente en el punto de Unidad como organización que se debe empezar a trabajar dado que, dentro de una misma empresa, cada área no debe verse ni mucho menos actuar como isla independiente sino como parte de un todo trabajando por uno o varios objetivos en común dependiendo del negocio. En este sentido, la responsabilidad del aseguramiento de la información no debe recaer solamente en el departamento de sistemas o de tecnología, sino que también debe compartirse con cada uno de los miembros de la organización involucrando por supuesto la alta gerencia, pero no solo la alta gerencia de tecnología sino también la dirección principal que encabeza la estructura organizacional.

La alta gerencia de la empresa debe apoyar y respaldar de manera activa la seguridad al interior de ella, a través de un conjunto de actividades las cuales se nombran a continuación:

1. Definir la postura de la dirección o la gerencia con respecto a la necesidad de proteger la información corporativa: Hablando propiamente de EMCALI E.I.C.E, pero aplicable a cualquier organización PYME de otros sectores, las gerencias de área de tecnología de la información en conjunto con la gerencia general deberán definir en primera instancia por qué se necesita asegurar la información que manejan, qué se necesita para lograr dicho aseguramiento y el cómo van a llevarlo a cabo. Es de suma importancia que la gerencia general esté involucrada ya que precisamente esta área por ser cabeza de la organización debe tener claro el por qué y el para qué de las medidas que al interior de la empresa se pondrán en acción.

2. Orientar a los miembros de la organización con respecto al uso de los recursos de información: No basta únicamente con que el departamento de tecnología y la dirección general definan por qué se necesita asegurar la información y el cómo van a hacerlo, sino también se hace necesario que esa concientización sea difundida y aplicada por toda la empresa. Para esto, se pueden utilizar estrategias como: talleres de sensibilización en cuanto a la importancia de la seguridad de la información, realizar periódicamente capacitaciones sobre las políticas de seguridad de la información de la empresa y las actualizaciones de las mismas y sensibilizar a los empleados sobre las amenazas a las que están expuestos.

3. Definir la base para la estructura de seguridad de la organización: es de gran importancia definir un área dentro de la organización cuyo foco sea la seguridad de la información; si la empresa aún no cuenta con esta área, podría iniciar delegando a un conjunto de personas para este fin. Dicho equipo de trabajo debe contar con el apoyo de la gerencia de tecnología y la dirección general.

De acuerdo a la NTC-ISO-IEC 27001, en términos del sistema de gestión de la seguridad de la información – SGSI, la empresa deberá brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI. Para esto, la organización deberá pensar en:

- Establecer unas políticas de seguridad, que a su vez servirán para la estructuración del SGSI
- Establecer los objetivos y planes del SGSI;

- Establecer funciones y responsabilidades de seguridad de la información;
- Comunicar a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua;
- Brindar y facilitar los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI.
- Decidir los criterios para aceptación de riesgos, y los niveles de riesgo aceptables;
- Realizar realizan auditorías internas del SGSI
- Efectuar revisiones por la dirección, del SGSI

## 3.2 FASE II: Planeación

### 3.2.1 Características mínimas a garantizar en el aseguramiento de la información

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411-1:2006].

Dentro de esta planeación se tendrán en cuenta los factores que se muestran en la Ilustración 7. No obstante, la organización podrá decidir que otros elementos tendrá en cuenta para la planeación del análisis de vulnerabilidades teniendo en cuenta las necesidades particulares y las herramientas y recursos con los que cuenta:

**Ilustración 8. Factores claves dentro de la planeación para el análisis de Vulnerabilidades**


Fuente: Elaboración propia

### 3.2.2 Misión y visión de la Organización

En arquitectura, para poder realizar una buena construcción es importante que los cimientos y la base de la estructura a edificar estén bien definidos y sólidos. Lo mismo sucede para cualquier ámbito donde se desea crear o construir algo nuevo; en este sentido, es de suma importancia que inicialmente se tenga muy claro y bien definido cuál es la misión y la visión de la empresa, cuáles son sus objetivos y sus metas, con el fin de generar una solución que este alineada a las necesidades puntuales de la organización. Para esto, la empresa puede hacer lo siguiente:

1. Definir el alcance y límites de la gestión de la seguridad en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, recurso humano, entre otros factores.
2. Fijar objetivos puntuales en cuanto a lo que la empresa desea en términos de seguridad de la información.
3. Tener en cuenta las reglamentaciones de ley que la empresa debe cumplir o los requisitos mínimos los cuales se deben garantizar tener al interior de la organización.
4. Identificar los activos dentro de la empresa que entrarían dentro de la gestión de seguridad de la información y los propietarios de dichos activos.

5. Identificar los posibles riesgos y amenazas que pueden afectar los activos de la organización
6. Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas. Para esto, la empresa puede apoyarse en escaneos a través de herramientas libres que le permitan analizar dichas vulnerabilidades.
7. Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.
8. Identificar y seleccionar un conjunto de políticas y controles de seguridad de la información que pueden aplicarse en la organización.

### 3.2.3 Activos de la empresa

Un Activo se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Los activos de información pueden clasificarse en las siguientes categorías:

- Datos: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.

- Aplicaciones: El software que se utiliza para la gestión de la información.
- Personal: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.

- Servicios: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo, la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo, la comercialización de productos).

- Tecnología: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)

- Instalaciones: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)

- Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.).

Con el fin de hacer la identificación de los activos de la empresa, es recomendable realizar un inventario de dichos activos. El inventario de activos a utilizarse para la gestión de la seguridad no debería duplicar otros inventarios, pero sí que debería recoger los activos más importantes e identificarlos de manera clara y sin ambigüedades.

El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos en funcionamiento e incluso poder recuperarse ante un desastre.

La información que describe a un activo deberá contener como mínimo:

- Identificación del activo: Un código para ordenar y localizar los activos.
- Tipo de activo: A qué categoría de las anteriormente mencionadas pertenece el activo.
- Descripción: Una breve descripción del activo para identificarlo sin ambigüedades.
- Propietario: Quien es la persona a responsable del activo.
- Usuario: Quien es la persona que lo usa
- Custodio: Quien resguarda el activo
- Ubicación: Dónde está físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.

### 3.2.4 Usuarios y Perfiles

En las organizaciones hay una variedad de personas haciendo uso de los recursos tecnológicos, físicos y en general, de todos los elementos que el que hacer debe proveer a los funcionarios para poder desempeñar sus tareas. Precisamente es aquí donde se hace necesario clasificar cada una de las personas que trabajan en la empresa, teniendo en cuenta sus funciones y a lo que deberían tener acceso y por supuesto cuales serían las restricciones que deberían tener.

Los funcionarios públicos, contratistas, pasantes y a nivel general, personal que labora para la organización, deben tener acceso solo a la información necesaria para el desarrollo de sus actividades y funciones propias de su cargo. En el caso de que personas ajenas a la empresa, se requerirá de privilegios especiales, los cuales deberán ser autorizados por la dirección de seguridad o del área encargada de otorgar dichos permisos.

El otorgamiento de acceso a la información deberá estar regulado mediante las normas y procedimientos definidos por la gerencia de tecnología y de seguridad de la información, con el aval de la dirección general de la empresa. Todos los privilegios para el uso de los sistemas de información de la organización deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad. En el caso de Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas. [8]

Para dar acceso a la información se debe tener en cuenta:

- La clasificación de la información misma al interior de la organización, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la misma.
- Monitoreo de eventos en los distintos recursos informáticos de la plataforma tecnológica de la empresa, como lo es el sistema operativo y la red de la organización.
- Seguimiento a los accesos realizados por los usuarios a la información de la empresa, con el fin de minimizar en tanto sea posible el riesgo de pérdida de integridad de la información.

Adicional a lo anterior, se deberá clasificar los grupos de usuario y definir cuáles serán sus permisos en términos de acceso y manipulación de la información de la empresa. a continuación de definen algunos conceptos para realizar la clasificación de los usuarios y perfiles:

1. Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los servicios tecnológicos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.
2. Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el de la Administración de usuarios.
3. Las Puertas Traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan. [8]

### 3.2.5 Clasificación de la Información

La información debe ser clasificada teniendo en cuenta su necesidad, prioridades y nivel de protección previsto para su manipulación y tratamiento.

La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar a las diferentes áreas de la organización la necesidad de medidas especiales para la manipulación de dicha información. Los atributos mínimos que se deben tener en cuenta para la clasificación de la información son los siguientes: Confidencialidad, Integridad y Disponibilidad; a continuación, se muestra en la tabla 1 la clasificación de la información de acuerdo a los atributos mínimos que esta debe tener:

**Tabla 1. Clasificación de la Información según sus atributos**

| | Confidencialidad | Integridad | Disponibilidad |
|---|---|---|---|
| **Clasificada** | X | X | X |
| **Reservada** | X | X | |
| **Privada** | X | | |
| **De uso Interno** | | | X |
| **Publica** | | X | X |

Fuente:http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Clasificacion_de_la_Informacion.pdf

Los parámetros o factores que se deben tener en cuenta para la clasificación de la información son:

- Costo de reemplazo o reconstrucción
- Interrupción del negocio
- Pérdida de clientes
- Violación de la propiedad
- Requerimientos Legales
- Pérdidas económicas

Los beneficios de clasificar la información son:

- Identificar qué información es sensible y vital para la organización, en este caso, EMCALI.
- Identificar quiénes son los dueños de la información y los responsables de la asignación de los permisos de acceso a la misma.
- Definir niveles apropiados de protección de la información y clasificación de acceso a la misma.
- Controlar y monitorear qué usuarios tienen acceso a la información. [9]

Riesgos de no clasificar la información:

- Asignación errada de niveles y/o permisos de acceso a la información que no corresponde.
- Pérdida de Información por acciones de usuarios malintencionadas.
- Modificación de la información sin previa autorización.
- Uso de la información por parte de usuarios con fines personales.

A continuación, se describen algunos criterios de evaluación que permiten clasificar o agrupar la información de acuerdo a sus características:

- Confidencialidad/Privacidad: Se refiere a que la información solo puede ser conocida por usuarios autorizados.
  - En este punto pensar: ¿Qué sucedería si la información de los clientes, proveedores, servicios, valores entre otros, es cedida a terceros?
- Integridad: Se refiere a que la información solo puede ser variada (modificada o borrada) por usuarios autorizados.
  - En este punto pensar: ¿Qué sucedería si alguien no autorizado realiza modificaciones en la información de presupuesto, información de clientes, información de facturación de servicios, etc.?

### 3.2.6 Selección de herramientas libres para la detección de vulnerabilidades

Como parte de las acciones preventivas que la organización debería ejecutar para identificar y prevenir ataques o cualquier tipo de situación que represente una amenaza para la seguridad de la información, se encuentra el análisis de vulnerabilidades. Para esto, existen herramientas free o de libre distribución que pueden ser utilizadas por las empresas y organizaciones. Específicamente para el contexto de la red interna y el sistema operativo de la empresa, se recomienda el uso de 3 herramientas para la detección de vulnerabilidades.

De acuerdo a la NTC-ISO/IEC 27001 la organización debe determinar acciones para eliminar la causa de no conformidades potenciales. Las acciones preventivas que se vayan a tomar deben ser apropiadas al impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva deberá definir requisitos para:

- Identificar no conformidades potenciales y sus causas;
- Evaluar la necesidad de acciones para impedir que las no conformidades ocurran.
- Determinar e implementar la acción preventiva necesaria;
- Registrar los resultados de la acción tomada (véase el numeral 4.3.3), y
- Revisar la acción preventiva tomada.

Por lo anterior, la organización deberá también identificar los cambios en los riesgos e identificar los requisitos en cuanto a acciones preventivas, concentrando la atención en los riesgos que han cambiado de manera significativa.

A continuación, se presentan 3 herramientas de libre distribución (Herramientas gratuitas) que EMCALI y a nivel general cualquier otra empresa, especialmente aquellas de pequeña y mediana escala pueden implementar para la detección de vulnerabilidades en sus sistemas:

- **Nessus**

Nessus es un programa de escaneo de vulnerabilidades en diversos entornos operativos. Consiste en un daemon (Nessusd), que realiza el escaneo en el sistema objetivo y Nessus cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Además de escanear diversos sistemas operativos, permite el escaneo de las redes en las cuales tiene la posibilidad de detectar posibles vulnerabilidades en las maquinas que funcionen en una red. Es por ello que esta se utiliza para comprobar la seguridad y encontrar vulnerabilidades para que puedan ser solucionadas por los administradores del sistema.

Nessus comienza escaneando los puertos con Nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, lenguaje de Scripting de ataques Nessus), el cual es un leguaje scripting optimizado para interacciones personalizadas en redes.

Nessus es un analizador de seguridad de redes potente y fácil de usar, con una amplia base de datos de pluggins que se actualiza a diario. Actualmente se encuentra entre los productos más importantes de este tipo en todo sector de la seguridad y cuenta con el respaldo de organizaciones profesionales de seguridad de la información, tales como SANS Institute.

A diferencia de muchos otros analizadores de seguridad, Nessus no da por hecho nada. Es decir, no supone que un servicio dado se ejecuta en un puerto fijo. Esto significa que, si se ejecuta el servidor web en el puerto 1234, Nessus lo detectara y probara su seguridad según corresponda. Por ello en cuando sea posible intentara validar una vulnerabilidad a través de su explotación. En los casos que no se confiable o se pueda afectar de manera negativa el destino, Nessus puede basarse en un banner del servidor para determinar la presciencia de la vulnerabilidad.

Esta herramienta aporta beneficios a la entidad que lo utiliza para identificar que tan vulnerable se encuentra la información dentro de la infraestructura manejada por la empresa. Por ende, provee los siguientes beneficios para la comprensión de los usuarios y estimación de vulnerabilidades que encuentran en las redes y sistemas operativos de la organización tales como:

- Proporciona una interfaz de usuario (GUI) en donde muestra los resultados de los análisis en tiempo real, por lo cual es necesario esperar que se terminen los análisis para poder revisar los resultados.
- Genera archivos .nessus que son utilizados por los productos deTenable como estándar para directivas de análisis y datos de vulnerabilidades.
- Brinda una interfaz unificada para el analizador Nessus que es independiente de la plataforma base.
- Los análisis siempre seguirán ejecutándose en el servidor, aun si nos desconectamos de la red.
- Permite conocer que agujeros de seguridad pueden tener los servicios susceptibles a ataques.
- Funciona mediante un procedimiento de alta velocidad por el que encuentra los datos sensibles y trabaja con la auditoria de configuraciones y el perfil activo.
- El servidor es el encargado de realizar todo el trabajo de escaneo que especifica el cliente.
- Indica la vulnerabilidad existente, e indica como explotar esta y como proteger al equipo de ella.
- Permite realizar auditorías de forma remota en una red en particular y determinar si ha sido comprometida o usada de alguna forma inadecuada.
- Nessus no solo informara que vulnerabilidades de seguridad existen en su red y el riesgo de cada una de ellas, sino que también notificara sobre como mitigarlas, ofreciendo soluciones.

Esta herramienta maneja 5 niveles de gravedad: Informativo, Riesgo Bajo, Riesgo Medio, Riesgo Alto y Riesgo Critico. Estos niveles de criticidad nos permitirán ver el estado de vulnerabilidad de la infraestructura tecnológica utilizada dentro de la empresa.

### ➢ OpenVas

OpenVas (Open Vulnerability Assessment System – sistema abierto de Evaluación de vulnerabilidades) es una herramienta gratuita que provee una solución para todo lo que está relacionado con el análisis de vulnerabilidades que se puedan estar presentando en un sistema y a partir de allí tomar medidas de seguridad que se verán reflejadas en un correcto funcionamiento de la estructura.

Esta herramienta protegerá el sistema ante vulnerabilidades de red o IP, además permitirá identificar fallas de seguridad, siendo un Framework que brinda servicios y herramientas para realizar análisis de vulnerabilidades y gestión de vulnerabilidades.

Openvas funciona principalmente con dos servicios o programas diferentes: Un servidor (escáner), que es el encargado de realizar el análisis de las vulnerabilidades y un cliente, que es utilizado por el usuario para configurar y presentar los resultados de los mismos. Ambos Perfiles pueden estar instalados en el mismo equipo, o también es posible tener instalado el servidor en un equipo diferente y realizar la conexión remota.

Es por ello que esta herramienta nos proporciona utilidades al momento de su uso tales como:

- Posibilita realizar un escaneo de forma simultánea en varios equipos.
- Soporta protocolo SSL.
- Permite implementar escaneos programados.
- Se puede pausar o reiniciar las tareas de escaneo en cualquier momento.
- Permite administrar usuarios desde la consola.
- Soporta protocolos de transferencia de datos como HTTP y HTTPS.
- Soporta multilenguaje
- Es multiplataforma
- Reportes claros y completos de los análisis realizados en la infraestructura tecnológica.

En la tabla 2 se presenta un cuadro comparativo entre ambas herramientas, destacando ventajas y desventajas en su uso:

**Tabla 2. Cuadro comparativo entre Nessus y OpenVas**

| | Nessus | OpenVas |
|---|---|---|
| Ventajas | • Fácil de instalar, en sus últimas versiones se ha reducido a la mínima expresión para que el usuario no tenga inconvenientes al realizarlo. | • El uso de opciones como métodos de acceso: puede ser utilizado como interfaz web como aplicación cliente. |
| | • Posee mayor cantidad de plugins para cubrir defectos locales y remotos. | • No tiene limitaciones, ni número de máquinas ni cantidad de análisis permitidos. |
| | • Los tiempos de escaneo son menores en comparación a otras herramientas de escaneo de vulnerabilidades. | • Ser gratuita la herramienta es una ventaja para su adquisición. |
| | • Interfaz limpia la cual es amigable y agradable a la vista. | • El soporte lo dan varias empresas. |
| | • Posee actualizaciones constantes de plugins para nuevos defectos encontrados en el entorno del sistema. | |
| | • El soporte lo realiza una sola empresa. | |

Continuación Tabla 2.

| | | |
|---|---|---|
| **Desventajas** | • Al ser la interfaz más simple, implica que también falten algunas características como por ejemplo el escalado de eventos ni la posibilidad de crear filtros para evitar los falsos positivos. | • Es un poco más complejo de instalar y configurar ya que consta de varios componentes. |
| | • El costo de la licencia para el uso anual de la herramienta profesional. | • Al tener más opciones de uso también resulta más complejo de usar. |
| | | • Por ser un producto open source puede ofrecer menos garantías de soporte. |
| | | • No cuenta con suficiente plugins para vulnerabilidades críticas. |

- **Kali Linux**

Kali Linux es la nueva generación de la distinguida distribución Linux BackTrack para realizar auditorías de seguridad y pruebas de penetración, siendo así una plataforma basada en GNU/Linux Debian y es una restauración completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades. Explotarlas, escalar privilegios y cubrir las huellas.

Kali Linux tiene preinstalados una gran cantidad de herramientas vinculadas con el tema de la seguridad informática (más de 600 programas), siendo algunas de las más conocidas como Wireshark (un sniffer), John the Ripper (un crackeador de passwords), Nmap (un escaneador de puertos) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas), además del extraordinario Metasploit, la gran suite de explotación de vulnerabilidades.

Esta distribución es muy fácil de instalar (posee la instalación de Debian), a pesar de no ser tan fácil de usar, hay gran variedad de información en la web y personas que saben usar el entorno y compartir sus conocimientos, por lo que facilita su aprendizaje.

Kali posee:

- Más de 300 herramientas de pruebas de penetración: Después de revisar todas las herramientas que se incluyen en BackTrack, hemos eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar.
- Gratis y siempre lo será: Kali Linux, al igual que su predecesor, es completamente gratis y siempre lo será. Nunca, jamás, tendrás que pagar por Kali Linux.
- Git – árbol de código abierto: Somos partidarios enormes de software de código abierto y nuestro árbol de desarrollo está disponible para todos y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.
- Obediente a FHS: Kali ha sido desarrollado para cumplir con el Estándar de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc.
- Amplio apoyo a dispositivos inalámbricos: Hemos construido Kali Linux para que soporte tantos dispositivos inalámbricos como sea posible, permitiendo que funcione correctamente en una amplia variedad de hardware y hacerlo compatible con varios USB y otros dispositivos inalámbricos.
- Kernel personalizado con parches de inyección: Como probadores de penetración, el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricas para que nuestro kernel tenga los últimos parches de inyección incluidos.
- Entorno de desarrollo seguro: El equipo de Kali Linux está compuesto por un pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros.
- Paquetes firmados con PGP y repos: Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos. Los repositorios posteriormente firman los paquetes también.
- Multi-lenguaje: Aunque las herramientas de penetración tienden a ser escritas en inglés, nos hemos asegurado de que Kali tenga soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.
- Totalmente personalizable: Estamos completamente conscientes de que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho lo más fácil posible para nuestros usuarios más aventureros puedan personalizar Kali Linux a su gusto, todo el camino hasta el núcleo.
- Soporte ARMEL y ARMHF: Dado a que los sistemas basados en ARM son cada vez más frecuentes y de bajo costo, sabíamos que el soporte de ARM de Kali tendrían

que ser tan robusta como podríamos administrar, resultando en instalaciones que trabajan en sistemas de ARMEL y ARMHF. Kali Linux tiene repositorios ARM integrado con la línea principal de distribución de modo que las herramientas para ARM serán actualizada en relación con el resto de la distribución.

## 3.3 FASE III: Políticas y Controles de Seguridad

Una política es un conjunto de orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado, en este caso, el campo de la seguridad de la información. En este sentido, una política en seguridad de la información debe tener unas políticas específicas, unos procedimientos, unos estándares o prácticas, unos controles y una estructura organizacional.

### 3.3.1 Políticas Específicas

Definen en detalle los aspectos específicos que regulan el uso de los recursos tecnológicos y recursos de información y suelen ser más susceptibles al cambio, a diferencia de la política general de la organización.

### 3.3.2 Procedimientos

Definen los pasos para realizar una actividad específica y evitan que se aplique el criterio personal, es decir, una actuar subjetivo de quien vive una situación determinada.

### 3.3.2 Estándares

Es un documento establecido por consenso que sirve de patrón, modelo o guía que se usa de manera repetitiva. Los estándares de seguridad suelen ser actualizados periódicamente ya que dependen directamente de la tecnología.

### 3.3.3 Creación De Una Política

De acuerdo a la NTC-ISO/IEC 27001, es de suma importancia que la empresa seleccione los controles y políticas para el tratamiento de los riesgos.
Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos.

Esta selección debe tener en cuenta los criterios para la aceptación de riesgos al igual que los requisitos legales, reglamentarios y contractuales.

Para crear una política de seguridad de la información, es importante tener en cuenta que dicha política debe tener:

- Objetivo: Qué se desea lograr.
- Alcance: Qué es lo que se protege y quienes deben cumplirla.
- Definiciones: Aclaración de términos utilizados.
- Responsabilidades: Qué debe y no debe hacer cada persona
- Revisión: Como será monitoreado el cumplimiento (Seguimiento, Indicadores, Resultados)
- Aplicabilidad: En qué casos será aplicable.
- Referencias: Documentos complementarios (Anexos). [3]

En el documento de la norma NTC-ISO/IEC 27001, se listan una serie de controles que la organización debería implementar, pero no necesariamente implica que deban implementarse en su totalidad; en este sentido, la empresa está en la libertad de analizar y seleccionar los controles que aplican para su necesidad puntual. No obstante, cualquier exclusión de controles, considerada necesaria para satisfacer los criterios de aceptación de riesgos, necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables. En donde se excluya cualquier control, las declaraciones de conformidad con esta norma no son aceptables a menos que dichas exclusiones no afecten la capacidad de la organización y/o la responsabilidad para ofrecer seguridad de la información que satisfaga los requisitos de seguridad determinados por la valoración de riesgos.

Los objetivos de control y los controles deben ser seleccionados como parte del establecimiento e implementación de políticas de seguridad al interior de la organización, que, a su vez, permitirán la estructuración de un sistema de gestión de la seguridad de la información. A continuación, en la figura 4, se muestran los dominios de la Norma ISO 27001 que se deben tener en cuenta para definir el plan de tratamiento de riesgos dentro de la empresa:

**Ilustración 9. Dominios de la Norma ISO 27001**


Fuente: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf

Para definir los controles a implementar en Emcali, es recomendable hacer una selección de aquellos controles que la organización considere más importantes y primordiales; no obstante, el estado ideal es que todos los controles sean implementados, pero la idea es que paulatinamente se vayan incorporando dichas políticas y controles conforme va madurando y creciendo el sistema de gestión de seguridad de la información en la organización.

Algunos criterios que se pueden tener en cuenta para la selección e implementación de los controles de seguridad de la información descritos en la Norma ISO 27001 son:

- Qué implicaciones tendría la implementación del control, en términos económicos como humanos. En este sentido, la empresa deberá preguntarse: ¿Tengo lo recursos económicos, humanos y técnicos para implementar e control?
- Que tan necesario es implementar un control u otro.
- Que controles ya existen en la organización. En este punto, la empresa deberá evaluar si el control existente se ha aplicado de manera correcta teniendo los resultados obtenidos o si por el contrario debe modificarse.

- Teniendo en cuenta que esta metodología se enfoca en el sistema operativo y la red interna de la organización, se recomienda seleccionar controles que le apunten a estos dos ámbitos inicialmente.

Adicional a lo anterior, es importante que, al momento de formular las políticas de seguridad de la información, se consideren aspectos como:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con las áreas o unidades dueñas de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada área o gerencia de la organización, pues son ellos los interesados en proteger los activos críticos en su área.
- Monitorear de manera periódica los procedimientos y operaciones de la empresa, de forma tal, que ante posibles cambios que se puedan presentar, dichas políticas puedan adaptarse a esos nuevos cambios.
- Detallar concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas establecidas. [10]

### 3.3.4 Implementación de controles

Seleccionar los objetivos de control y los controles para el tratamiento de riesgos deberá incluir la elaboración de un documento donde se incluya:

1. Los controles más importantes que se seleccionaron para ser implementados.
2. Los objetivos de control y controles que actualmente se encuentran implementados en la organización.
3. Listado de controles que se excluyeron de la implementación con la respectiva justificación de porque no se implementaran dentro de la organización. Cabe aclarar que el hecho de que un control sea excluido no implica que más adelante la organización determine incluirlo.

Una vez se haga la selección de los controles, es de suma importancia que la organización evalúe y verifique el correcto funcionamiento de dichos controles. Para esto, los dueños o propietarios de los activos objeto de protección deberán definir objetivos e indicadores que permitan medir que tan efectivos están siendo los controles implementados.

### 3.3.5 Controles que se deben aplicar en la empresa EMCALI E.I.C.E

A continuación, se relacionan los controles a tener en cuenta, específicamente en el ámbito de sistema operativo y red interna de la empresa EMCALI E.I.C.E.

En el anexo 1, se relaciona el detalle de cada uno de los controles descritos a continuación, basados en la Norma ISO 27001:

3.3.5.1 Controles y políticas relacionadas con la misión y visión de EMCALI E.I.C.E

- Definición de Política De Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Cambios en los contratos de terceros
- Categorización y clasificación de la documentación

3.3.5.1 Controles y políticas relacionadas con el personal y recursos humanos de EMCALI E.I.C.E

- Seguridad de los recursos humanos
- Definiciones de la contratación de personal (Antes, durante y después del contrato)
- Definición de roles y responsabilidades.
- Educación, Formación y concientización sobre la Seguridad de la Información

3.3.5.2 Controles y políticas relacionadas con los sistemas de información de EMCALI E.I.C.E

- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Protección contra amenazas externas y ambientales
- Ubicación y protección de los equipos
- Gestión de la Prestación del Servicio por Terceras Partes
- Planificación y aceptación del sistema.
- Protección de la integridad del software y de la información
- Monitoreo del uso de los sistemas
- Controles de acceso a la información por parte de los usuarios.

- Control de accesos a la red
- Control de acceso a sistema operativo
- Controles criptográficos
- Gestión de la vulnerabilidad técnica
- Cumplimiento de los requisitos legales

## 3.4 FASE IV: Aseguramiento y configuración del sistema operativo y redes internas de la organización.

Uno de los factores más importantes dentro de la metodología de análisis de vulnerabilidades en la organización es el aseguramiento de la información y la forma como se configuración los servicios que brinda la empresa y las herramientas que esta usa para prestar tales servicios.

Dentro de las herramientas que la empresa usa a diario, se encuentra el sistema operativo el cual control el acceso y uso de los recursos de un equipo de cómputo, lo que lo hace uno de los elementos más aptos para intentar explotar cualquier vulnerabilidad o posible brecha de seguridad. Por lo anterior, a nivel del sistema operativo se deben contemplar factores como los que se mencionan a continuación:

- Control de acceso a los recursos del sistema
- Autenticación de usuarios
- Monitoreo de las acciones que realizan los usuarios
- Seguimiento de los eventos que representan posibles riesgos o amenazas
- Garantía de integridad de los datos almacenados en los equipos de cómputo
- Garantía de la disponibilidad de los recursos

De acuerdo a Garzón, Ratkovich y Vergara (2005), *"La mayoría de los problemas de seguridad comienzan por una mala configuración de los servicios, los cuales son dispuestos con sus configuraciones por defecto, lo que hace que, para un atacante, sea mucho más sencillo el tener control de estos"*. Por lo anterior, se recomienda que la empresa se apoye en el uso de herramientas como escaneadores de puertos, así como el uso de firewalls los cuales ayudan a proteger de la red interna de la organización; no obstante, el uso de estas herramientas por si solas constituyen una solución final a todos los problemas de seguridad.

Precisamente en pro del aseguramiento de los sistemas de la organización, el análisis de vulnerabilidades se convierte en una práctica de suma importancia como medida de control

y prevención de posibles ataques a la información donde quiera que esta se encuentre dispuesta, en este caso específicamente, en el sistema operativo y la red interna de la organización. Siguiendo la misma línea de aseguramiento y dentro del contexto de las herramientas que ayudan a garantizar esta tarea, se encuentran los antivirus de marcas distinguidas de libre distribución o bajo costo como lo son AVG, Kaspersky, Bitdefender, entre otros; dichas herramientas permiten reconocer de manera óptima los archivos sospechosos , archivos con apariencia de virus y virus como tal, lo que los hace muy útiles a la hora de buscar una solución free o de bajo costo a la hora de buscar un antivirus.

Cabe resaltar que no basta solamente con realizar el análisis de vulnerabilidades sino también se hace necesario categorizar dichos hallazgos y generar planes de acción que busquen mitigar en tanto sea posible que esas vulnerabilidades se conviertan en una amenaza y aún más se materialicen.

Según lo anterior, las vulnerabilidades a nivel de red o sistema operativo pueden catalogarse de la siguiente forma:

- Vulnerabilidad de Diseño: Se basan en problemas basados en el planteamiento de las políticas de seguridad del sistema o en el desarrollo de los protocolos utilizados por la red.
- Implementación: Basadas en fallos tanto en la planificación, como en la programación final del software que permiten por error del fabricante posibles “puertas traseras” que facilitan la manipulación de los equipos por individuos no deseados.
- Utilización: Se debe a desconocimiento y falta de responsabilidad en la utilización de los equipos que, combinada con una mala configuración de los sistemas (ya sea por ignorancia o por negligencia), puede provocar una disponibilidad indeseada de herramientas que faciliten los ataques.

Una vez conocidos los diferentes tipos de vulnerabilidades en función de su origen, es posible detallar una a una las vulnerabilidades en función de sus causas y de los efectos que producen:

- Vulnerabilidad de validación de entrada: Es aquella que se produce cuando la entrada que procesa un sistema no es comprobada adecuadamente y puede dar pie a una entrada corrupta.
- Vulnerabilidad de salto de directorio: Se aprovecha la debilidad de la seguridad o su completa ausencia en un servicio de red para acceder a los diferentes directorios hasta llegar a la raíz del sistema.

- Vulnerabilidad de seguimiento de enlaces: En esta ocasión y de forma muy parecida a la citada anteriormente, se produce el salto entre directorios a través de un enlace simbólico o un acceso directo.
- Vulnerabilidad de inyección de comandos en el sistema operativo: No es más que la capacidad de un usuario para teclear instrucciones que puedan comprometer la seguridad.
- Vulnerabilidad de ejecución de código cruzado: Se basa en la ejecución de un script de código por parte de un atacante en un dominio ajeno. Normalmente el aprovechamiento de esta vulnerabilidad se hace efectivo sobre aplicaciones web o funcionalidades del propio navegador. El objetivo que se tiene es obtener datos cruzados o incluso el control de sesiones. Se puede presentar dos versiones, siendo la primera "reflejada", en la que se pasan variables entre dos páginas web para evitar el uso de sesiones de tal forma que se aprovechan las cookies o incluso la cabecera HTTP para el ataque. La segunda versión sería la "persistente", en la que se localizan puntos débiles en los que se incrusta código.
- Vulnerabilidad de inyección SQL: Esta vulnerabilidad se da directamente sobre las bases de datos basadas en lenguaje SQL. El objetivo es explotarla añadiendo código SQL sobre otro código SQL para cambiar el comportamiento del mismo. Se pueden cambiar consultas en las que se obtiene información por otras en las que se elimina o se pueden sobrescribir datos. Esta vulnerabilidad suele ser causa de la negligencia del administrador de sistemas que puede dejar la base de datos montada con problemas de seguridad y siendo vulnerable a la ejecución de código ajeno.
- Inyección directa de código estático: En este caso, un fallo en el software permite que se inyecte código en un archivo de salida que vaya a procesarse posteriormente. Puede llegar a almacenarse este código en una base de datos con lo que ésta quedaría corrupta y se debería considerar como tal.
- Vulnerabilidad de error de búfer: Esta vulnerabilidad es una de las más comunes puesto que se aprovecha de la necesidad de las aplicaciones de utilizar búferes para almacenar información temporalmente mientras se procesa.
- Agotamiento de búfer: es una vulnerabilidad que aparece cuando en un búfer de comunicación entran tan pocos datos como para que la velocidad con que se leen sea mayor que la velocidad con que entran datos. Para evitar este fallo se necesita que el búfer detenga el proceso cuando esto ocurra. [4]

# 4. EXPERIMENTACIÓN: ANALISIS DE VULNERABILIDADES EN SISTEMA OPERATIVO Y RED DE EMCALI E.I.C.E

## 4.1 Evaluación de la Metodología propuesta

La metodología propuesta en este trabajo es un hibrido entre las buenas practicas mencionadas en la Norma ISO 27001 y la Metodología propuesta por Garzón, Ratkovich y Vergara (2005). La importancia de la metodología aquí propuesta radica en que ésta se enfoca en el análisis de vulnerabilidades a niel del sistema operativo y la red interna de una organización como parte del 'Hacer' en términos de gestión de la seguridad de la información. A continuación, se presenta en la tabla 3, un cuadro comparativo entre las metodologías:

**Tabla 3. Metodología Hibrida Vs Metodología Javeriana Vs Norma ISO 27001**

| | Metodología Hibrida | ISO 27001 | Metodología Javeriana |
|---|---|---|---|
| **Estructura** | Se estructura en 4 fases, cada una con una serie de objetivos. | Se estructura en una serie de pasos y recomendaciones. | Se estructura en 6 fases, cada una con unos objetivos concretos. |
| **Tipo de empresa donde se puede aplicar** | La metodología está dirigida a las pequeñas y medianas empresas. | Esta Norma se puede aplicar en cualquier tipo de organización. | La metodología está dirigida a las empresas de mediana y pequeña escala. |
| **¿Que define la metodología?** | Define unas fases, específicamente para realizar análisis de vulnerabilidades a nivel del sistema operativo y red. | Define los requisitos para gestionar la seguridad de la información en una organización. | Define una serie de fases para realizar análisis de vulnerabilidades en los diferentes sistemas que contienen la información de la organización. |
| **¿Cuál es el aspecto que más resalta?** | El relacionamiento con la gerencia de la organización como parte vital del cambio. | Resalta varios aspectos internos de la organización con el mismo nivel de importancia. | No hace mención del papel que debe jugar la gerencia en la definición de políticas en cuestión del aseguramiento de la información. |

| | | | |
|---|---|---|---|
| **¿Qué herramientas sugiere para su uso?** | Sugiere el uso de herramientas libres para el escaneo de vulnerabilidades a nivel del sistema operativo y la red de la organización. | No hace mención de herramientas. Se enfoca en dar las pautas de las actividades y tareas a realizar. | Define recomendaciones globales a nivel técnico sin sugerir herramientas. |
| **¿Qué modelo de procesos trabaja?** | Toma como foco principal la fase de "Hacer" del modelo de procesos PHVA. | Adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) de manera completa. | Se centra en el aseguramiento de los recursos de la empresa tomando como base los 5 pilares de la seguridad informática |
| **¿Qué medidas en cuanto a la clasificación de la información sugiere?** | Involucra una forma de clasificar la información que se maneja al interior de la organización, teniendo en cuenta los atributos mínimos que esta debe cumplir. | No detalla una forma específica de clasificación de la información. | No se sugiere una forma o mecanismo para realizar dicha clasificación. |
| **¿Qué tipos de controles y políticas de seguridad de información abarca?** | Contiene una selección de controles y objetivos de control que apuntan a la misión y visión de la organización, los recursos humanos y los sistemas de información. | Contiene un amplio listado de objetivos de control que apuntan a varios ámbitos de la organización. | Contempla una fase de políticas de seguridad, pero no se especifica cuáles políticas se pueden implementar. |
| | Recomienda a la organización formular sus propias políticas de seguridad teniendo en cuenta sus necesidades puntuales. | No se da detalle de cómo podría crearse una política ni qué elementos deberían componer dicha política. | No se da detalle de cómo podría crearse una política ni qué elementos deberían componer dicha política. |

## 4.2 Métricas De Puntuación De Vulnerabilidad Según La Unión Internacional De Comunicaciones

La Recomendación UIT-T X.1521 sobre el sistema común de puntuación de la vulnerabilidad (CVSS) proporciona un marco abierto para comunicar las características y los efectos de las vulnerabilidades de las tecnologías de la información y las comunicaciones en los programas comerciales o de código abierto utilizados en las redes de comunicaciones, o cualquiera de los otros tipos de TIC capaces de ejecutar software. El objetivo de la Recomendación es permitir a los administradores de TIC, proveedores de boletines de vulnerabilidad, proveedores de seguridad, proveedores de aplicaciones e investigadores hablar desde un lenguaje común para anotar las vulnerabilidades de las TIC.

El grupo de métricas base representa las características intrínsecas de una vulnerabilidad que son constantes en el tiempo y en entornos de usuario. Se compone de dos conjuntos de métricas: las métricas de explotabilidad y las métricas de impacto. [11]

Las métricas de explotabilidad reflejan la facilidad y los medios técnicos por los cuales la vulnerabilidad puede ser explotada. Es decir, representan características de lo que es vulnerable, a lo que nos referimos formalmente como el componente vulnerable. Por otro lado, las métricas de impacto reflejan la consecuencia directa de una explotación exitosa y representan la consecuencia de la cosa que sufre el impacto, a la que nos referimos formalmente como el componente impactado.

Si bien el componente vulnerable suele ser una aplicación de software, un módulo, un controlador, etc. (o posiblemente un dispositivo de hardware), el componente afectado podría ser una aplicación de software, un dispositivo de hardware o un recurso de red. Este potencial para medir el impacto de una vulnerabilidad que no sea el componente vulnerable, es una característica clave de CVSS v3.0.

El grupo de métricas temporales refleja las características de una vulnerabilidad que puede cambiar con el tiempo, pero no entre los entornos de usuario. Por ejemplo, la presencia de un kit de exploit simple de usar aumentaría la puntuación CVSS, mientras que la creación de un parche oficial lo disminuiría.

Generalmente, las métricas Base y Temporal son especificadas por analistas de boletines de vulnerabilidad, proveedores de productos de seguridad o proveedores de aplicaciones, ya que normalmente poseen la información más precisa sobre las características de una vulnerabilidad. Por otro lado, las métricas ambientales son especificadas por las organizaciones de usuarios finales porque son las mejores capaces de evaluar el impacto potencial de una vulnerabilidad dentro de su propio entorno informático.

La puntuación de las métricas CVSS también produce una cadena vectorial, una representación textual de los valores de métrica utilizados para puntuar la vulnerabilidad. Esta cadena vectorial es una cadena de texto con formato específico que contiene cada valor asignado a cada métrica y siempre debe mostrarse con la puntuación de vulnerabilidad.

### 4.2.1 Métricas de explotación

Como se mencionó, las métricas de explotabilidad reflejan las características de lo que es vulnerable, a lo que se hace referencia formalmente como el componente vulnerable. Por lo tanto, cada una de las métricas de explotabilidad enumeradas a continuación debe ponerse en relación con el componente vulnerable y reflejar las propiedades de la vulnerabilidad que conducen a un ataque exitoso.

- **Vector de acceso (AV)**

Esta métrica refleja cómo se explota una vulnerabilidad; Cuanta mayor sea la distancia a la que un agresor puede atacar a un anfitrión, mayor será la puntuación de la vulnerabilidad. La lista de valores posibles se presenta en la Tabla 5.

**Tabla 4. Vector de Ataque**

| Valor Métrico | Descripción |
|---|---|
| Local (L) | Una vulnerabilidad que sólo pueda explotarse a través de acceso local requiere que el agresor tenga acceso físico al sistema vulnerable o una cuenta local (shell). Ejemplos de vulnerabilidades explotables en local son los ataques a través de elementos periféricos, tales como ataques a través de cortafuegos /USB DMA y ataques con escalado basado en privilegios locales (por ejemplo, sudo). |
| Red Adyacente (A) | Una vulnerabilidad que pueda explotarse mediante el acceso desde una red adyacente requiere que el agresor tenga acceso al dominio de difusión o de colisión del software vulnerable. Son ejemplos de redes locales las subredes IP, Bluetooth, IEEE 802.11 y el segmento local Ethernet. |
| Red (N) | Una vulnerabilidad que pueda explotarse mediante el acceso a través de la red significa que el software vulnerable está asociado a la capa de red, no requiriendo el agresor acceso a través de red local o de acceso local. Dicha vulnerabilidad se denomina a menudo "explotable a distancia". Un ejemplo de ataque de red es el desbordamiento de la memoria intermedia RPC. |

- **Complejidad de ataque (AC)**

Esta métrica mide la complejidad del ataque requerido para explotar la vulnerabilidad una vez que el agresor ha ganado acceso al sistema objetivo. En otras palabras, este factor se refiere a la complejidad del ataque que se lleva a cabo para aprovechar esta vulnerabilidad y sus valores pueden ser alto, medio o bajo. La lista de valores posibles se presenta en la Tabla 6.

**Tabla 5. Complejidad de Ataque**

| Valor Métrico | Descripción |
|---|---|
| Alto (H) | Las condiciones de acceso son especiales. Por ejemplo:<br>• En la mayoría de las configuraciones, la parte agresora debe tener un elevado nivel de privilegios o actuar con una identidad falsa en otros sistemas, además de atacar el sistema objetivo (por ejemplo, apropiación de DNS).<br>• El ataque se basa en métodos de ingeniería social que serían fácilmente detectados por personas con suficientes conocimientos. Por ejemplo, cuando la víctima lleva a cabo actuaciones sospechosas o atípicas.<br>• La configuración vulnerable es muy poco frecuente en la práctica.<br>• Si se produce un estado de carrera, la ventana es muy estrecha. |
| Medio (M) | Las condiciones de acceso son en cierta medida especiales; por ejemplo:<br>• La parte agresora se limita a un grupo de sistemas o usuarios con un determinado nivel de autorización, posiblemente no fiable.<br>• Es necesario recopilar determinada información antes de lanzar un ataque con éxito.<br>• La configuración afectada no es la utilizada por defecto ni la que se configura normalmente (por ejemplo, una vulnerabilidad que se produce cuando un servidor realiza la autentificación de la cuenta de un usuario mediante un esquema especial, pero que no está presente para otros esquemas de autentificación).<br>• El ataque exige una cierta dosis de ingeniería social que puede ocasionalmente engañar a usuarios cautelosos (por ejemplo, ataques de suplantación que modifican la barra de estado de los navegadores para mostrar enlaces falsos o utilizar la lista de contactos de alguien para enviar mensajería instantánea maliciosa). |
| Bajo (L) | No existen condiciones de acceso especiales o circunstancias atenuantes. |

- **Autentificación (Au)**

Esta métrica mide el número de veces que un agresor debe autentificarse ante un objetivo para explotar una vulnerabilidad. Esta métrica no mide la fortaleza o complejidad del proceso de autentificación, sino el hecho de que el agresor deba presentar credenciales antes de explotar la vulnerabilidad. En la tabla 7 se enumeran los posibles valores de esta métrica. Cuantas menos instancias de autentificación sean necesarias, más alta será la puntuación de vulnerabilidad.

**Tabla 6. Autenticación**

| Valor Métrico | Descripción |
|---|---|
| Múltiple (M) | Explotar la vulnerabilidad requiere que el agresor se autentifique dos o más veces, incluso si cada vez se utilizan las mismas credenciales. Por ejemplo, un agresor que se autentifique ante un sistema operativo además de presentar sus credenciales para acceder a una aplicación que aloje dicho sistema. |
| Sencillo (S) | La vulnerabilidad requiere que el agresor se registre en el sistema (por ejemplo, en una línea de instrucción o a través de una sesión o una interfaz web). |
| Ninguno (N) | No se requiere autentificación para explotar la vulnerabilidad. |

De acuerdo a lo anterior, el cálculo total de la "Explotabilidad" se realiza con la siguiente formula:

**Explotabilidad = 20 * Vector_de_acceso * Complejidad_de_acceso * Autenticación**

Dónde:

**Los valores para la variable Vector_de_acceso son:**

a) Local = 0.395
b) Adyacente = 0.646
c) Red = 1

**Los valores para la variable Complejidad_de_acceso son:**

a) Alto: 0.35
b) Medio: 0.61
c) Bajo: 0.71

**Los valores para la variable Autenticación son:**

a) Múltiple: 0.45
b) Simple: 0.56
c) Ninguno: 0.704

### 4.2.2 Métricas de Impacto

- **Impacto sobre la confidencialidad (C)**

Esta métrica mide el impacto sobre la confidencialidad de una vulnerabilidad explotada con éxito. La confidencialidad conlleva limitar el acceso a la información y su divulgación exclusivamente a usuarios autorizados, así como a impedir el acceso o descubrimiento a usuarios no autorizados. La confidencialidad se refiere a limitar el acceso a la información y la divulgación sólo a los usuarios autorizados, así como impedir el acceso o la divulgación a personas no autorizadas. La lista de valores posibles se presenta en la Tabla 9.

**Tabla 7. Impacto de Confidencialidad**

| Valor Métrico | Descripción |
|---|---|
| Ninguno (N) | No hay impacto sobre la confidencialidad del sistema. |
| Parcial (P) | Se produce un descubrimiento considerable de información. Aunque es posible acceder a algunos ficheros del sistema, el agresor no tiene control de lo que consigue o el ámbito de la pérdida está limitado. Un ejemplo de ello es la vulnerabilidad que divulga sólo algunas tablas de una base de datos. |
| Completo (C) | Toda la información queda al descubrimiento, como consecuencia de lo cual todos los ficheros del sistema son revelados. El agresor puede leer todos los datos del sistema (memoria, ficheros, etc.). |

- **Impacto de integridad (I)**

Esta métrica mide el impacto sobre la integridad de una vulnerabilidad explotada con éxito. La integridad hace referencia al grado de confianza y garantía de veracidad de la información. La lista de valores posibles se presenta en la Tabla 10.

**Tabla 8. Impacto de integridad**

| Valor Métrico | Descripción |
|---|---|
| Ninguno (N) | No hay impacto en la integridad del sistema. |
| Parcial (P) | Es posible modificar algunos ficheros o información, pero el agresor no controla lo que ha modificado o el ámbito del ataque es limitado. Por ejemplo, el sistema o los ficheros de una aplicación pueden ser sobrescritos o modificados, pero el agresor no controla los ficheros afectados, o bien, sólo puede modificar ficheros en un contexto o ámbito limitado. |
| Completo (C) | La integridad del sistema está completamente en riesgo. La pérdida de protección del sistema es total. El agresor puede modificar cualquier fichero del sistema objetivo. |

- **Impacto sobre la disponibilidad (A)**

Esta métrica mide el impacto sobre la disponibilidad de una vulnerabilidad explotada con éxito. La disponibilidad hace referencia al acceso a recursos de información. Los ataques que consumen anchura de banda, ciclos de proceso o espacio en el disco, afectan a la disponibilidad de un sistema. La lista de valores posibles se presenta en la Tabla 11. Este valor métrico aumenta con la consecuencia del componente impactado.

**Tabla 9. Impacto de Disponibilidad**

| Valor Métrico | Descripción |
|---|---|
| Ninguno (N) | No hay impacto en la disponibilidad del sistema. |
| Parcial (P) | Se reducen las prestaciones o se producen interrupciones en la disponibilidad del recurso. Un ejemplo de ello es un ataque desde la red por inundación que permita mantener activas un número limitado de conexiones a un servicio de acceso a Internet. |
| Completo (C) | Se produce una caída completa del recurso afectado. El agresor puede hacer que el recurso quede completamente indisponible. |

De acuerdo a lo anterior, el cálculo total del "Impacto" se realiza con la siguiente formula:

**Impacto = 10.41 * (1 - (1 – Imp. Confidencialidad) * (1 – Imp. Integridad) * (1 – Imp. Disponibilidad))**

Dónde**:**

**Los valores para la variable Impacto de confidencialidad son:**

a) Ninguno: 0
b) Parcial: 0.275
c) Completo: 0.660

**Los valores para la variable Impacto de la Integridad**

a) Ninguno: 0
b) Parcial: 0.275
c) Completo: 0.660

**Los valores para la variable Impacto de la Disponibilidad son:**

a) Ninguno: 0
b) Parcial: 0.275
c) Completo: 0.660

De acuerdo a los resultados obtenidos del cálculo de explotabilidad y de impacto detallados anteriormente, se puede obtener el puntaje o valor general del CVSS del BaseScore con la siguiente La fórmula:

**BaseScore = (0.6 * Impacto + 0.4 * Explotabilidad - 1.5) * f (Impacto)**

Donde **f (impacto)** debe reemplazarse por:

- Si el valor de la variable impacto es igual a cero (0) entonces f(impacto) = 0
- Si el valor de la variable impacto es diferente de cero (0) entonces f(impacto) = 1.176

### 4.2.3 Escala de calificación cualitativa

De acuerdo al puntaje o valor del CVSS del BaseScore obtenido, se puede categorizar de manera cualitativa el tipo de vulnerabilidad detectada en términos de factor de riesgo. En este sentido, entre más alto sea el puntaje de CVSS para una vulnerabilidad, mas aumenta el riesgo de que dicha vulnerabilidad se materialice como un riesgo. En la tabla 15 se definen los valores con su respectiva categorización o clasificación del factor de riesgo.

**Tabla 10. Escala de calificación Cualitativa**

| Clasificación | Puntaje CVSS |
|---|---|
| Ninguna | 0.0 |
| Baja | 0.1 – 3.9 |
| Media | 4.0 – 6.9 |
| Alta | 7.0 – 8.9 |
| Critica | 9.0 – 10.0 |

***Nota:*** En la *Tabla 12. Resultados del análisis de Vulnerabilidades en SO y red* de EMCALI, se muestran los resultados del análisis de vulnerabilidades realizado en Emcali, donde el puntaje obtenido se encuentra sombreado del color que representa la clasificación de la vulnerabilidad detectada.

## 4.3 Glosario Técnico de las métricas

- Autoridad: Un contenedor informático que otorga y administra privilegios a los recursos. Ejemplos de autoridades incluyen, una aplicación de base de datos, un sistema operativo y un entorno de entorno limitado.

- Puntuación encadenada: La puntuación de base se obtiene al anotar dos o más vulnerabilidades encadenadas.

- Componente: Se refiere a un componente de software o hardware.

- Componente de software: Un programa o módulo de software que contiene instrucciones de la computadora a ejecutar. Por ejemplo, un sistema operativo, una aplicación de Internet, un controlador de dispositivo.

- Componente impactado: El componente (o componentes) que sufre (s) la consecuencia de la vulnerabilidad explotada. Éstos pueden ser el mismo componente que el componente vulnerable o, si se ha producido un cambio de ámbito, uno diferente.

- Privilegios: Una colección de derechos (normalmente leídos, escritos y ejecutados) otorgados a un usuario o proceso de usuario que define el acceso a los recursos informáticos.

- Recursos: Objeto de software o de red al que se accede, se modifica o se consume por un dispositivo informático. Por ejemplo, archivos de ordenador, memoria, ciclos de CPU o ancho de banda de red.

- Vulnerabilidad: Una debilidad o falla en un componente de software (o hardware).

- Acceso: Capacidad de un sujeto para visualizar, modificar o comunicarse con un objeto. El acceso permite el flujo de información entre el sujeto y el objeto.

- Disponibilidad: Acceso fiable y oportuno en el tiempo a datos y recursos realizado por individuos autorizados.

- Confidencialidad: Principio de seguridad destinado a asegurar que la información no se pone a disposición de sujetos no autorizados.

- Integridad: Principio de seguridad que asegura que la información y los sistemas no son modificados de forma maliciosa o accidental.

- Riesgo: Impacto relativo que tendría la explotación de una vulnerabilidad sobre el entorno de un usuario.

- Amenaza: Probabilidad o frecuencia de ocurrencia de un evento perjudicial.

## 4.4 Resultados de análisis de Vulnerabilidades en SO y red de EMCALI E.I.C.E

Como parte de la experimentación de la metodología, se realizó un análisis de vulnerabilidades en el sistema operativo y la red interna de EMCALI en el área de Gerencia de Tecnología de la Información – GTI; para dicho escaneo se hizo uso de la herramienta libre Nessus. En la tabla 4 se muestra el consolidado de las vulnerabilidades detectadas y las posibles alternativas de solución que podrían ayudar a mitigar que dichas vulnerabilidades se materialicen como riesgos o amenazas:

**Tabla 11. Resultados del análisis de Vulnerabilidades en SO y red de EMCALI**

| Objeto del análisis | Factor de Riesgo (critica, alta, media y baja) | Titulo vulnerabilidad | Descripción de la vulnerabilidad | Alternativa de mitigación. |
|---|---|---|---|---|
| DNS | ALTA | Acceso a Recursos compartidos NFS Remotos | Algunas de las partes NFS exportadas por el servidor remoto podrían ser montadas por el host escaneado. Un atacante podrá explotar este problema para poder leer (posiblemente escribir) el acceso a los archivos en el host remoto.<br>Hay que tener en cuenta que los privilegios de root no eran necesarios montarlos en los recursos compartidos remotos. | Configurar NFS en el host remoto para que solo los hosts autorizados puedan acceder a los recursos compartidos remotos.<br>El NFS remoto debe impedir que las solicitudes puedan acceder al puerto |
| | **Puntaje de Métrica:** CVSS Base Score - 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) | | | |
| | MEDIA | El servidor DNS es vulnerable a los ataques de detección de cache | Es posible que el servidor DNS remoto responda a las consultas de terceros ya que los dominios no tienen el bit de recursividad establecido. Esto puede permitir a un atacante remoto determinar que dominios han sido accedidos recientemente a través de este servidor.<br>Nota: si se trata de un servidor DNS interno no accesible a las redes externas, los ataques se limitarían a la red. Esto puede incluir empleados, consultores y potencialmente a usuarios en una red de invitados o conexión WiFi. | Ponerse en contacto con el proveedor del servicio DNS para minimizar la brecha y encontrar una solución. |
| | **Puntaje de Métrica:** CVSS Base Score - 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **DNS** | MEDIA | Los servicios del servidor no están autenticados a nivel de red | Los servicios del servidor no están configurados para utilizar autenticación de nivel de red (NLA). Esta autenticación utiliza al proveedor de soporte de seguridad de credenciales (CredSSP) para realizar una autenticación en el servidor fuerte TLS / SSL o Kerberos, los cuales son mecanismos que protegen contra ataques main in the middle. Además, esta autenticación también ayuda a proteger el quipo remoto de usuarios malintencionados y software malicioso. | Habilitar la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña configuración “Sistema” en Windows. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) | | | |
| | MEDIA | Se ha firmado un certificado SSL en la cadena de certificados con un algoritmo de Hash débil. | El servicio remoto utiliza una cadena de certificados SSL que se han firmado utilizando un Hash Criptográfico débil (por ejemplo, MD2, Md4, MD5 o SHA1). Estos algoritmos de firma son conocidos por ser vulnerables a la colisión de ataques. Es decir que un atacante podrá explotar esto para generar otro certificado con la misma firma digital, lo que le permite al atacante disfrazarse dentro del servicio afectado.<br>Nota: Tener en cuenta que este complemento informa todas las cadenas de certificados SSL firmados con SHA1 que expiran después del 1 de enero de 2017 como vulnerable. | Ponerse en contacto con la autoridad de certificación para que se vuelva a emitir el certificado. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **DNS** | MEDIA | No se puede confiar en el certificado SSL para este servicio. | ❖ El certificado X.509 del servidor no tiene una firma de una autoridad de certificado público reconocida. Esta situación puede Ocurrir de tres formas diferentes, cada una de las cuales da como resultado una interrupción en la cadena por debajo de la cual no se puede confiar en los certificados.<br>Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de un certificado público conocido autentico. Esto puede ocurrir ya sea cuando la parte superior de la cadena es una parte no reconocida, autenticada o Certificada, o cuando Faltan certificados intermedios que conecten la parte superior de la cadena de certificados a un certificado público conocido autentico.<br>❖ En segundo lugar, la cadena de certificados puede contener un certificado que no es válido en el momento del análisis. Esto puede ocurrir bien sea cuando el escaneo ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado.<br>❖ En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no puede ser verificado.<br>❖ Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e | Comprar o generar un certificado adecuado para este servicio |

| | | | | |
|---|---|---|---|---|
| | | | identidad del servidor web. Esto podría facilitar la realización de "man in the middle" que sería un ataque contra el host remoto. | |
| | **Puntaje de Métrica:** CVSS Base Score - 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | | | |
| **DNS** | MEDIA | El certificado SSL para este servicio es para un Host diferente | El nombre común (CN) del certificado SSL presentado en este servicio es para una maquina diferente | Comprar o generar un certificado adecuado para este servicio |
| | **Puntaje de Métrica:** CVSS Base Score - 5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N) | | | |
| | MEDIA | La cadena de certificados para este servicio (DNS) termina en una línea de autenticación no reconocida por el certificado | La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es el anfitrión público en la producción, esto anula el uso de SSL como cualquier persona podría establecer un main in the middle el cual es un ataque dirigido en contra del host remoto. | Generar un certificado adecuado para este servicio. |
| | **Puntaje de Métrica:** CVSS Base Score - 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | | | |
| | MEDIA | El Host Remoto puede verse afectado por una vulnerabilidad que permite a un atacante remoto descifrar potencialmente TLS capturando trafico | El host remoto admite SSLv2 por lo tanto puede verse afectado por una vulnerabilidad *Bleichenbacher padding oracle ataque conocido como DROWN (Descifrar RSA con eNcryption obsoleto y débil*). Esta vulnerabilidad existe debido a una falla en la implementación de *secure sockets Layer Version* (SSLv2), la cual permite captura de trafico TLS para ser descifrado. | Deshabilite SSLv2 y los conjuntos de cifrado de criptografía de grado de exportación.<br>Asegúrese de que las claves privadas no se utilicen ya que el servidor admite conexiones SSLv2. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **DNS** | MEDIA | Puede ser posible obtener el acceso al host remoto. | La versión remota Desktop Protocol Server (Terminal Service) es vulnerable a un ataque (MiTM). El cliente RDP no está realizando ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.<br>Esta falla existe porque el servidor RDP almacena una RSA en la biblioteca mstlsapi.dll y cualquier usuario con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para ejecutar este ataque. | Se debe forzar el uso de SSL como capa de transporte para este servicio si esta soportado se debe seleccionar "permitir conexiones solo desde equipos que ejecutan escritorio remoto con autenticaciones de nivel de red" si está disponible. |
| | **Puntaje de Métrica:** CVSS Base Score - 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | | | |
| | MEDIA | El Host remoto utiliza débil | El servicio de terminal de servicios remoto no está configurado para utilizar criptografía fuerte.<br>El uso de criptografía débil con este servicio puede permitir que un atacante escuche con más facilidad las comunicaciones y obtener capturas de pantalla y / o pulsaciones de teclas. | Cambiar el nivel de cifrado RDP a nivel alto y cumplir con FIPS. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) | | | |
| | MEDIA | El servicio remoto cifra el trafico utilizando un protocolo con debilidades conocidas | El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y SSL 3.0 estas versiones de SSL son afectadas por varios defectos criptográficos. Un atacante puede explotar estos defectos con un ataque man in the middle con el cual, podrá descifrar las comunicaciones entre el servicio afectado y los clientes. | Verificar la documentación de la aplicación para deshabilitar las conexiones SSL 2.0 y 3.0 y utilizar TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar. |
| | **Puntaje de Métrica:** CVSS Base Score - 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **DNS** | MEDIA | El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios | El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en el administrador de cuentas de seguridad (SAM) y de la autoridad de seguridad local (Domain Policy) (LSAD) debido a un nivel de autenticación incorrecto en la negociación sobre los canales de llamada de procedimiento remoto (RPC). Un atacante puede ser capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM donde pueden explotar esto para forzar autenticación, lo que permite al atacante suplantar a un usuario autenticado y acceder a la base de datos SAM. | Utilizar los parches publicados por Microsoft para Windows vista, 2008, 7,8, 2008 R2, 2012,8.1, RT 8.1, 2012 R2 y 10. |
| | **Puntaje de Métrica:** CVSS Base Score - 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P) | | | |
| | MEDIA | El servidor NFS remoto exporta trabajos compartidos | El servidor NFS remoto está exportando una o más acciones sin restringir el acceso (basado en el nombre del host, IP o IP según su rango) | Asignar las restricciones adecuadas en todos los recursos compartidos de NFS. |
| | **Puntaje de Métrica:** CVSS Base Score - 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | | | |
| | MEDIA | Es posible obtener información confidencial desde el host remoto con SSL/TLS enable. | El host está siendo afectado por un mensaje (MitM) vulnerabilidad de divulgación de información conocida como POODLE. Esta vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes en relleno al descifrar mensajes cifrados mediante el bloque usando cifras en el modo de encadenamiento de bloques de cifrado (CBC). | Deshabilitar SSLv3.<br>Los servicios que deben soportar SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda deshabilitar SSLv3. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **DNS** | BAJA | El servicio remoto admite el uso del certificado RC4 | El host remoto admite el uso de RC4 en una o más suites de cifrado. Este cifrado es defectuoso en su generación de pseudo-aleatorio flujo de bytes en el cual hay variedad de sesgos pequeños introducidos en la corriente, disminuyendo su aleatoriedad. Si el texto plano se cifra repetidamente (por ejemplo, cookies HTTP), el atacante podrá ser capaz de derivar el texto plano siempre y cuando obtenga una gran cantidad de texto cifrado. | Configurar la aplicación afectada, si es posible evitar el uso de cifras RC4. Para este caso sería recomendable usar TLS 1.2 con AESGCM. Estas suites estarían sujetas a soporte para navegador y servidor web. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |
| | BAJA | El servicio remoto admite el uso de 64 bits para bloquear cifras. | El host remoto admite el uso de un cifrado de bloque con 64 bit en una o más suites de cifrado. Por lo tanto, es afectado por una vulnerabilidad conocida como SWEET32, debido al uso cifrado de 64 bits débiles usados para bloquear cifras. Un atacante que tenga los recursos suficientes puede explotar esta vulnerabilidad a través de un ataque de “cumpleaños”, para detectar una colisión que filtra el XOR entre el secreto fijo y un texto claro conocido, permitiendo la divulgación del texto secreto, como por ejemplo la protección de cookies HTTPS, o concluir el secuestro de una sesión autenticada. | Configurar la aplicación o servicio afectado para evitar el uso del bloqueo de los 64 bits. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **OPEN System (Base Datos)** | CRITICA | El servicio rexecd se está ejecutando en el host remoto. | Este servicio está diseñado para permitir a los usuarios de una red ejecutar comandos de forma remota. Sin embargo, rexecd no proporciona buenos medios de autenticación, por lo que puede ser abusado por un atacante para escanear un host de terceros. | Es necesario que comente la línea 'exec' en /etc/inetd.conf y reinicie el proceso inetd. |
| | **Puntaje de Métrica:** CVSS Base Score - 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | | | |
| | CRITICA | El host remoto está ejecutando un producto no compatible que puede verse afectado por varias vulnerabilidades | De acuerdo a su versión, el servidor de IBM Tivoli Storage Manager que se ejecuta en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzara nuevos parches de seguridad para el producto bajo un contrato de soporte estándar. Como resultado, es probable que contenga vulnerabilidades de seguridad | Actualizar a una versión que sea compatible. Además de solicitar soporte por parte del proveedor. |
| | **Puntaje de Métrica: CVSS Base Score - 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)** | | | |
| | CRITICA | El host remoto ejecuta una versión no compatible de un servidor de base de datos. | De acuerdo con su versión, la instalación de Base de Datos de Oracle que se ejecuta en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzara nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. | Es necesario actualizar la versión de la Base de Datos de Oracle que este actualmente disponible. |
| | **Puntaje de Métrica:** CVSS Base Score - 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | | | |

| | | | | |
|---|---|---|---|---|
| | ALTA | Los atacantes remotos pueden evitar la autenticación | Se está ejecutando el banner Open SSH versión 4.7 en el host remoto. Esta versión contiene una vulnerabilidad de derivación de autenticación. En este caso OpenSSH no crea una cookie confiable para un cliente X. debido a esto la partición temporal usara una cookie de confianza. Esto permite a los atacantes violar la política prevista y obtener privilegios haciendo que su cliente X sea tratado como cliente de confianza. | Actualizar la versión de OpenSSH 4.7 a una versión actualizada. |
| | **Puntaje de Métrica:** CVSS Base Score - 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) | | | |
| | MEDIA | El servicio SSH que se está ejecutando en el host remoto tiene una vulnerabilidad de divulgación de información. | Una falla en el diseño de la especificación SSH podría permitir a un atacante recuperar hasta 32 bits de texto plano de un SSH protegido en la configuración estándar, además podría explotar esto para obtener acceso a información confidencial. | Es recomendable actualizar la versión de Open SSH a la versión 5.2 o una versión más avanzada en la cual no se evidencie esta vulnerabilidad. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:P/A:N) | | | |
| | MEDIA | El servicio de SSH se encuentra propenso a una vulnerabilidad de secuestro de sesión X11. | Según el banner con la versión de SSH instalada en el host remoto es una versión inferior a 5.0. Estas versiones pueden permitir a un usuario local secuestrar las sesiones X11, ya que vincula incorrectamente los puertos TCP en la interfaz IPv6 local si se utilizan los puertos correspondientes en la interfaz IPv4. | Es necesario actualizar la versión de OpenSSH a la versión 5.0 o una más avanzada. |
| | **Puntaje de Métrica:** CVSS Base Score - 6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C) | | | |

| | | | | |
|---|---|---|---|---|
| **OPEN( Sistema Base Datos)** | MEDIA | La versión de SHH que se está ejecutando en el host remoto tiene una vulnerabilidad de inyección de comandos. | Según su banner, la versión de OpenSSH que se está ejecutando en el host remoto esta potencialmente afectada por una vulnerabilidad de ejecución de comandos arbitraria. La utilidad scp no desinfectara adecuadamente la entrada de los usuarios antes de hacer el llamado de la función system (). Un atacante local podría explotar esto creando nombres de archivo con metacaracteres de Shell, lo que podría causar que se ejecute código arbitrario si es copiado por un usuario que ejecute scp. | Es recomendable actualizar la versión a una versión posterior a la 4.3. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P) | | | |
| | MEDIA | El servicio remoto SSH se ve afectado por una vulnerabilidad de bypass de seguridad. | Según este banner, la versión de OpenSSH instalada en el host remoto es inferior a la versión 4.9. Puede permitir que un usuario remoto autenticado eluda el 'sshd_config' 'ForceCommand' modificando el archivo de sesión ssh / rc'. | Es recomendable actualizar la versión de OpenSSH 4.9 a una posterior. |
| | **Puntaje de Métrica:** CVSS Base Score - 6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P) | | | |
| | MEDIA | El servidor SSH remoto se encuentra configurado para permitir algoritmos de encriptación débiles o ningún algoritmo en absoluto. | Nessus ha detectado que el servidor SSH está configurado para utilizar el cifrado de flujo de RC4 o ningún cifrado en absoluto. RFC 4253 recomienda no usar RC4 debido a un problema con las teclas débiles. | Contactar al proveedor del servicio y consulte la documentación del producto para eliminar cifrados débiles. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) | | | |
| **OPEN System (Base Datos)** | MEDIA | el servicio remoto ofrece un protocolo criptográfico inseguro | El dominio SSH remoto admite conexiones realizadas con la versión 1.33 y / o 1.5 del protocolo SSH. Estos protocolos no son completamente criptográficamente seguros por lo que no deben ser utilizados. | Deshabilitar la compatibilidad con la primera versión del protocolo |
| | **Puntaje de Métrica:** CVSS Base Score - 4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| | BAJA | El servicio SSH puede verse afectado por una vulnerabilidad de secuestro de Puerto de reenvío X11. | Según su banner, la versión de SSH instalada en el host remoto es anterior a 5.1 y puede permitir que un usuario local secuestre el puerto de reenvío X11. La aplicación establece incorrectamente la opción de socket 'SO_REUSEADDR' cuando la opción de configuración 'X11UseLocalhost' esta deshabilitada.<br>Tenga en cuenta que la mayoría de los sistemas operativos, al intentar vincular a un puerto que ha sido previamente vinculado con la opción 'SO_REUSEADDR', comprobara que el ID de usuario efectivo coincide con el enlace anterior (sistemas comunes BSDderived) o que las direcciones de enlace no se superponen (Linux y Solaris). Esto no es el caso con otros sistemas operativos como HP-UX. | Es necesario actualizar la versión de OpenSSH a una posterior a la versión 5.1. |
| | **Puntaje de Métrica:** CVSS Base Score - 1.2 (CVSS2#AV:L/AC:H/Au:N/C:P/I:N/A:N) | | | |
| **OPEN System (Base Datos)** | BAJA | El servicio SSH remoto tiene múltiples vulnerabilidades | El reenvió de X11 se puede habilitar involuntariamente cuando se realizan varias solicitudes de reenvío en la misma sesión o cuando un oyente X11 queda huérfano después de que una sesión se va. (CVE20052797). Intentar iniciar sesión como un usuario inexistente hace que el proceso de autenticación se bloquee, lo que podría explotarse para enumerar cuentas de usuario válidas. | Actualizar a OpenSSH 4.2 o una versión posterior. Para OpenSSH en Mac OS X 10.4.x, aplique actualización de seguridad de Mac OS X 2006004 |
| | **Puntaje de Métrica:**CVSS Base Score - 3.5 (CVSS2#AV:N/AC:M/Au:S/C:P/I:N/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| **OPEN System (Base Datos)** | BAJA | Los ataques locales pueden tener acceso a información confidencial | Según su banner, la versión de OpenSSH que se ejecuta en el host remoto en anterior que 5.8p2. Estas versiones pueden verse afectadas por una vulnerabilidad de divulgación de información local que podría permitir que el contenido de la clave privada del host sea accesible rastreando localmente la ejecución de la utilidad SSH clave. Tener la clave privada del host puede permitir la suplantación del host. Tenga en cuenta que las instalaciones solo son vulnerables si ssh rand helper se habilito durante el proceso de compilación, lo que no es el caso de * BSD, OS X, Cygwin y Linux. | Actualizar la versión portable de OpenSSH 5.8p2 a una versión posterior. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N) | | | |
| | BAJA | El servidor SSH remoto está siendo afectado por una vulnerabilidad de divulgación de información. | Según su banner, el host remoto está ejecutando una versión de OpenSSH antes de 4.0. Las versiones de Open SSH anteriores a 4.0 se ven afectadas por una vulnerabilidad de divulgación de información porque la aplicación almacena nombre de host, direcciones IP y claves en texto sin formato en el archivo 'known_hosts'. Un atacante local, explotando esta falla, podría tener acceso a información confidencial que podría ser utilizada en ataques posteriores. | Es recomendable actualizar a OpenSSH 4.0 o una versión posterior. |
| | **Puntaje de Métrica:** CVSS Base Score - 1.2 (CVSS2#AV:L/AC:H/Au:N/C:P/I:N/A:N) | | | |
| **OPEN System (Base Datos)** | BAJA | El servidor SSH está configurado para utilizar Cipher Block Chaining. | El servidor SSH está configurado para admitir cifrado Cipher Block Chaining (CBC). Esto puede permitir a un atacante recuperar el mensaje de texto plano de texto cifrado. | Póngase en contacto con el proveedor o consulte la documentación del producto para desactivar el modo CBC cifrado y habilitar el cifrado CTR o GCM. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| | BAJA | El servidor SSH remoto está configurado para permitir algoritmos MD5 y 96 bit MAC. | El servidor SSH remoto está configurado para permitir algoritmos MAC MD5 o 96bit, ambos considerados débiles.<br>Tenga en cuenta que este complemento solo comprueba las opciones del servidor SSH y no comprueba las versiones de software vulnerables. | Contactar con el proveedor o consultar la documentación del producto para desactivar los algoritmos MD5 y 96bit MAC. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |
| **Red Informática de la Empresa (Intranet)** | MEDIA | La firma no es necesaria en el Servidor SMB remoto. | Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques main in the middle contra el servidor SMB. | Imponga la firma de mensajes en la configuración del host. En Windows, se encuentra en la configuración de directiva 'Servidor de red de Microsoft: Firma digital de comunicaciones (siempre)'. En samba, la configuración se denomina "firma de servidor". |
| | **Puntaje de Métrica:** CVSS Base Score - 5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N) | | | |
| **Red Informática de la Empresa (Intranet)** | MEDIA | Se ha firmado un certificado SSL en la cadena de certificados con un algoritmo de hash débil. | El servicio remoto no utiliza una cadena de certificados SSl que se ha firmado utilizando un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se enmascare como el servicio afectado.<br>Se debe de tener en cuenta que este complemento informa todas las cadenas de certificados SSL firmadas con SHA1 que caducan después del 1 de enero de 2017 como vulnerables. | Ponerse en contacto con la autoridad de certificación para que se vuelva a emitir el certificado. |
| | **Puntaje de Métrica:** CVSS Base Score - 4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N) | | | |

| | | | | |
|---|---|---|---|---|
| | MEDIA | La cadena de certificación SSL para este servicio termina en un certificado autenticado no reconocido. | La cadena de certificado X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque main in the middle contra el host remoto.<br>Hay que tener en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no es autenticado, pero que está firmado por una autoridad de certificación no reconocida. | Es necesario comprar o generar un certificado adecuado para este servicio. |
| | **Puntaje de Métrica:** CVSS Base Score - 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | | | |
| **Red Informática de la Empresa (Intranet)** | MEDIA | No se puede confiar en el certificado SSL para este servicio | El certificado X.509 del servidor no tiene una firma de una autoridad de certificado público conocida. Esta situación puede ocurrir de tres maneras diferentes, cada una de las cuales da lugar a una interrupción en la cadena por debajo de la cual no se puede confiar en los certificados.<br>En primer lugar, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida.<br>Esto puede ocurrir cuando la parte superior de la cadena es un certificado no autenticado, o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados a una autoridad de certificación publica conocida.<br>En segundo lugar, la cadena de certificados puede contener un certificado que no es válido en el momento del análisis. Esto | Comprar o generar un certificado adecuado para este servicio. |

| | | | | |
|---|---|---|---|---|
| | | | puede ocurrir cuando el análisis se produce antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado.<br>En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo verificarse. Las firmas malas pueden ser fijadas consiguiendo el certificado con la mala firma para ser renunciado por su emisor. Las firmas que no pudieron verificarse son el resultado del emisor del certificado que utiliza un algoritmo de firma que Nessus no admite o no reconoce.<br>Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques main in the middle contra el host remoto. | |
| | **Puntaje de Métrica:** CVSS Base Score - 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | | | |
| | MEDIA | Los servicios de terminal server remotos no utilizan autenticación de nivel de red solamente. | Los servicios de terminal server remotos no están configurados para utilizar autenticación de Nivel de Red (NLA) solamente.<br>NLA utiliza el protocolo CredSSP (Credential Security Provier) para realizar autenticación de servidor fuerte a través de TLS/ SSL o mecanismos Kerberos, que protegen contra ataques de main in the middle.<br>Además de mejorar la autenticación, NLA también ayuda a proteger el equipo remoto de usuarios malintencionados y software completando la autenticación del usuario | Habilite autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña 'Remoto' de la configuración 'System' de Windows. |

| | | | | |
|---|---|---|---|---|
| | | | antes de que se establezca una conexión RDP completa | |
| | **Puntaje de Métrica:** CVSS Base Score - 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) | | | |
| | MEDIA | El host remoto utiliza criptografía débil. | El servicio de terminal remoto no está configurado para utilizar criptografía fuerte.<br>El uso de criptografía débil con este servicio puede permitir que un atacante espíe comunicaciones más fácilmente y obtener capturas de pantalla y/ o pulsaciones de teclas. | Cambiar el nivel de cifrado RDP a uno de los siguientes:<br>3. Alta<br>4. Cumple con FIPS |
| | **Puntaje de Métrica:** CVSS Base Score - 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N) | | | |
| **Red Informática de la Empresa (Intranet)** | MEDIA | Puede ser posible obtener acceso al host remoto. | La versión remota del servidor de protocolo de escritorio remoto (Terminal Service) es vulnerable a un ataque de main in the middle (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer cifrado con el cliente y el servidor sin ser detectado. Un atacante MiTM de esta naturaleza permitiría al atacante obtener cualquier información confidencial transmitida, incluyendo credenciales de autenticación.<br>Este defecto existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier usuario local con acceso a este archivo (en cualquier sistema Windows) puede utilizar la clave y utilizarla para este ataque. | Forzar el uso SSL como capa de transporte para este servicio si esta soportado<br>Seleccione la opción “Permitir conexiones solo de equipos que ejecutan escritorio remoto con autenticación de nivel de red si está disponible |
| | **Puntaje de Métrica:** CVSS Base Score - 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | | | |
| | BAJA | El servicio remoto admite el uso del cifrado RC$ | El host remoto admite el uso de RC4 en una o más suites de cifrado. El cifrado RC4 es defectuoso en su generación de una | Reconfigurar la aplicación afectada, si es posible, para evitar el uso de cifras RC4. |

| | | | | |
|---|---|---|---|---|
| | | | corriente pseudo-aleatoria de bytes de modo que presenta una amplia variedad de sesgos pequeños se introducen en la corriente, disminuyendo su aleatoriedad | Considere la posibilidad de usar TLS 1.2 con suites AESGCM sujetas a soporte de navegador y servidor web. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |
| **Red Informática de la Empresa (Intranet)** | BAJA | El servicio remoto admite el uso de cifrados de bloques de 64 bits. | El host remoto admite el uso de un cifrado de bloque de 64 bits en una o más suites de cifrado. Es, por lo tanto, afectado por una vulnerabilidad, conocida como SWEET32, debido al uso de débiles cifrado de bloques de 64 bits.<br>Un atacante main in the middle que tiene recursos suficientes y puede explotar esta vulnerabilidad, a través de un ataque de "cumpleaños", para detectar una colisison que filtra el XOR entre el secreto fijo y un texto claro conocido, permitiendo la divulgación del texto secreto, como las cookies HTTPS seguras, y posiblemente resultando en el secuestro de una sesión autenticada.<br>Prueba de los conceptos han demostrado que los atacantes pueden recuperar las cookies de la autenticación de una sesión HTTPS en tan solo 30 horas. | Configure la aplicación afectada, si es posible, para evitar el uso de todos los 64 bits bloquear cifras. |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |
| | BAJA | El host remoto no es compatible con FIPS140. | La configuración de cifrado utilizada por el servicio de Terminal Server remoto no es compatible con FIPS140. | Cambiar el nivel de cifrado RDP a: 4. Cumple con FIPS |
| | **Puntaje de Métrica:** CVSS Base Score - 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | | | |

De los resultados detallados en la anterior tabla, se puede concluir que:

- La configuración del servidor DNS deberá ser evaluada por la organización dado que terceros no autenticados ni autorizados pueden realizar consultas o peticiones al mismo sin previa validación de identificación de usuario.
- Falta autenticar los servicios del servidor a nivel de red.
- Existen métodos de cifrado de información débiles o no apropiados lo que puede generar que personas o factores externos accedan a dichos datos sin la debida autorización.
- Aunque Emcali ha instaurado políticas en el aseguramiento de la información, el resultado del análisis refleja que aún existen brechas de seguridad específicamente en la red interna y sistema operativo. Para ser más precisos, hace falta reforzar principalmente aspectos como la autenticación de usuarios, la actualización de versiones de la base de datos por obsolencia y acceso remoto a algunos servicios de terceros no autorizados.
- Existen perfiles administradores y servicios compartidos en host remotos, lo que los hace accesibles por cualquier persona no identificada
- Como buena práctica, la organización deberá realizar auditorías internas periódicas (se recomienda dos al año como mínimo) con el fin de detectar brechas en seguridad de la información y aún más teniendo en cuenta que en la actualidad Emcali realiza auditorías a nivel de Gestión de calidad mas no en términos de seguridad de la información.

La tabla de resultados anterior permite también concluir que a nivel de sistema operativo y red interna de una organización pueden presentarse un sin número de vulnerabilidades que pueden dar origen a amenazas y riesgos que fácilmente pueden materializarse por aspectos tan aparentemente simples como lo es la actualización de versión de una base de datos o de un parche en el sistema operativo. Es precisamente estos dos factores en los cuales se centra la metodología propuesta en este trabajo dado que la red interna y el sistema operativo pueden entenderse como el corazón y las arterias que sostienen todo el sistema de la organización y en este contexto, sería el sistema que contiene, maneja y almacena toda la información de la empresa.

Otras metodologías como la propuesta por Garzón, Ratkovich y Vergara (2005) y la Norma ISO 27001 dan pautas generales para realizar análisis de vulnerabilidades y en términos globales, sugieren cómo implementar un sistema de gestión de la seguridad de la información al interior de una empresa. Sin embargo, una de las preguntas que toda

organización debe hacerse al momento de decidir incursionar en el tema de la seguridad de la información es, ¿Cómo lo hago?, ¿Por dónde empiezo? Y precisamente estos cuestionamientos cobran más importancia cuando la empresa apenas está iniciando su labor y se está desarrollando. Es en estos interrogantes que la metodología propuesta en este trabajo se basa, en enfocarse como primera medida en dos aspectos tecnológicos de suma importancia como lo son el sistema operativo y la red interna de la organización sin subestimar o dejar por fuera otros elementos importantes que deben incluirse dentro del aseguramiento de la información. En este sentido, la metodología propuesta brinda una pauta para las pequeñas y medianas empresas de cómo empezar y donde empezar a trabajar, en este caso: En el análisis de vulnerabilidades de dos elementos que son la red interna de la empresa y el sistema operativo.

En contraste con los resultados obtenidos en este análisis, encontramos por ejemplo que en la metodología propuesta por Garzón, Ratkovich y Vergara (2005) los resultados del análisis varían dependiendo de las herramientas usadas, los dispositivos y los sistemas operativos y para este último caso, se detectó que haciendo uso de Firewalls los diferentes tipos de ataques son significativamente más efectivos en Windows que en Linux. Los resultados obtenidos por la metodología de Garzón, Ratkovich y Vergara fueron consecuencia de pruebas de explotación en ambientes controlados, simulando acciones maliciosas mientras que en la metodología propuesta en este trabajo no se realizó simulación de ataques sino que se ejecutó un escaneo de vulnerabilidades en el sistema operativo y red interna sin riesgo de afectación alguna de la información analizada, lo que representa un buen primer paso en la detección de brechas de seguridad y lo que puede dar un parte de tranquilidad a la gerencia de la organización al no poner en riesgo los datos a analizar . Ya después de que la empresa vaya madurando y desarrollando su sistema de gestión de seguridad de la información, podrá ir profundizando en los análisis de vulnerabilidades haciendo uso de ataques simulados en ambientes controlados.

Adicional, se puede deducir que aunque el análisis que se realizó en el presente trabajo se enfocó en dos elementos principalmente (sistema operativo y red interna), dichos elementos pueden verse aparentemente como muy básicos o sencillos, sin embargo, la verdad es que en términos de vulnerabilidades hay mucho qué analizar y qué revisar, y por supuesto, hay varias brechas que necesitan ser cerradas o reducidas al mínimo en tanto sea posible.

# CONCLUSIONES

Al plantear la metodología propuesta fue indispensable identificar los procesos de negocio de la empresa EMCALI E.I.C.E, entender su modelo organizacional, determinar la clasificación de activos de información, identificar las vulnerabilidades y sus posibles acciones de mitigaciones lo que también facilitará el desarrollo de un sistema de gestión de seguridad de la información en la empresa que ira madurado y creciendo con el tiempo y la experiencia.

La presente metodología basada en la metodología propuesta por Garzón, Ratkovich y Vergara (2005) y la Norma ISO 27001 y su guía de buenas prácticas, permitirán a la empresa EMCALI E.I.C.E tener un punto de partida para la detección e identificación de posibles brechas en los sistemas de información y en consecuencia la toma de decisiones en relación con el aseguramiento de los datos que se manejan al interior de la organización. Por otro lado, esta metodología permitirá a organizaciones de pequeña y mediana escala implementar planes de seguridad que se adapten a sus condiciones, necesidades y capital, buscando minimizar en tanto sea posible los riesgos que puedan afectar su activo más valioso: La información. Aunque el factor monetario es muchas veces uno de los elementos más preocupantes para las organizaciones a la hora de querer asegurar la información de una empresa, claramente no debe verse como un impedimento para dar los primeros pasos en el contexto de la seguridad de la información. Por lo anterior, esta metodología representa una oportunidad para ir avanzando e incursionando, a un bajo costo, en el tema del aseguramiento de la información y a nivel general en el desarrollo de un plan de seguridad que cobije todas as áreas de la organización, teniendo en cuenta que este proceso no se logra de la noche a la mañana, sino que es un proceso que se ira dando paso a paso y de manera iterativa.

Finalmente, el análisis de vulnerabilidades permitirá al área de Gerencia de Tecnología de la Información (GTI) conocer el estado general de los mecanismos para salvaguardar la información, plantear estrategias de mejora de los mismos, validar medidas de seguridad aplicadas y resultados obtenidos, valorar y fortalecer las medidas de seguridad para los activos de posibles riesgos y vulnerabilidades identificadas permitiendo la toma de decisiones en la mejora continua de la organización.

# REFERENCIAS

[1]. Mifsud, Elvira. (2012). Observatorio tecnológico. Ministerio de educación, cultura y deporte. Gobierno de España. MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. Recuperado de: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

[2] Kaspersky Lab. (2013). Exploits y vulnerabilidades en sistemas operativos. Recuperado de: http://www.kaspersky.es/internet-security-center/threats/malware-system-vulnerability

[3] Ministerio de Tecnologías de Información y las Comunicaciones de Colombia. Guía Técnica. Seguridad y Privacidad de la Información. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

[4] Ríos, Javier. (2014). Técnicas y herramientas de análisis de vulnerabilidades de una red. Tesis de Pregrado. Escuela Técnica Superior De Ingeniería Y Sistemas De Telecomunicación. Madrid. Recuperado de: http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf

[5] Caire, Ramiro. 2014. Seguridad y ética. Herramientas de Vulnerability Assessment y Gestión de Incidencias. Recuperado de: https://seguridadetica.wordpress.com/

[6] Morales, Madelayne. 2016. FCAPS Caso aplicado: EMCALI. Proyecto de Curso - Sistemas Gerenciales de Ingeniería. Pontificia Universidad Javeriana. Cali.

[7] Garzón, Ratkovich, Vergara. (2005). Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. Artículo en Línea. Recuperado de: https://repository.javeriana.edu.co/bitstream/handle/10554/7467/tesis181.pdf?sequence=1&isAllowed=y

[8] Barón, Carlos. (2010). Metodología De Análisis De Vulnerabilidades Para La Red De Datos En La Dirección De Telemática De La Policía Nacional. Libro final de Pasantía. Universidad Militar Nueva Granada. Recuperado de: http://repository.unimilitar.edu.co/bitstream/10654/502/1/BaronDuquezCarlos2010.pdf

[9] Sosa, Johana. (2012). Clasificación de la Información - Tipos de Clasificación. Documento en Línea. Pontificia Universidad Javeriana. Bogotá, Colombia. Recuperado de: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Clasificacion_de_la_Informacion.pdf

[10] Burgos, Jorge. Campos, Pedro. (2008). Modelo Para Seguridad de la Información en TIC. Artículo en Línea. Universidad del Bio-Bio. Chile. Recuperado de: http://ceur-ws.org/Vol-488/paper13.pdf

[11] Unión Internacional de Telecomunicaciones. (2011). Sistema común de puntuación de vulnerabilidades. Documento en Línea. Recuperado de: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiJ_tu4ysTRAhUFPiYKHRzoD_MQFggeMAE&url=https%3A%2F%2Fwww.itu.int%2Frec%2Fdologin_pub.asp%3Flang%3De%26id%3DT-REC-X.1521-201104-S!!PDF-S%26type%3Ditems&usg=AFQjCNF9B1uR2tLCwJhc0wYw-yiw6Yhslw&sig2=tmFRnB8i9pH2eiFXZhCerA

# ANEXOS

**Anexo 1. Controles y objetivos de control para EMCALI E.I.C.E**

| Sección | Subsección | Objetivo | Control | Aplica | Justificación |
|---|---|---|---|---|---|
| **A.5 POLÍTICA DE SEGURIDAD** | A.5.1 Política de seguridad de la información | Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. | A.5.1 Documento de la política de seguridad de la información. | SI | La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes. |
| **A.6 Organización De La Seguridad De La Información** | A.6.1 Política de Organización Interna | Proporcionar interacción entre la dirección general de la empresa y el departamento de informática de la empresa para la toma de decisiones y conocimiento de responsabilidades de la seguridad de la información. | 6.1.1 Documento donde se especifique detalladamente los procedimientos y la toma de decisiones para el mejoramiento de estructuración de la arquitectura de la seguridad de la información dentro de la empresa. | SI | Este objetivo de control propone que la dirección general de la empresa apoye activamente la seguridad dentro de la Empresa con compromiso demostrado en las responsabilidades de la seguridad de la información. |
| | | | 6.1.5 Acuerdos de confidencialidad | SI | Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización para la protección de la información. |

| | | | | | |
|---|---|---|---|---|---|
| | | | A.6.1.6 Contacto con grupos de interés especiales. | SI | Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información y asociaciones de profesionales. |
| | A.6.2 Política de Partes Externas | Mantener la seguridad dela información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por estas. | A.6.2.1 Identificación de los riesgos relacionados con las partes. | SI | Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso. |
| | | | A.6.2.3 Consideraciones de la Seguridad en los Acuerdos con Terceras Partes. | SI | Los acuerdos con terceras partes que implicaban acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adicción de productos o servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad. |

| | | | | | |
|---|---|---|---|---|---|
| **A.7 Gestión de Activos** | A.7.1 Responsabilidad de los activos | Lograr y mantener la protección adecuada de los activos organizacionales | A.7.1.1 Inventario de Activos | SI | Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes. |
| | A.7.2 Clasificación de la Información | | A.7.2.1 Directivas de Clasificación | SI | La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización. |
| | | | A.7.2.2 Etiquetado y Manejo de Información | SI | Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización. |
| **A.8 Seguridad de los Recursos Humanos** | A.8.1 Antes de la Contratación Laboral<br>A.8.2 Durante la Vigencia de la Contratación Laboral | Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones<br>Asegurar que todos los empleados, | A.8.1.1 Roles y Responsabilidades | SI | Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización. |
| | | | A.8.1.2 Selección | SI | Se deben realizar para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y |

| | | | | | |
|---|---|---|---|---|---|
| | | contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al Igual que reducir el riesgo de error humano. | | | las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. |
| | | | A.8.1.3 Términos y Condiciones Laborales | SI | Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información. |
| | | | A.8.2.1 Responsabilidades de la Dirección | SI | La dirección debe exigir que los empleados, contratistas y usuario de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización. |
| | | | A.8.2.2 Educación, Formación y concientización sobre la Seguridad de la Información | SI | Todos los empleados de la organización y cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | sus funciones laborales. |
| | | | Proceso Disciplinario | SI | Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad. |
| | A.8.3 Terminación o Cambio del Contrato Laboral | Asegurar que los empleados, contratistas y usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada | 8.3.1 Responsabilidades en la terminación | SI | Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral. |
| | | | 8.3.2 Devolución de Activos | SI | Todos los empleados, contratistas o usuarios de terceros partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo. |
| | | | 8.3.3 Retiro de los derechos de Acceso | SI | Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se dejen ajustar después del cambio. |
| **A.9 Seguridad Física y del Entorno** | A.9.1 Áreas Seguras | Evitar el acceso físico no autorizado, el daño e | A.9.1.1 Perímetro de Seguridad Física | SI | Se deben utilizar perímetros de seguridad (barreras tales como paredes, |

| | | | | | |
|---|---|---|---|---|---|
| | | interferencia a las instalaciones y a la información de la organización. | | | puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información. |
| | | | A.9.1.2 Controles de Acceso Físico | SI | Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. |
| | | | A.9.1.4 Protección contra amenazas externas y ambientales | SI | Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial. |
| | A.9.2 Seguridad Física y Entorno | Evitar perdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización. | A.9.2.1 Ubicación y Protección de los equipos. | SI | Los equipos deben estar ubicados o protegidos para reducir el riego debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado. |
| | | | A.9.2.2 Servicios de Suministro | SI | Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. |
| | | | A.9.2.3 Seguridad del Cableado | SI | El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | servicios de información debe estar protegidos contra interceptaciones o daños. |
| | | | A.9.2.4 Mantenimiento de los Equipos | SI | Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. |
| | | | A.9.2.5 Seguridad de los equipos fuera de las Instalaciones. | SI | Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. |
| | | | A.9.2.6 Seguridad en la Reutilización o Eliminación de los Equipos | SI | Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación. |
| | | | A.9.2.7 Retiro de Activos. | SI | Ningún equipo, información ni software se deben retirar sin autorización previa. |
| **A.10 Gestión de Comunicaciones y operaciones** | A.10.1 Procedimientos Operacionales y Responsabilidades | Asegurar la operación correcta y segura de los servicios de procesamiento de información. | A.10.1.4 Separación de las Instalaciones de Desarrollo, Ensayo y Operación | SI | Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo. |

| | | | | | |
|---|---|---|---|---|---|
| | A.10.2 Gestión de la Prestación del Servicio por Terceras Partes | Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos prestación del servicio por terceras partes | A.10.2.1 Prestación del Servicio | SI | Se deben garantizar que los controles de seguridad, las definiciones del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes. |
| | | | A.10.2.2 Monitoreo y revisión de los servicios por terceras partes | SI | Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares. |
| | A.10.3 Planificación y aceptación del sistema | Minimizar el riesgo de fallas de los sistemas. | A.10.3.2 Aceptación del Sistema | SI | Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación. |
| | A.10 Gestión de Comunicaciones y Operaciones | Proteger la integridad del software y de la información. | Controles contra códigos maliciosos. | SI | Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos malicioso, así como procedimientos apropiados de concientización de los usuarios. |
| | A.10.5 Respaldo | Mantener la integridad y disponibilidad de la información y delo los servicios de procesamiento de información. | Respaldo de la Información | SI | Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada. |
| | A.10.6 Gestión de la seguridad | Asegurar la protección de la | A.10.6.1 controles de la | SI | Las redes se deben mantener y controlar |

| | | | | | |
|---|---|---|---|---|---|
| | de las redes | información en las redes y la protección de la infraestructura de soporte. | seguridad de las redes. | | adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito. |
| | | | A.10.6.2 Seguridad de los Servicios de la Red | SI | En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente. |
| | A.10.7 Manejo de los Medios | Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. | A.10.7.3 Procedimientos para el manejo de la información | si | Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no Autorizada o uso inadecuado. |
| | A.10.8 Intercambio de la Información | mantener la seguridad de la información y del software que se intercambian Dentro de la organización y con cualquier entidad externa. | A,10.8.1 Políticas y procedimientos para el intercambio de información | Si | Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de Servicios de comunicación. |
| | | | A.10.8.4 Mensajería Electrónica | SI | La información contenida en la mensajería electrónica debe tener la protección adecuada |
| | A.10.9 | Garantizar la | A.10.9.1 | SI | La información |

| | | | | | |
|---|---|---|---|---|---|
| | Servicios de Comercio Electrónico | seguridad de los servicios de comercio electrónico, y su utilización segura. | Comercio Electrónico | | involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no Autorizada. |
| | | | A.10.9.2Transacciones en Línea | SI | La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión Incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje. |
| | | | A.10.9.3 Información disponible al público | SI | La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no Autorizada. |
| | A.10.10 Monitoreo | Detectar actividades de procesamiento de la información no autorizadas. | Registro de auditorías | SI | Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Monitoreo del uso del sistema | SI | Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad |
| | | | Protección de la información del registro | SI | Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados. |
| | | | Registros del administrador y del operador | SI | Se deben registrar las actividades tanto del operador como del administrador del sistema. |
| | | | Registro de fallas | SI | Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas. |
| **A.11 Control de Acceso** | A.11.2 Gestión de acceso a usuarios | Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información. | A.11.2.1 Registro de usuarios. | SI | Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. |
| | | | A.11.2.2 Gestión de privilegios. | SI | Se debe restringir y controlar la asignación y uso de privilegios. |
| | | | A.11.2.3 Gestión de contraseñas para usuarios. | SI | La asignación de contraseñas se debe controlar a través de un proceso formal de gestión. |
| | A.11.3 Responsabilidad de los usuarios | Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información. | A.11.3.1 Uso de Contraseñas | SI | Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas. |
| | | | A.11.3.2 Uso de Usuario | SI | Los usuarios deben asegurarse de que a |

| | | | | | |
|---|---|---|---|---|---|
| | | | Desatendido | | los equipos desatendidos se les da protección apropiada. |
| | A.11.4 Control de Accesos a las Redes | Evitar el acceso no autorizado a servicios en red. | A.11.4.1 Política de uso de los servicios de red. | SI | Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados. |
| | | | A.11.4.2 Autenticación de usuarios para conexiones externas. | SI | Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos. |
| | | | A.11.4.3 Identificación de los equipos en las redes. | SI | La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas. |
| | | | A.11.4.6 Control de conexión a las redes. | SI | Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio (véase el numeral 11.1). |
| | | | A.11.4.7 Control de enrutamiento en la red. | SI | Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio. |

| | | | | | |
|---|---|---|---|---|---|
| | A.11.5 Control de Acceso al Sistema Operativo | Evitar el acceso no autorizado a los sistemas operativos. | A.11.5.1 Procedimientos de ingreso seguros | SI | El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro. |
| | | | A.11.5.2 Identificación y autenticación de usuarios. | SI | Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario. |
| | | | A.11.5.3 Sistema de gestión de Contraseñas. | SI | Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las Contraseñas. |
| | | | A.11.5.4 Uso de las utilidades del sistema | SI | Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación. |
| | A.11.7 Computación móvil y trabajo remoto | Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto. | A.11.7.1 Computación y comunicaciones móviles. | SI | Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles. |
| | | | A.11.7.2 Trabajo remoto. | SI | Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto. |
| **A.12 Adquisición, desarrollo y mantenimiento de sistemas de información** | A.12.3 Controles criptográficos | Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos. | A.12.3.1Política sobre el uso de controles criptográficos. | SI | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. |
| | A.12.4 Seguridad de los Archivos del | Garantizar la seguridad de los archivos del | A.12.4.1 Control del software operativo. | SI | Se deben implementar procedimientos para controlar la instalación de |

| | | | | | |
|---|---|---|---|---|---|
| | Sistema | sistema. | | | software en sistemas operativos. |
| | | | A.12.4.2 Protección de los datos de prueba del sistema. | SI | Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse |
| | A.12.5 Seguridad en los procesos de desarrollo y soporte | Mantener la seguridad del software y de la información del sistema de aplicaciones. | A.12.5.5 Desarrollo de software contratado externamente | SI | La organización debe supervisar y monitorear el desarrollo de software contratado externamente. |
| | A.12.6 Gestión de la vulnerabilidad técnica | Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas. | A.12.6.1 Control de vulnerabilidades técnicas | SI | Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados. |
| **A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** | A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio | Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna. | A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información | SI | Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio. |
| **A.15 CUMPLIMIENTO** | A.15.1 Cumplimiento de los requisitos legales | Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad. | A.15.1.4 Protección de los datos y privacidad de la información personal. | SI | Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato. |
| | A.15.2 Cumplimiento de las políticas y las | Asegurar que los sistemas cumplen con las normas y políticas de | A.15.2.2 Verificación del cumplimiento | SI | Los sistemas de información se deben verificar periódicamente para determinar el |

| | | | | | |
|---|---|---|---|---|---|
| | normas de seguridad y cumplimiento técnico | seguridad de la organización. | técnico. | | cumplimiento con las normas de implementación de la seguridad. |
| | A.15.3 Consideraciones de la auditoría de los sistemas de información | Maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia. | A.15.3.1 Controles de auditoría de los sistemas de información. | SI | Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio. |
| | | | A.15.3.2 Protección de las herramientas de auditoría de los sistemas de información. | SI | Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro. |