Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO27000/IEC, O-ISM3 Y COBIT, APLICADAS A UNA RED DE ÁREA LOCAL

Carla Lucrecia Jiguan Aguilón
Asesorada por el Ing. Herman Igor Véliz Linares

Guatemala, octubre de 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO27000/IEC, O-ISM3 Y COBIT, APLICADAS A UNA RED DE ÁREA LOCAL

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CARLA LUCRECIA JIGUAN AGUILÓN
ASESORADA POR EL ING. HERMAN IGOR VÉLIZ LINARES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO a.i.	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Ing. Kevin Vladimir Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. César Augusto Fernández Cáceres
EXAMINADOR	Ing. Luis Fernando Espino Barrios
EXAMINADOR	Ing. Sergio Arnaldo Méndez Aguilar
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO27000/IEC, O-ISM3 Y COBIT, APLICADAS A UNA RED DE ÁREA LOCAL

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 15 de marzo de 2023.

Carla Lucrecia Jiguan Aguilón

Guatemala, 22 de septiembre de 2023

Ingeniero
Carlos Alfredo Azurdia
Coordinador de Privados y Trabajos de Tesis
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería - USAC

Respetable Ingeniero Azurdia:

Por este medio hago de su conocimiento que en mi rol de asesor del trabajo de investigación realizado por el estudiante **CARLA LUCRECIA JIGUAN AGUILÓN** con carné **200515929 y CUI 1603 77102 0101** titulado **"DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO2700/IEC, O-ISM3 YCOBIT, APLICADAS A UNA RED DE ÁREA LOCAL",** luego de corroborar que el mismo se encuentra finalizado, lo he revisado y doy fé de que el mismo cumple con los objetivos propuestos en el respectivo protocolo, por consiguiente, procedo a la aprobación correspondiente.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Herman Igor Véliz Linares
Colegiado No. 4836

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 9 de octubre de 2023

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación de la estudiante **CARLA LUCRECIA JIGUAN AGUILÓN** con carné **200515929** y CUI **1603 77102 0101** titulado **"DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO27000/IEC, O-ISM3 Y COBIT, APLICADAS A UNA RED DE ÁREA LOCAL",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados y Revisión
de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

SIST.LNG.DIRECTOR.12.EICCSS.2023

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador de área y la aprobación del área de lingüística del trabajo de graduación titulado: **DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO27000/IEC, O-ISM3 Y COBIT, APLICADAS A UNA RED DE ÁREA LOCAL**, presentado por: **Carla Lucrecia Jiguan Aguilon**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería.

"ID Y ENSEÑAD A TODOS"

Ingeniero Carlos Gustavo Alonzo
DIRECTOR
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, octubre de 2023

Decanato
Facultad e Ingeniería

24189101- 24189102

LNG.DECANATO.OIE.99.2023

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **DISEÑO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO27000/IEC, O-ISM3 Y COBIT, APLICADAS A UNA RED DE ÁREA LOCAL**, presentado por: **Carla Lucrecia Jiguan Aguilon** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Firmado electrónicamente por: José Francisco Gomez Rivera
Motivo: Orden de impresión
Fecha: 25/10/2023 18:16:36
Lugar: Facultad de Ingeniería, USAC.

Ing. José Francisco Gómez Rivera
Decano a.i.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO a.i.
Facultad de Ingeniería

Guatemala, octubre de 2023

ACTO QUE DEDICO A:

Dios	Mi Señor y Salvador por su amor y fidelidad a lo largo de toda mi vida.
Mis padres	Pablo Jacinto Jiguan López (q. e. p. d) y Flory Amparo Aguilón Guzmán por ser un ejemplo de trabajo, paciencia, perseverancia, amor y apoyo incondicional.
Mis hermanos	Brenda, Pablo, Lusaida y Marggie Jiguan por su amor fraternal.
Mis amigos	Tito y Épsilon Sarmiento por acompañarme en mis noches de desvelo.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por darme la oportunidad de ser una profesional y cumplir así una de mis metas.
Mis catedráticos	Por compartir sin egoísmo sus conocimientos.
Ing. Herman Véliz	Por brindarme su apoyo y asesoría profesional para desarrollar esta investigación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Gbps	Gigabyte por segundo
Mbps	Megabyte por segundo

GLOSARIO

Activo Bien físico o recurso de información que posee algún valor para la compañía.

Amenaza Evento inesperado con el potencial de causar daño.

Análisis de riesgos Metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

COBIT Modelo de objetivos de control para tecnologías de la información que permite implementar un marco de control y gobernabilidad.

Conmutador Dispositivo digital lógico de interconexión de equipos cuyo fin es dividir una red de área local en múltiples dominios de colisión.

Cortafuegos Sistema de seguridad que bloquea accesos no autorizados.

Enrutador Dispositivo electrónico encargado de conectar a los dispositivos de red a una red.

Gusano Programa que se replica así mismo al estar dentro de una red cuyo fin es infectar otras computadoras

	mientras permanece activo en los sistemas infectados.
IATA	Asociación Internacional de Transporte Aéreo.
IEC	Comisión Electrotécnica Internacional que establece estándares internacionales en los ámbitos de electrónica, electricidad y telecomunicaciones.
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos encargados de crear estándares en el mundo.
ISO	Organización internacional de estandarización encargada de elaborar normas internacionales para garantizar la calidad.
ITU	Unión Internacional de Telecomunicaciones.
LAN	Red de área local que interconecta dispositivos electrónicos dentro de un área limitada.
Malware	*Software* malicioso que se infiltra en los dispositivos, servicios de red con el fin de dañarlos o extraer información.
MAN	Red de área metropolitana que interconecta una colección de redes más pequeñas dispersas en una ciudad.

PAN	Red de área personal que conecta dispositivos electrónicos dentro del área inmediata de un usuario.
RFID	Identificación por radio frecuencia.
SGSI	Sistema de gestión de seguridad de la información que se encarga de tratar los riesgos de seguridad.
SMTP	Protocolo de red utilizado en el envío y recepción de correo electrónico.
TCP	Protocolo de red que permite que dos anfitriones se conecten e intercambien flujo de datos.
TI	Término utilizado como sinónimo para los identificar a ordenadores, redes de computadoras y el *software.*
Troyano	Código fuente que se esconde dentro de un programa útil, realizando acciones ilícitas.
VPN	Red privada virtual de conexión privada y segura a través de Internet entre un dispositivo y una red privada.
WAN	Red de área amplia que interconecta grupos o redes de ordenadores a grandes distancias.
WIFI	Tecnología de red inalámbrica entre sistemas informáticos y electrónicos.

RESUMEN

En las organizaciones se llevan a cabo diversas actividades que tienen la finalidad de resguardar y proteger sus recursos tecnológicos, para lo cual se apoyan en sistemas y tecnologías modernas. Al implementar nuevas tecnologías se exponen a nuevos riesgos para los cuales no están preparados.

Por esto se propone un diseño de políticas de seguridad basadas en normas y estándares internacionales enfocadas en la seguridad de la información. Para realizar este diseño, se deberán identificar los activos de la organización, identificar las posibles amenazas o vulnerabilidades, definir control de accesos y establecer probabilidades de ocurrencia.

Con base a los hallazgos se establecen una serie de políticas de seguridad y políticas de acción o de respuesta ante la amenaza o ataque. Las políticas implementadas y puestas en marcha ayudarán a medir los logros y mejoras obtenidas en el ámbito de seguridad de la información de la organización.

OBJETIVOS

General

Proponer políticas de seguridad para una red de área local basadas en la Norma Internacional ISO27000, el estándar O-ISM3 y COBIT.

Específicos

1. Identificar las vulnerabilidades físicas y lógicas dentro de una red de área local.

2. Proponer estrategias de seguridad con el fin de minimizar las vulnerabilidades identificadas.

3. Proponer un modelo de red que permita gestionar la seguridad dentro del área local.

4. Proponer un plan para crear una cultura de seguridad en el departamento de TI y otros usuarios.

.

INTRODUCCIÓN

Una red de datos es la interconexión de equipo informático y dispositivos de red donde se permite transmitir información a través del intercambio de los datos, esta red debe estar protegida ante amenazas externas o internas. En la actualidad surge la necesidad de incrementar los niveles de seguridad ya que la información y los servicios son el bien más preciado de toda organización.

Sin embargo, para poder proveer de seguridad una red de comunicaciones es necesario conocer el tipo de la red sobre la cual trabajamos, y la seguridad tanto física como lógica que podemos aplicar, para ello es primordial identificar los bienes físicos y lógicos que la conforman y a partir de allí establecer las vulnerabilidades físicas y lógicas que puedan presentarse.

En este sentido, esta investigación permitirá establecer una serie de recomendaciones para encontrar vulnerabilidades físicas y lógicas de una red de Área Local, con ello se proponen algunas políticas que puedan implementarse ofreciendo así alternativas que puedan solventar la falta de seguridad en la red.

1. RED DE DATOS

Según Baltazar y Campuzano (2011), una red de datos es un conjunto de dispositivos electrónicos conectados por un medio de una red, siendo el medio un cable o una conexión inalámbrica por ondas o radiofrecuencias, estos dispositivos electrónicos son coordinados por un servidor o por un dispositivo de interconexión de red, pudiendo ser este un enrutador, un conmutador o un concentrador de red.

Las redes de datos surgen con la necesidad de enviar y recibir información, modificar y actualizar recursos y programas que pueden estar ubicados dentro de la misma o fuera de ella. Desde sus inicios y hasta el día de hoy siguen creciendo y evolucionando, poniendo al alcance de las personas recursos o información que pueden estar en otro país u otro continente, comunicándolos de manera inmediata en casi cualquier parte del hemisferio terrestre.

1.1. Tipos de redes

Según la distancia que cubre y el tamaño de su arquitectura física se clasifican en redes de área personal (PAN), redes de área local (LAN), redes de área metropolitana (MAN) y redes de área amplia (WAN).

1.1.1. Redes de área personal

La red de área personal también conocida como red PAN conectan dispositivos cuyo alcance está dentro del rango de una persona, o una habitación,

este tipo de red puede transmitir información mediante conexión cableada o inalámbrica. Hoy en día es muy común ver este tipo de redes conectadas mediante la tecnología Bluetooth. Esta tecnología permite la transferencia de datos mediante ondas de radio a corta distancia, para ello los dispositivos que se quieren conectar deben poseer esta tecnología, ya que esta permitirá encontrar y conectar dispositivos entre sí ya que utiliza el modelo maestro-esclavo.

Este modelo se rige por las órdenes que el nodo maestro proporciona a los dispositivos que se han conectado con él, estos pueden ser hasta 7 nodos esclavos activos a una distancia no mayor de 10 metros, indicándoles cuando pueden transmitir la información, por cuanto tiempo y que frecuencias usar. Con la ayuda de otras tecnologías como la identificación por radio frecuencia (RFID) también se pueden construir redes de área personal donde los dispositivos se comunican dentro de rangos cortos usando etiquetas o microchips; poseen un identificador único y una antena que recibe transmisiones por radio (Tanenbaum & Wetherall, 2012).

1.1.2. Redes de área local

Las redes de área local o redes LAN, son conocidas como redes empresariales que están limitadas a edificios, casas y oficinas, usadas con el fin de compartir información y recursos dentro del área que cubre, el alcance de dicha área puede ser de metros o kilómetros cuadrados. Este tipo de redes tienen una velocidad de transmisión de entre 10 y 100 Mbps, conectadas por enrutadores, conmutadores, concentradores y puntos de acceso para el envío de información a los dispositivos periféricos como computadoras, servidores e impresoras. Los enrutadores o conmutadores son dispositivos que están diseñados para resolver problemas de rendimiento, congestión de la red y cuellos de botella. Están configurados mediante el estándar de comunicación Ethernet,

establecidos para recibir los paquetes por una interfaz reenviándolos a otra interfaz, encapsulando los paquetes utilizando la dirección para saber a qué dispositivos final debe enviar la información, al hacer uso de conmutadores también reciben el nombre de redes conmutadas y al hacer uso de concentradores o *hubs* con salida o sin salida a otras redes, se denominan redes LAN compartidas ya que comparten el ancho de banda entre los equipos que forman parte de la red, asignando el ancho de banda al equipo que emite la información, mientras que el resto se queda en espera, mostrándose un retardo de la comunicación entre los equipos.

La conexión de las redes LAN puede darse por medio de red como el cable o a través de ondas. Las redes LAN alámbricas o cableadas utilizan cable de cobre o fibra óptica pudiendo comunicar dispositivos a velocidades que van desde los 100 Mbps a 1Gbps, ya que por el poco alcance tienen un buen rendimiento en la transmisión de la información, a diferencia de las redes LAN inalámbricas que no utilizan cables para transmitir la información, estas redes poseen velocidades de transmisión de la información que van desde cientos de Mbps hasta 1 Gbps, en este tipo de red LAN cada dispositivo posee un equipo de radio y un dispositivo central llamado punto de acceso cuya función es retransmitir los paquetes entre los dispositivos conectados inalámbricamente, utilizando el estándar IEEE 802.11 o más conocido como WIFI (Tanenbaum & Wetherall, 2012).

Componentes para una red de área local

- Tarjetas de interfaz de red
- Computadoras
- Conexión cableada o inalámbrica
- Dispositivos periféricos

- Dispositivos de red

1.1.3. Redes de área metropolitana

A las redes MAN se les conoce como redes de área metropolitana ya que cubre una gran extensión geográfica pudiendo ser ciudades pequeñas o zonas, compartiendo información de voz y video a una velocidad de hasta 20 Mbps si la conexión es mediante varios pares de cobre trenzados, pero si la conexión es a través de fibra óptica la velocidad de transmisión de la información puede ser de hasta 10 Gbps.

Estas redes se dividen en redes de área metropolitana pública y privada. Las redes de área metropolitana pública con de poca velocidad de transmisión ya que operan menos de 2 Mbps a diferencia de las redes de área metropolitana privada que son más rápidas y seguras que las públicas, ya que facilita la instalación del cableado. Al igual que las redes de área local, las redes de área metropolitana están conectadas por enrutadores y conmutadores configurados para gestionar el tráfico y el flujo de la información, mediante diversos protocolos.

Las redes de área metropolitana están compuestas por nodos de red, que almacena de manera temporal la información que van a transmitir hasta que el canal que transmite se libere, también la conforma un sistema de cableado para conectar los nodos de red, puestos de trabajo como computadoras, servidores y protocolos de comunicación.

Algunas ventajas de este tipo de red son:

- Los tiempos de acceso a la red son mínimos.

- Son óptimas para entornos de tráfico multimedia y óptimas en la transmisión de información.
- Poseen mecanismos automáticos de recuperación frente a los fallos.
- Son más seguras al estar conectadas por fibra óptica.

1.1.4. Red de área amplia

Las redes de área amplia son el conjunto de varias redes de menor tamaño, pudiendo ser estas las redes de área local o las redes de área metropolitana, abarcando así mayor extensión geográfica como un país o un continente, las redes de área amplia están conformadas por líneas de transmisión y dispositivos de red, siendo las líneas de transmisión las encargadas de mover la información entre dispositivos finales y los dispositivos de red, estos últimos son los encargados de conectar estas líneas de transmisión (Stallings, 2004).

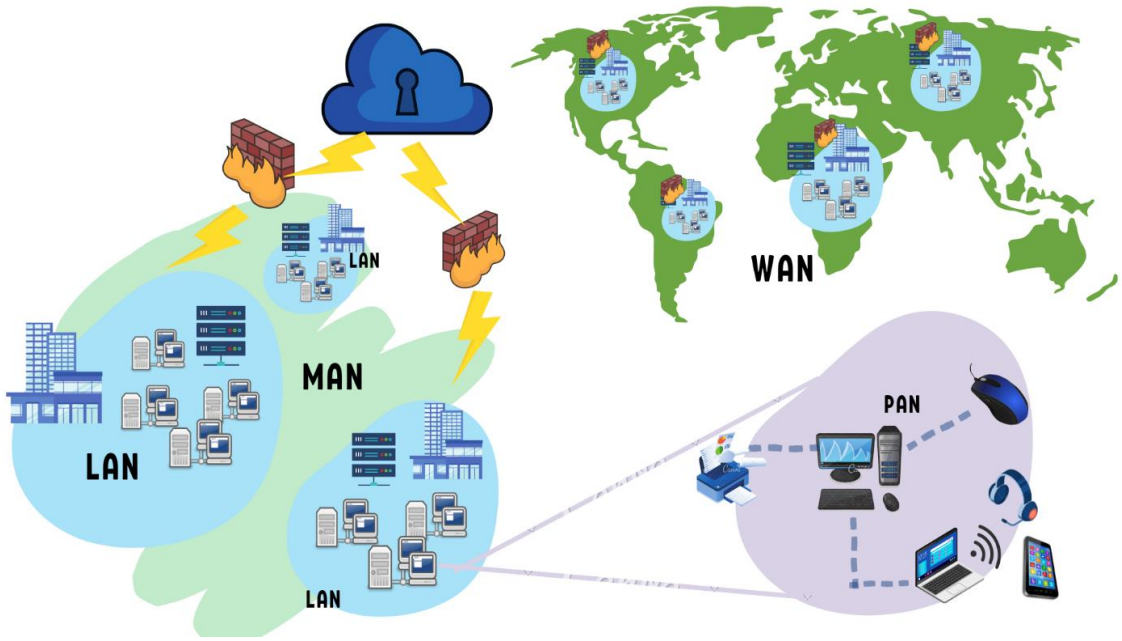
Este tipo de red puede utilizar tecnología inalámbrica como alámbrica, al hacer uso de la tecnología inalámbrica y conectar países necesitan tener en la tierra computadoras de antena capaz de recibir y enviar datos a un satélite en órbita, un enrutador para transmitir la información de un host a otro y un canal que transporta la información de un punto hacia otro.

Estas redes tienen una topología lógica y una topología física, entre las topologías físicas se encuentran las siguientes:

- Red directa
- Red anillo
- Red de árbol
- Red estrella
- Redes irregulares

Figura 1.

Tipos de redes



Nota. Tipos de redes según su tamaño y arquitectura física. Elaboración propia, realizado con Canva

2. SEGURIDAD DE LA RED

Se define como seguridad toda aquella actividad que está diseñada para resguardar los accesos, el uso y la integridad de la información que se envía y recibe en una red. Este concepto cobra fuerza e importancia desde el momento en que se conectan dos o más computadoras a una red interna o bien a la internet con el fin de recibir, almacenar, enviar información, compartir recursos o servicios. Pero la seguridad va más allá de proteger la información ya que es de suma importancia proteger todos los bienes de una organización, tanto el *hardware* (componentes físicos) como el *software* (componentes lógicos) que conforman la red (Cisco, 2023).

Se cataloga como seguridad física la que está orientada a proteger todo el *hardware* que forma parte de la red, esta seguridad va desde los controles perimetrales, entornos de laboratorio como paredes que eviten visualizar el laboratorio de red, al mismo tiempo impedir filtraciones que puedan dañar el equipo. Asimismo, se debe tomar en cuenta la temperatura y humedad del cuarto donde se mantiene alojado el equipo. Mientras que la seguridad lógica es aquella que se encarga de proteger configuraciones de equipo, servicios que provee la organización y la información que circula por todo el *hardware* de red, para ello es importante tener un control de acceso a la información y al equipo de red, impedir el acceso al equipo interno desde equipos externos, configurar dispositivos como un corta fuegos para proteger la red de ataques externos y la implementación de herramientas que mantengan los dispositivos de red libre de virus, *antispyware*, *antimalware* y otros programas que ayuden a analizar el tráfico de la red.

La seguridad no solo incluye cuidar o resguardar los bienes físicos y lógicos de una organización, la seguridad también toma en cuenta al recurso humano, ya que este es considerado como el eslabón más débil y parte fundamental para evitar que *software* malicioso se filtre y se distribuya en la red. Para lo anterior es necesario educarlo en el tema de seguridad a fin de que aprenda a gestionar lo mejor posible los errores que pudiesen cometer dentro del rol que le corresponde en la seguridad.

2.1. Principios de la seguridad

La Norma ISO 27001 provee un conjunto de recomendaciones bien estructuradas con el objetivo de proteger los activos de la empresa, definiendo áreas de seguridad que esclarecen los objetivos de estas. Al mismo tiempo esta norma se basa en la preservación de la confidencialidad, integridad y disponibilidad de la información, catalogándolos, así como principios de la seguridad.

2.1.1. Confidencialidad

Según la Norma ISO/IEC 27002, la confidencialidad está definida como garantizar que la información es accesible sólo para aquellos autorizados a tener acceso, por lo que la confidencialidad es parte de los principios de la seguridad y se puede decir que la importancia data en el campo político y militar, ya que se utilizaban diversos métodos para enviar la información para evitar que ajenos a está pudieran interceptarla y corromper su contenido o robarlo.

Al pasar de los años y épocas este fin no cambia ya que solo pueden tener acceso a la información debiendo ser entendible a aquellas entidades o

individuos que fueron autorizados, este acceso a la información incluye leer, ver, imprimir y estar al tanto de la existencia de la información.

Para poder garantizar la confidencialidad es necesario que se tenga un control sobre el acceso e identificación de aquellos que tienen acceso, teniendo la certeza que son quienes dicen ser, al mismo tiempo es necesario gestionar los privilegios o roles para aquellos que tengan acceso al sistema puedan operar o acceder únicamente a la información en la cual están autorizados, estos permisos se pueden dividir en accesos solo de lectura o escritura en función del usuario autorizado y aplicar algún mecanismo de cifrado o encriptación, transformando la información de una forma inteligible en una forma no legible a aquellos que tenga o no tengan acceso a ella, esto aplicado a la información que viaja por toda la red, como a la información que está siendo almacenada.

2.1.2. Integridad

El segundo principio de la seguridad consiste en asegurar que la Información sea precisa, completa y consistente, mientras esté siendo almacenada o hasta el momento en que personas autorizadas alteren la información, es decir, debe ser precisa y confiable durante todo su ciclo de vida, este principio evita que la información sea alterada por algún programa, proceso o personas no autorizadas alteren o cambien su estado.

La integridad se logra implementando medidas de seguridad como por ejemplo adhiriendo datos de comprobación de integridad como alguna firma digital, un algoritmo hash, monitorear el tráfico que viaja en la red en busca de intrusos o bien registrar cada actividad que se realice dentro del sistema, cuando se hace y con qué información lo hacen. También es posible implementar algún sistema de control cambios, en el cual se compruebe si los datos son cambiados

o bien la creación de respaldos en los casos en los que la información ha sido alterada, el respaldo permite restaurar la información a su estado anterior.

2.1.3. Disponibilidad

Este principio asegura que los procesos, entidades o personal autorizado tengan acceso a la información y a los sistemas cuando así lo requieran, la información debe permanecer accesible de manera permanente independientemente del lugar y el momento.

Para que la información esté disponible se deben aplicar algunas medidas para permitir la disponibilidad de la información en cualquier momento, entre estas buenas prácticas están implementar un balanceador de carga, este permite que el sistema se mantenga disponible y pueda ser capaz de servir la información en cualquier momento, evitando así que el tráfico de la red se concentre en un solo servidor. El balanceador de carga se clasifica como de tipo *hardware*, de tipo switch o basado en *software*. Otra forma de ofrecer disponibilidad en la información es tener una copia de seguridad de la base de datos y del código fuente del sistema o implementar una réplica de la base de datos, esto permitirá que los datos se mantengan disponibles en caso de un tiempo de inactividad de los servicios o procesos. Una réplica permitirá sincronizar la información entre un publicador y un suscriptor en un tiempo determinado, para poder implementar una réplica es necesario disponer de suficiente espacio de almacenamiento y una infraestructura potente para poder mantenerla, es importante saber que la infraestructura juega un papel imprescindible dentro de este principio, ya que el nivel de disponibilidad dependerá de lo que se desea proteger.

Figura 2.

Principios de la seguridad

Nota. Principios de la seguridad de la información. Elaboración propia, realizado con Power Point.

3. VULNERABILIDAD, ATAQUES Y AMENAZAS

Hoy en día no es un secreto que toda la información que viaja en la Internet está expuesta a ataques, siendo el problema principal que los sistemas de red no cuentan con la seguridad adecuada ya sea por el desconocimiento en el tema o el incontrolable crecimiento de la red corporativa haciendo difícil la tarea de corregir los problemas de la red y del resguardo de la información, dando como resultado alguna debilidad en la red y en los servicios que ofrece, estas debilidades son puertas abiertas para cualquier persona malintencionada, cuyo fin es atacar las comunicaciones, servicios o corromper la información.

Al existir una debilidad en la red, se genera una condición que se aprovecha regularmente para dañar y esto da lugar a un ataque.

3.1. Vulnerabilidad

Una vulnerabilidad es una debilidad de un componente, servicio o *software* que se encuentra dentro de la red de una organización provocando daños y pérdida de la integridad de la información o robo de ésta. La debilidad puede ser originada por algún error de configuración de uno o varios componentes a partir de errores individuales que al interactuar generan la inseguridad de la red, estas debilidades son muy peligrosas ya que algunas no necesitan la intervención humana.

Las vulnerabilidades se pueden clasificar entre vulnerabilidades físicas, de *software* y de *hardware* y vulnerabilidades en la transmisión de datos.

3.1.1. Vulnerabilidades físicas

Dentro de las vulnerabilidades físicas se encuentran aquellas que pueden llegar a afectar la infraestructura física de la organización como estar ubicados en una zona de alto riesgo a inundaciones, sismos o desastres naturales, al estar expuestos a este tipo de vulnerabilidad la información puede carecer de disponibilidad, otras vulnerabilidades físicas es la falta de aislamiento del equipo de red, tener poco control en el acceso al cuarto físico donde se encuentra alojada la infraestructura puede provocar el sabotaje y el robo de la información.

Las vulnerabilidades de *hardware* están dadas por defectos de fábrica en los equipos, y falta del equipo apropiado dentro de la infraestructura de red.

3.1.2. Vulnerabilidades lógicas

Las vulnerabilidades lógicas son aquellas que afecta directamente al desarrollo y desempeño del sistema y los servicios que ofrece una organización, especialmente se inclinan más al *software* mal instalado, configuraciones incompletas en conmutadores o corta fuegos, falta de actualización del sistema operativo, falta de antivirus en los equipos y *software* no licenciado.

Estas vulnerabilidades pueden ser aprovechadas de forma remota provocando la caída de la red mediante ataques a los servidores, extrayendo información a través de puertos abiertos o mediante la infiltración de usuarios externos aplicando ingeniería social.

3.2. Amenaza

Las amenazas son circunstancias o condiciones que se dan con el fin de causar pérdidas, daños al sistema o a los activos de la organización, comprometiendo la seguridad de los datos y de toda la red. Las amenazas pueden ser producidas por personas, programas maliciosos, factores técnicos o catástrofes naturales.

Dentro de las amenazas que se pueden controlar están las que se producen por las personas de manera voluntaria ya que, al no tener un control en los accesos. Estas pueden explorar el sistema en busca de puertas traseras con el fin de instalar programas maliciosos, virus informáticos, gusanos o bien robar información confidencial perjudicando a la organización o simplemente exponer los accesos a terceros con el fin de comprometer la seguridad de la información y del sistema. También están las amenazas producidas de manera involuntaria como las efectuadas por personas inexpertas, las originadas por el mal funcionamiento del equipo de red o fallo del sistema y las amenazas que difícilmente se pueden controlar como las creadas por los desastres naturales, pero que es posible reducir el impacto negativo que estas pueden tener como tener copias de seguridad en la nube, y principalmente tener sumo cuidado en el entorno donde se instalará el equipo de red.

3.3. Ataque

Un ataque es una violación que atenta contra los principios de la seguridad y se vale de una debilidad en la red, estos pueden ser intencionales y no intencionales provocados o no por entidades humanas, lógicas o por la naturaleza. Los ataques son realizados de manera remota, por medio de ingeniería social, ataques internos, acceso físico a los dispositivos o penetración,

teniendo como consecuencia la pérdida, alteración de la información y del correcto funcionamiento del equipo de red, pérdidas económicas, incumpliendo con los servicios que el sistema proporciona y la alteración del flujo de datos.

Los ataques se dividen en ataques lógicos y físicos, siendo este último el más crítico ya que si la seguridad física falla, todos los mecanismos de seguridad lógica como firmas digitales, cifrados, servicios de VPN y corta fuegos fallará. Dentro de estos ataques también se incluyen los provocados por las fuerzas de la naturaleza como las tormentas, incendios accidentales, inundaciones y temblores. Los ataques lógicos son aquellos que tienen como fin explotar las debilidades en los protocolos configurados en los dispositivos de red, en el *software* mal instalado, o carente de actualizaciones. Es importante que se tenga un amplio conocimiento y un especial cuidado en la seguridad física y lógica, así como también conocer la forma en que se lleva a cabo un ataque.

3.3.1. Tipos de ataques

Entre los tipos de ataques se encuentran:

- Denegación de servicio
- Acceso no autorizado a los recursos y a la información
- Enmascaramiento
- *Malware*

3.3.1.1. Denegación de servicio

Este tipo de ataque busca sobrecargar la capacidad de un servidor inundando la red con demasiadas conexiones simultáneas, con el fin de interrumpir el correcto funcionamiento de los dispositivos u ocasionando la caída

de la red, afectando la disponibilidad de la información. Este ataque proviene de un único ordenador o de varias fuentes provocando una sobreescritura en el búfer de datos, esto puede modificar la memoria de un servidor controlando la ejecución de los servicios que estén alojados en este o inhabilitando los servicios que la red provea. Otro tipo de ataque de denegación de servicio es inundar un enrutador con paquetes no ruteados provocando un mal desempeño en la transmisión de paquetes ya que estos paquetes que provocan la inundación son transmitidos.

3.3.1.2. Ataque no autorizado a recursos y a la información

Dentro de los ataques que facilitan el acceso no autorizado a recursos de la red y a la información se encuentran los siguientes.

Spoofing o suplantación, este ataque busca suplantar la identidad de usuarios autorizados para obtener información, monitoreando el tráfico de paquetes alterados que se envían desde una falsa ruta, buscando una puerta trasera para controlar los sistemas y tener acceso a ellos.

Secuestro de sesión: este ataque busca tener acceso no autorizado secuestrando la sesión, en este ataque el intruso retiene las credenciales y la información personal de un usuario legítimo. Aprovecha las vulnerabilidades de los servidores o de las aplicaciones *web* inyectando scripts en el lado del cliente con el cual pueden obtener los accesos a la red.

Otro ataque que tiene como fin penetrar la red y tener accesos no autorizados es el denominado El hombre en el medio, este busca robar información mientras monitorea el tráfico de la red entre usuarios legítimos

interceptando, modificando o destruyendo la información, comprometiendo así la integridad y disponibilidad de esta.

3.3.1.3. Enmascaramiento

El enmascaramiento es un ataque en el que el intruso manipula los datos que viajan en la red con el fin de falsificar direcciones IP fingiendo ser un usuario legítimo. Estos ataques utilizan rastreadores de contraseñas, modificadores de secuencia, herramientas de pruebas de puertos TCP para servicios específicos, al obtener toda la información que necesite puede deducir vulnerabilidades del sistema al cual pretende vulnerar.

3.3.1.4. *Malware*

El *malware* o programa malicioso se clasifica en la forma en que opera y se propaga. Dentro de los más conocidos están los virus, gusanos, troyanos y programas espía.

Vieites (2013) define virus como un programa desarrollado en un lenguaje de programación en específico que tiene como fin infectar un sistema informático. Los virus son usados por los atacantes para alterar el funcionamiento del equipo provocando la pérdida de la información, daños en el arranque del equipo ya que puede alojarse en el sector de arranque y al momento de cargar el sistema operativo el virus se ejecuta y obtiene el control de algunas funciones permitiendo su fácil propagación. Asimismo, pueden generar tráfico excesivo dentro de la red o bloqueo de funciones del sistema operativo donde reside. La forma de propagación más común es abrir un correo electrónico infectado, intercambio de datos por medio de dispositivos extraíbles, un sitio web, conexiones a una red pública o conexiones a Internet. Estos programas se ejecutan automáticamente

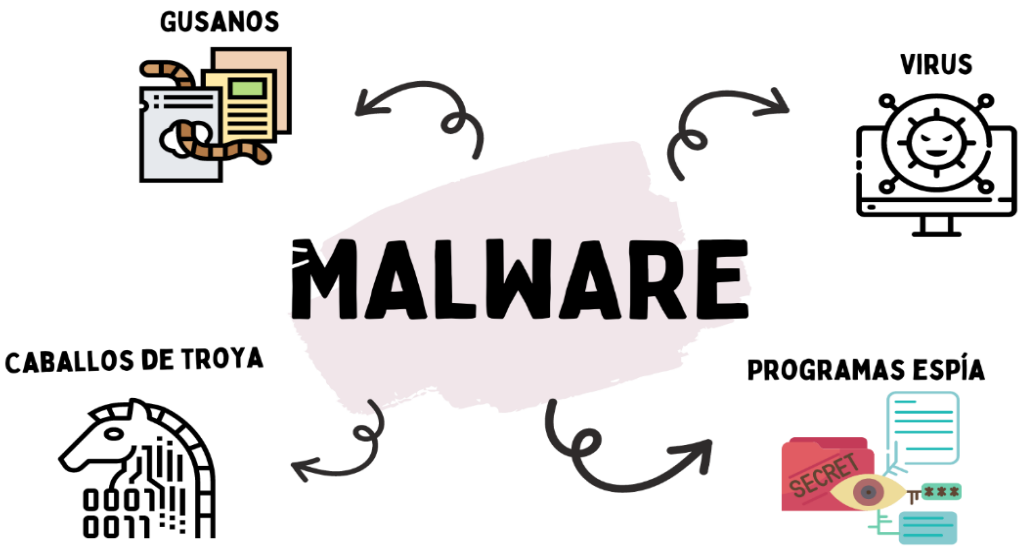
o puede activarse mediante una tarea o evento, copiándose a sí mismos y alojándose en memoria y al ejecutarse infecta programas con extensión exe, com y sys.

Los gusanos también se catalogan como programas maliciosos, ya que contienen instrucciones que le permiten propagarse por todo el equipo a través de la red. Estos se clasifican según el método de propagación: los gusanos de Internet cuyo propósito es escanear equipos buscando aquellos cuyo sistema operativo o programas que no estén parchados y al encontrar una vulnerabilidad en el sistema se instala y ejecuta su código y se copia a sí mismo en todo el sistema. Los gusanos de mensajería instantánea que se propagan por mensajes instantáneos enviando a todos los contactos enlaces a sitios *web* infectados. Los gusanos de correo electrónico buscan propagarse por conexiones a servidores SMTP, servicios de mensajería instantánea y mediante algunas funciones del sistema operativo.

Dentro de la categoría de programas maliciosos también están los caballos de Troya o más comúnmente llamados Troyanos, que no son más que programas en apariencia útiles pero que al estar dentro del sistema operativo realizan las peticiones que el usuario requiere y al mismo tiempo ejecutan otros procesos como capturar información de accesos o simplemente crean puntos de acceso para el ingreso. Los programas espía también son catalogados como programas maliciosos ya que se alojan en los sistemas, recopilando información de todo lo que se realiza en el sistema especialmente datos de usuarios con el fin de distribuirlo a sitios de internet que usan la imagen corporativa de otros.

Figura 3.

Clasificación del malware



Nota. Clasificación en la forma que opera un programa malicioso. Elaboración propia, realizado con Canva

4. ESTÁNDARES Y NORMAS INTERNACIONALES DE SEGURIDAD

Hoy en día existen soluciones de seguridad basadas en estándares y normas internacionales que permiten detectar vulnerabilidades mediante marcos de trabajo y buenas prácticas que se asocian a la gestión de vulnerabilidades y gestión de riesgos, que combinado a otras disciplinas se enfocan en promover una adecuada administración de políticas o reglas cuyo fin es la gestión de la seguridad de la información.

Los estándares y normas internacionales proveen un marco estructurado de seguridad de la información, siendo esta la base para la gestión de la seguridad. Este marco permite identificar y atenuar vulnerabilidades, definir roles y controles de accesos a usuarios, monitorear los procesos de gestión de riesgo, definir activos, identificar debilidades, documentar, comunicar y establecer políticas a partir de los objetivos y metas de seguridad.

4.1. Estándar

Según Cifre (2018), los estándares son documentos técnico-legales en los que se describen especificaciones técnicas. Dichos documentos son elaborados consensuadamente por partes interesadas como asociaciones, centros de investigación y laboratorios, mejorados y aprobados por organismos reconocidos a nivel regional o internacional.

Estos documentos proporcionan de manera clara y precisa la forma de trabajo concreto, haciendo posible que un producto, materiales, procesos o

servicios pueda funcionar de la mejor manera con otros productos independientemente del fabricante con el fin de que puedan cumplir su propósito. Al ser implementados aumenta el potencial de la organización previniendo errores humanos.

Los estándares de seguridad de la información ayudan en el uso de mejores buenas prácticas, enfocando a la organización a un objetivo en común, a la creación de un marco de trabajo y la aplicación de la experiencia adquirida, al certificar un estándar la organización mejora su imagen organizacional interna y externa, además de proveerles mejores y más oportunidades de negocio.

4.2. Norma

Una norma se define como documento establecido por consenso y aprobado por un organismo reconocido, que provee, para el uso común y repetitivo, reglas, directrices o características para actividades o, sus resultados dirigidos a alcanzar el nivel óptimo de orden en un concepto dado. Estos documentos con especificaciones técnicas que son aprobados por un ente nacional o internacional de normalización reconocido, cuya elaboración fue un consenso entre fabricantes, administradores, consumidores y asociaciones.

Estos documentos permiten implementar de forma precisa métodos que se rigen por procedimientos bien definidos; las organizaciones que implementan las normas obtienen un nivel de ordenamiento óptimo mejorando la ventaja competitiva frente a otras organizaciones otorgándoles un conjunto de certificaciones, si cumplen las exigencias establecidas en dicho documento; aumentando el potencial organizacional y optimizando el recurso a nivel nacional e internacional.

En la actualidad, existen organismos nacionales e internacionales que se dedican a crear estas reglas entre las más importantes están:

- ISO (Organización Internacional Para la Normalización)
- IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)
- IATA (Asociación Internacional de Transporte Aéreo)
- ITU (Unión Internacional de Telecomunicaciones)

4.3. ISO 27000/IEC

La Organización Internacional para la Estandarización conocida por sus siglas en inglés como ISO, es un ente fundado en 1946 y conformado por 157 países miembros de organizaciones nacionales de estándares, entre ellos destacan ANSI, BSI, AFNOR y DIN. La ISO produce gran variedad de estándares internacionales en diferentes ámbitos además de cooperar en la creación de estándares con otras organizaciones, con el fin de evitar incompatibilidad de dos estándares internacionales oficiales (Tanenbaum & Wetherall, 2012).

Dentro de los estándares más importantes a nivel mundial se destacan ISO/IEC 27000 y el estándar O-ISM3.

La familia ISO/IEC 27000 es un conjunto de estándares desarrollados por la Organización Internacional de Normalización y la Comisión electrotécnica Internacional, estos estándares proveen un conjunto de buenas prácticas para la gestión de la seguridad de la información y el modo de implementar controles de seguridad de la información, monitoreando, estableciendo mejoras y someterlas a revisiones, describiendo los lineamientos de implementación, definiendo vulnerabilidades específicos y técnicas de diseño tomando como guía escenarios típicos de una red.

La finalidad de la norma ISO/IEC 27000 permite:

- Asegurar los activos críticos
- Administrar los riesgos de una manera efectiva
- Demostrar conformidad con las mejores prácticas internacionales
- Desarrollar una postura de seguridad de la información junto con los desarrollos tecnológicos.

4.3.1. ISO 27001

Esta norma define los requisitos que se deben establecer, implementar, evaluar y para documentar un sistema de gestión de la seguridad de la información, asimismo buscar evidenciar el funcionamiento correcto del sistema, mediante la creación y gestión de los controles de seguridad que se deben considerar, así como también las revisiones y las mejoras del SGSI. El tema principal de esta norma se basa en investigar donde se producen los riesgos para luego establecer un plan sistémico de cómo evitarlos. Las ventajas que una organización tiene a la hora de implementar esta norma es la reducción de costos ya que se evitan los incidentes, obtienen una ventaja comercial comparadas con otras organizaciones, ya que su interés se centra en mantener de forma segura la información, poseen una metodología de cumplimiento relacionados con la seguridad de la información, así mismo la organización tiene una mejor orientación de cómo hacer y qué hacer en cada situación que se les presente reduciendo así el tiempo entre situaciones.

A continuación, se describen algunos puntos importantes para aplicar esta norma.

- La organización debe determinar el contexto interno y externo para tener claro su propósito evitando así que afecten el logro de sus resultados.

- Determinar los requisitos y las partes interesadas para el sistema de gestión de la seguridad.

- Determinar los límites, el alcance y la aplicabilidad del sistema de gestión de seguridad de la información.

- Se debe demostrar compromiso con todos los elementos que intervendrán al sistema de gestión de la información.

- La organización debe establecer una política de seguridad que incluya objetivos alcanzables, que incluya el compromiso de que se cumpla y el compromiso de mejorar continuamente el sistema de gestión de la información.

- Asignar responsabilidades y roles.

- Planificar cómo tratar los riesgos a fin de prevenir o reducir los efectos no deseados.

- Determinar los recursos necesarios para establecer, mantener y aplicar la mejora continua.

- Planificar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información.

- Medir y analizar el desempeño de la seguridad de la información.

- Mejorar de manera continua la eficacia, la adecuación del sistema de gestión de la información.

4.3.2. ISO 27002

Esta norma complementa la Norma ISO 27001 ya que describen los mecanismos de control que pueden ser implementados, siguiendo las directrices de la ISO 27001. Estos controles buscan mitigar el impacto de los riesgos a los que se encuentra expuesta la organización y desarrollar sus propias guías de gestión de seguridad de la información.

La estructura de esta norma se organiza en seguridad organizacional, seguridad técnica y seguridad normativa. La sección de controles se considera una guía aplicable como punto de partida para desarrollar reglas específicas de la organización, estos controles deben ser tomados en cuenta en las actualizaciones, mejoras y cambios que se apliquen a los sistemas de información tomando en cuenta los riesgos y escenarios actuales y futuros. Estos controles deben tener un objetivo específico de lo que se desea conseguir y los controles aplicables para alcanzar ese objetivo, proporcionando a detalle la implementación del control.

4.3.3. ISO 27003

La ISO 27003 busca establecer un marco de trabajo, con el fin de implementar un Sistema de Gestión de Seguridad de la Información, basado en las directrices de la norma ISO 27001. Esta norma describe la especificación y diseño de un SGSI desde el inicio hasta la implementación, en esta se define el alcance y objetivos, definiendo las políticas de seguridad. Además de hacer una evaluación de los requerimientos de seguridad de la información y de los riesgos,

debe formular un plan de tratamiento de estos. Dependiendo del contexto de la organización, está indicará que parte de esta guía es aplicable y se adecua a la misma.

En esta norma se define una estructura de implementación:

- Obtener la aprobación de la gerencia para iniciar el proyecto SGSI
- Definir el alcance y políticas del SGSI
- Realizar un análisis de la organización
- Estimar los requisitos de seguridad para la información
- Establecer riesgos y una planificación para tratarlos
- Diseñar el SGSI

4.3.4. ISO 27005

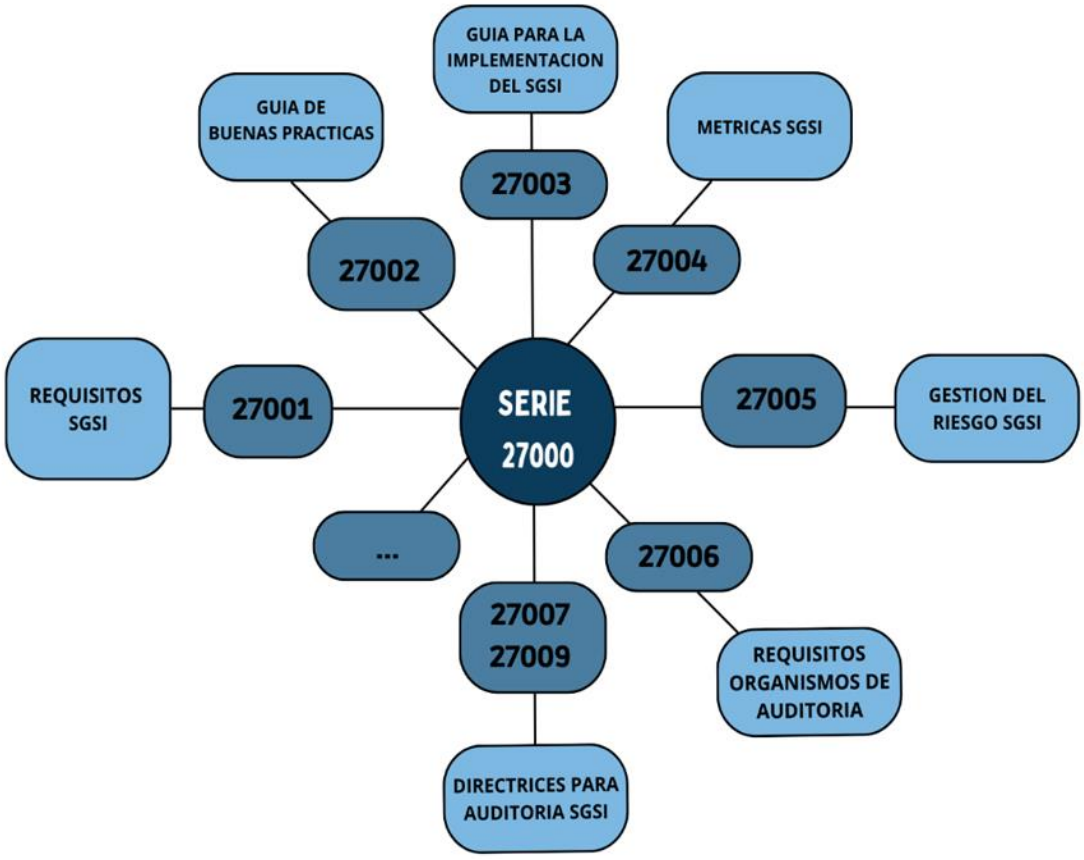
A diferencia de las otras normas esta busca plantear reglas para la gestión del riesgo en la Seguridad de la Información, y ya que no brinda ninguna metodología para la gestión de riesgo en la seguridad de la información, se puede implementar la metodología que mejor se ajuste al enfoque de la gestión de riesgo de la información, pero siempre bajo la estructura que describe esta norma.

La gestión de riesgo en la seguridad de la información analiza los posibles escenarios que se pueden dar y sus consecuencias, con el fin de reducir los riesgos, identificar los posibles riesgos, evaluar cada escenario y las consecuencias y las posibilidades que estos se repitan. Además, quienes pueden tomar decisiones sobre los riesgos y cómo mitigarlos, comunicar la información sobre los riesgos para mejorar el enfoque de la gestión de riesgos y educar a

todos dentro de la organización, así como también se deben mantener revisiones regularmente y monitorear los procesos de gestión de riesgo.

Figura 4.

Familia ISO 27000



Nota. Familia de estándares ISO 27000. Elaboración propia, realizado con Canva.

4.4. O-ISM3

Este modelo de Open Group es un marco para la gestión de la seguridad de la información orientado a procesos pensado para mejorar la integración de metodologías y normas como COBIT, ITIL o CMMI, compatible con la norma

ISO/IEC 27001. La idea de este marco es lograr la prevención de los ataques que se presenten en la organización, es por ello que asigna a la empresa la responsabilidad de definir los objetivos de seguridad empresarial, para luego ofrecer un conjunto de procesos de gestión de seguridad.

La orientación del modelo O-ISM3 cubre la evaluación de riesgos, auditoría, auditoría de cumplimiento, supervisión, pruebas, diseño, mejoras, optimización y un análisis de dependencia para el cumplimiento de los objetivos de la seguridad de la organización, entre estos objetivos está poner como prioridad, la disponibilidad de los servicios que ofrece la organización, respaldos e identificar los posibles puntos de fallas, cuidar que se provee la integridad de la información, la calidad y consistencia de los repositorios, así como tener un control de accesos, permisos, roles y la seguridad técnica orientada a la infraestructura del centro de datos.

4.5. COBIT

COBIT es un marco de gestión de TI que ayuda a las empresas en la gestión e implementación de estrategias de procesos de TI además de identificar los recursos esenciales para el éxito de los procesos ya que se ajusta con los objetivos del negocio. También ayuda a gestionar los riesgos y a asegurar el cumplimiento, la continuidad, seguridad y la privacidad,

Este marco alinea los marcos existentes con los que ya cuenta una organización. Además de controlar el rendimiento de estos, se adapta mejor a las organizaciones que utilizan ITIL, ISO/27000 y CMI. COBIT propone estructurar los procesos de la organización en 4 dominios, planificar y organizar, adquirir e implementar, entregar y dar soporte, evaluar y monitorizar.

Figura 5.

Estructura de los procesos

Nota. Estructura de los procesos de organización en 4 dominios recomendado por CoBIT, Elaboración propia, realizado con Canva.

5. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

Las políticas de seguridad son reglas necesarias en toda organización ya que hay personas que realizan actividades que van en contra de la organización entorpeciendo el buen funcionamiento del sistema. Estas se deben definir claramente evitando ambigüedades que ayuden a controlar el acceso a los sistemas, que se alineen a los objetivos de la organización, que sean realistas y que puedan trabajar juntamente con otras políticas existentes.

A la hora de aplicar las políticas de seguridad el recurso humano es el elemento más difícil de convencer ya que la falta de conocimiento en el tema de seguridad hace que desconozcan el nivel de alcance de una vulnerabilidad o un ataque a todo el sistema, por ello es necesario darles a conocer detalladamente qué es lo que pueden y no pueden hacer con el equipo del que hacen uso, además de cómo resguardar la información que manipulan.

5.1. Política de seguridad

Una política es una pauta de la alta gerencia para crear un programa de reglas específicas en donde se establecen objetivos y se asignan responsabilidades para un sistema en particular, así mismo las políticas de seguridad son reglamentos diseñados por una organización para establecer procedimientos de prevención, protección y la forma de manejar los riesgos ante los daños que se puedan presentar de tanto los elementos físicos que conforman una red y principalmente el resguardo y acceso a la información.

Al definir las políticas se debe contemplar todo el ciclo de vida:

- Definición y especificación de la política
- Implementación de la política
- Verificación del cumplimiento
- Revocación y revisión continua

Figura 6.

Ciclo de vida

Nota. Ciclo de vida de la política de seguridad. Elaboración propia, realizado con Power Point.

Una política de seguridad debe incluir los siguientes componentes (WALC 2002):

- Una política de privacidad

- Una política de acceso
- Una política de autenticación
- Planes para satisfacer la disponibilidad de los recursos de todo el sistema
- Una política de mantenimiento para la red
- Sanciones para aquellos que infrinja las políticas
- Una política de reporte de incidentes y divulgación de información

5.1.1. Características

Al crear una política de seguridad se debe definir el alcance, los sistemas y personas sobre las cuales se aplicará, la forma de implementación ya sea a través de procedimientos administrativos o a través de pautas directivas aceptables. Cada política debe describir claramente los objetivos y los elementos involucrados al momento de definirse, establecer las responsabilidades para todos los niveles de la organización y para cada uno de los recursos y servicios informáticos, así mismo definir las violaciones y sanciones al no cumplirse. Debe ser variable según los cambios tecnológicos, debe poder cumplirse además de ser simple y desarrollable.

Al establecer políticas de seguridad se buscar informar a todo el recurso humano las normas establecidas que se deben cumplir para proteger todos los componentes físicos y no físicos del sistema de la organización, además de proporcionar los criterios para configurar y auditar los sistemas de red para que estén alineados con las políticas de seguridad definidas, en la elaboración de las políticas de seguridad los principales involucrados en la creación de las políticas van desde el administrador de seguridad, todo el personal técnico, administradores de grupos de usuarios y si la organización así lo desea pueden estar involucrados un consejo legal.

5.2. Procedimiento para crear una política de seguridad

Para desarrollar una política de seguridad se debe tener claro el objetivo y las expectativas de la organización, definiendo cada procedimiento para la prevención ante los incidentes de seguridad.

Entre los principales aspectos para crear una política es importante tener en claro los objetivos y directrices de la organización, cada política debe estar acorde a los reglamentos existentes de la organización, identificar los recursos disponibles de la organización y establecer la importancia de los recursos y cuáles se deben proteger. Establecer los roles y responsabilidades de los recursos a proteger, identificar las amenazas, establecer qué medidas se deben implementar para resguardar los recursos, y quienes son los ejecutores de estas.

5.2.1. Identificación de activos

Los activos van a depender del giro de la organización, pero en general los activos de una organización serán los recursos físicos, lógicos y los relacionados con este, para que la organización funcione correctamente.

Para establecer los activos de una organización, la Norma ISO 27001 indica establecer un criterio de identificación de activos. Para identificar los activos hay que determinar las características que lo definen, por ejemplo; el nombre, el tipo de activos, la ubicación, el servicio soportado y la unidad o área responsable. Al identificar los activos se deben clasificar según la naturaleza de este, por ejemplo; equipo informático, redes de comunicación, información y personas, y funciones relacionadas con los sistemas de Información, además es importante establecer un etiquetado de acuerdo con el esquema de clasificación

que la organización haya adoptado. Crear una lista de los recursos tangibles y no tangibles que se necesite proteger.

- Equipo físico (*hardware*), *switches*, enrutadores, monitores, computadoras, unidades de almacenamiento, impresoras, servidores.

- *Software*, licencias, actualizaciones de *software*, código fuente, configuraciones.

- Información, respaldos, bases de datos, almacenamiento local y externo.

- Documentación física y lógica de la red, del equipo físico, del código fuente y del *software*.

Tabla 1.

Clasificación de activos

Clasificación	Activo
Equipo Informático	Computadoras de escritorio
	Computadoras portátiles
	Enrutadores
	Conmutadores
	Corta fuegos
	Servidores
	Estaciones de trabajo
Redes de comunicaciones	Antenas
	Puntos de acceso
	Unidades de almacenamiento
	Cableado
	Racks
	Fuentes de alimentación

Continuación de la tabla 1.

Clasificación	Activo
Información	Datos
	Base de datos
	Documentación
	Bitácoras
	Respaldos
	Archivos de configuración de equipos y de *software*
	Certificados
	Código fuente
Personal y funciones	Usuarios
	Desarrolladores
	Operadores
	Aplicativos
	Sistemas operativos
	Software

Nota. Clasificación de los activos. Elaboración propia, realizado con Excel.

Al identificar los activos se debe dar una valoración según los atributos que lo hacen valioso. Los criterios de valoración de los activos deben darse sobre los principios de la seguridad de la información. Disponibilidad, la importancia que tendría que el activo no estuviera disponible, integridad, establecer un criterio sobre qué importancia tendría que el activo puede ser alterado y la confidencialidad debe responder a la pregunta sobre qué importancia tendría que el activo sea accedido de manera no autorizada.

Tabla 2.

Valoración del activo por disponibilidad

Valor	Criterio
0	No es relevante
1	Debe estar disponible al menos 10 % de tiempo
2	Debe estar disponible al menos el 50 % del tiempo
3	Debe estar disponible al menos el 99 % de tiempo

Nota. Posible valoración de los activos en función de un rango numérico y el impacto del daño que provocaría en la organización si no está disponible. Elaboración propia, realizado con Excel.

Tabla 3.

Valoración del activo por confidencialidad

Valor	Criterio
0	No es relevante
1	El daño es bajo y no trasciende del área donde se encuentra.
2	El daño es relevante y trasciende a otras áreas
3	Los daños son catastróficos para el desempeño de la empresa.

Nota. Valoración de los activos en función de un rango numérico y el impacto que se tendría si el activo es accedido de manera no autorizada. Elaboración propia, realizado con Excel.

Tabla 4.

Valoración del activo por integridad

Valor	Criterio
0	No es relevante
1	El daño es bajo y el impacto no es significativo

Continuación de la tabla 4.

2	El daño ocasionado puede retrasar las funciones de los servicios que se ofrecen
3	El activo gestiona información y la pérdida de exactitud genera pérdidas económicas.

Nota. Valoración de los activos en función de un rango numérico y el impacto que se tendría en la integridad del activo. Elaboración propia, realizado con Excel.

5.2.2. Identificación de control de acceso

El control de acceso supone definir los accesos por parte de los sujetos sobre los objetos, siendo el sujeto cualquier ente como usuarios, procesos, servicios, tareas y sistema y el objeto cualquier ente que contiene la información es decir archivos, sistemas o directorios, estos son usados para prevenir los ataques o para determinar si hay un ataque o intentos de ataque.

Existen tres modelos sobre los que se basa el control de acceso, control de acceso discrecional, control de acceso mandatorio y control de acceso basado en roles.

El control de acceso discrecional es un control de restricción basada en limitación de privilegios, donde se crean reglas de acceso a los recursos de los cuales se tiene acceso. En este se definen dos niveles de asignación de privilegios; el nivel de cuenta, nivel que especifica los privilegios de cada usuario y el nivel de relación donde se controlan los privilegios para tener acceso a las vistas individuales, a diferencia del control mandatorio que otorga privilegios, clasificando a los usuarios y a los datos de acuerdo a etiquetas de seguridad, si

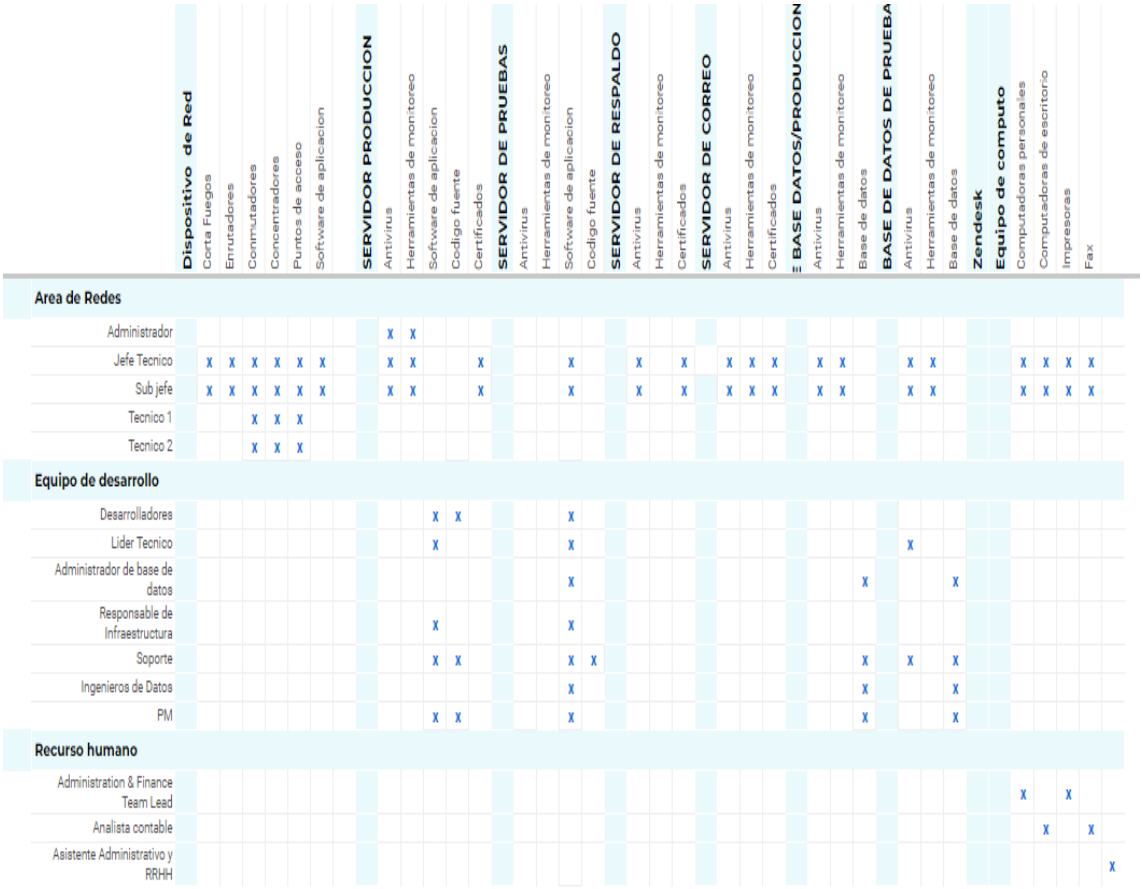
los datos poseen una etiqueta más baja que la etiqueta del usuario entonces el acceso es permitido, las etiquetas de los datos se pueden clasificar desde las más altas siendo estas públicas y las más altas aquellas privadas y confidenciales.

El control de acceso basado en roles se define por el papel del individuo dentro de la organización, este tipo de acceso es recomendado en organizaciones donde el personal cambia frecuentemente.

Al identificar los roles que existen dentro de la organización se debe listar el equipo físico, aplicaciones, bases de datos, respaldos, servidores o ambientes que figuran con información sensible y crítica, seguidamente se debe definir los permisos y accesos que serán asignados a los roles que se han identificado, esta última fase se debe analizar, corregir y controlar periódicamente. Los niveles de acceso se deben definir desde el acceso solo de lectura hasta el acceso total dependiendo del rol. El control de acceso también incluye diseñar y aplicar protección física contra desastres naturales, ataques o accidentes.

Figura 7.

Matriz de control de acceso



	Dispositivo de Red							SERVIDOR PRODUCCION					SERVIDOR DE PRUEBAS					SERVIDOR DE RESPALDO					SERVIDOR DE CORREO					BASE DATOS/PRODUCCION				BASE DE DATOS DE PRUEBA				Zendesk	Equipo de computo				
	Corta Fuegos	Enrutadores	Conmutadores	Concentradores	Puntos de acceso	Software de aplicacion		Antivirus	Herramientas de monitoreo	Software de aplicacion	Codigo fuente	Certificados	Antivirus	Herramientas de monitoreo	Software de aplicacion	Codigo fuente	Antivirus	Herramientas de monitoreo	Certificados	Antivirus	Herramientas de monitoreo	Certificados	Antivirus	Herramientas de monitoreo	Base de datos	Antivirus	Herramientas de monitoreo	Base de datos	Computadoras personales	Computadoras de escritorio	Impresoras	Fax
Area de Redes																																						
Administrador								X	X																													
Jefe Tecnico	X	X	X	X	X	X		X	X			X			X			X		X			X	X	X				X	X			X	X	X	X	
Sub jefe	X	X	X	X	X	X		X	X			X			X			X		X			X	X	X				X	X			X	X	X	X	
Tecnico 1			X	X	X																																	
Tecnico 2			X	X	X																																	
Equipo de desarrollo																																						
Desarrolladores										X	X				X																							
Lider Tecnico										X					X																X							
Administrador de base de datos															X										X			X										
Responsable de Infraestructura										X					X																							
Soporte										X	X				X	X									X	X		X										
Ingenieros de Datos															X										X			X										
PM										X	X				X										X			X										
Recurso humano																																						
Administration & Finance Team Lead																																				X		X		
Analista contable																																					X		X	
Asistente Administrativo y RRHH																																								X

Nota. Matriz de acceso basada en roles. Elaboración propia, realizado con Excel.

5.3. Análisis de riesgo

El análisis de riesgo busca analizar aquellas actividades que dentro de la red pueden estar expuestas a un riesgo, este análisis da como resultado medidas de seguridad que se desean aplicar con el fin de prevenir y mitigar los daños. Al identificar los activos de la organización y definir los controles de acceso la norma ISO 27005 recomienda valorizar el riesgo en la seguridad de la información, al

realizar un análisis de riesgo, se persigue determinar el cómo, dónde y por qué podría ocurrir una pérdida, concienciar a los todos los interesados de la existencia de los riesgos a los cuales está expuesta una red y la necesidad de gestionar los riesgos, esto evita la improvisación y abusos que se pueda dar por parte de quien pueda tener el control. El análisis de riesgo conlleva identificar las amenazas y vulnerabilidades, evaluación del riesgo que estas provocan para establecer una estimación cualitativa y cuantitativa.

5.3.1. Identificación de vulnerabilidades y amenazas

La identificación de vulnerabilidades están asociados a los activos de la organización y los tipos de amenazas están representados en 3 grupos propuestos por la ISO 27005 siendo estas, las amenazas deliberadas; siendo algunas de estas la saturación del sistema, espionaje remoto o el uso no autorizado del *hardware*, las amenazas accidentales aquellas que se dan por descuido o las producidas por factores que pueden afectar el funcionamiento de la red, como la pérdida del suministro de energía eléctrica, saturación del búfer del servidor y el daño físico del equipo de red, y las amenazas de entorno son originadas por en el medio ambiente, inundaciones, y la infraestructura estas amenazas provocan daño en el equipo físico que conforma la red.

Tabla 5.

Identificación de vulnerabilidades y amenazas

Tipos	Ejemplos de vulnerabilidad	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información.
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
Software	Configuración incorrecta de parámetros. Fechas incorrectas,	
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.	Error en el uso
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Falta de copias de respaldo	Manipulación con *software*
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del *software*
	Abuso de privilegios de acceso	Abuso información privilegiada y actos no autorizados
	Alteración de la información	Ataque interno/ externo
	Denegación de servicio	Sistemas automatizados y código malicioso

Continuación de la tabla 5.

Tipos	Ejemplos de vulnerabilidad	Ejemplos de amenazas
Red	Falta de prueba del envío o la recepción de mensajes	Negación de acciones
	Tráfico sensible sin protección y Líneas de comunicación sin protección	Escucha subrepticia
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones.
	Arquitectura insegura de la red y transferencia de contraseñas autorizadas	Espionaje remoto
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Errores de configuración	Fallos en el sistema y en el medio ambiente
	Caída del sistema por sobrecarga	Fallos en el sistema
Personal	Entrenamiento insuficiente en seguridad, uso incorrecto de *software* y *hardware*	Error en el uso
	Falta de conciencia acerca de la seguridad	
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos.
	Ingeniería social	Ataque interno/externo

Continuación de la tabla 5.

Tipos	Ejemplos de vulnerabilidad	Ejemplos de amenazas
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible a inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía.
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo
Organización	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	
	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	
	Falta de procedimientos de identificación y evaluación de riesgos	

Nota. Ejemplos de algunas vulnerabilidades tomadas del Anexo D de la norma ISO 27005. Elaboración propia, realizado con Excel.

5.3.2. Valoración de riesgo e impacto

La valoración del riesgo está dada por la relación de la probabilidad y el riesgo de ocurrencia sobre los activos de la organización, en donde los involucrados deberán valorar las amenazas y vulnerabilidades con base al conocimiento y la experiencia en que se pueden ver afectados los activos y el impacto que provocaría al presentarse algunas de estas amenazas.

Tabla 6.

Escala de valoración de probabilidades de ocurrencia

Escala de valoración	Valoración	Rango- tiempo
1	Muy baja	Una vez al año
2	Baja	Dos veces al año
3	Media	Una vez cada 2 meses
4	Alta	Una vez a la semana
5	Muy alta	Una vez al día

Nota. Escala de probabilidades de ocurrencia con relación a la ocurrencia en un tiempo determinado. Elaboración propia, realizado con Excel.

5.3.2.1. Valoración de impacto

La identificación de las amenazas y vulnerabilidades de la tabla 4 se deben valorar en el sentido de probabilidad que estas se materialicen con respecto a la frecuencia de ocurrencia.

Tabla 7.

Escala numérica de valoración según el impacto

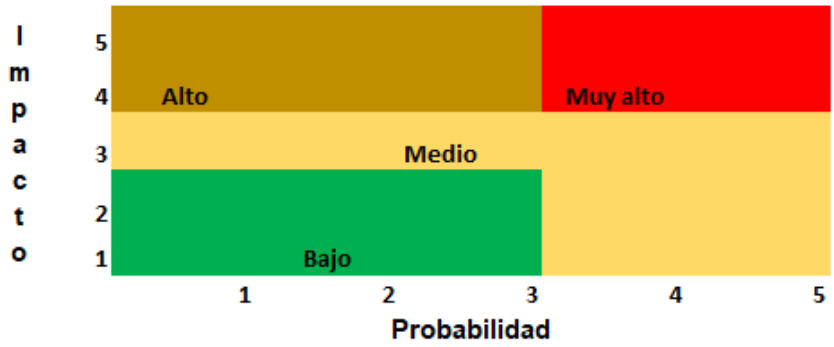
Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día a nivel de confidencialidad, disponibilidad e integridad	5
Frecuencia alta	1 vez cada 1 semana a nivel de C.I.D	4
Frecuencia media	1 vez cada 2 meses a nivel de C.I. D	3
Frecuencia baja	1 vez cada 6 meses a nivel de C.I. D	2
Frecuencia muy baja	1 vez al año a nivel de C.I. D	1

Nota. Escala de valoración frecuencial de amenazas, a nivel de disponibilidad, confidencialidad e integridad. Elaboración propia, realizado con Excel.

Lasso (2015), expresa que la valoración impacto potencial, es una medida sobre los activos al materializarse una amenaza y se calcula con la valoración de los activos de las tablas 2 y 3. En cambio la valoración riesgo potencial se calcula sobre el impacto por dimensión y la frecuencia de amenaza.

Figura 8.

Escala valoración del riesgo



Nota. Escala valoración del riesgo. Obtenido de C. Lasso (2015). *Auditoría en seguridad informática en base de datos del grupo de trabajo de infraestructura y soporte de tecnologías de la información del departamento para la prosperidad social*. (p. 109.).

Al consultar con conocedores en la materia sobre el impacto de las vulnerabilidades y amenazas a las que se expone día con día la red LAN de una organización se tomaron como relevantes las siguientes, al mismo tiempo estas nos conducen a los impactos descritos en la Norma ISO 27005.

Figura 9.

Valoración impacto y riesgo

		Valoracion Impacto potencial			Valoracion riesgo potencia		
Activo/Amenaza	**Frecuencia de amenaza**	**C**	**I**	**D**	**C**	**I**	**D**
Hardware/Perdida del suministro de energia	2	2	0	3	Bajo		Medio
Software/ Denegación de servicio	2	3	2	4	Medio	Bajo	Alto
Red/ Caida del sistema por sobrecarga	3	3	1	4	Medio	Bajo	Alto
Identificacion de amenazas, Tabla 4.	*Ver tabla 5*	*Ver tabla 3*	*Ver tabla 4*	*Ver tabla 2*	*Valores dados por la relacion entre impacto y la frecuencia de la amenaza. Figura 8*		

Nota. Valoración impacto y riesgo. Obtenido de C. Lasso (2015). *Auditoría en seguridad informática en base de datos del grupo de trabajo de infraestructura y soporte de tecnologías de la información del departamento para la prosperidad social*. (p. 99.).

5.4. Política de seguridad de la información

La creación de esta política busca proporcionar un panorama claro de tipo orientativo y de apoyo para gestionar la seguridad de la información, según el giro de negocio, normas y leyes internas de la organización. La política de seguridad debe tomar en cuenta las políticas internas, normas, contratos y leyes con las que cuenta la organización además de plantear objetivos alcanzables para poder orientar todas las actividades concernientes a la seguridad de la información.

Dentro de esta política se deben asignar responsabilidades específicas y generales en la gestión de la seguridad de la información para los roles definidos. Esta política se enfoca en temas a nivel general, además de apoyarse en políticas sobre temas específicos como las políticas preventivas tales como la gestión de

vulnerabilidades técnicas, controles criptográficos, protección ante *software* malicioso, establecer controles de acceso, manejo adecuado de los activos, copias de seguridad, restricciones de instalación y uso de *software*, todo lo concerniente al usuario final, como uso adecuado del correo electrónico.

5.4.1. Política de control de acceso

La política de control de acceso debe asegurar que el acceso a la información esté controlado, así como las aplicaciones y los accesos a cada uno de los dispositivos de red. Al definir esta política se deben tomar en cuenta los siguientes aspectos:

- Definir el ente que suministre las claves y los usuarios con acceso a los servicios de red.

- Definir y autorizar que los usuarios podrán instalar *software* o *hardware* en los equipos que conforman la red.

- Registrar y auditar los accesos remotos a través de conexiones seguras.

- Creación y revocación de los usuarios en los sistemas y dispositivos de red.

- Gestionar contraseñas seguras para usuarios, definiendo el tiempo de durabilidad de esta.

- Definir los caracteres permitidos para actualizar las contraseñas.

- Se debe definir el tiempo de revisión de los accesos cada vez que haya cambio en el personal.

5.4.2. Política de organización interna

Esta política debe garantizar el soporte operativo para todas aquellas actividades de la seguridad de la información.

Definir los roles de los accesos y responsabilidades de los colaboradores internos y externos que accedan a la infraestructura de la organización, de los activos definidos deberán asignarse a los colaboradores internos siendo estos los responsables de proteger la integridad, disponibilidad y confidencialidad, así como también de darle el uso adecuado, esta política va de la mano con la política de control de acceso.

5.4.3. Política de clasificación de la información

La clasificación de la información debe ir de acuerdo con los niveles de acceso, público, interno, confidencial y reservado para ello es importante tomar en cuenta los roles definidos en la política de organización interna. Se debe mantener un registro de los receptores de la información, restringir el acceso y otorgarlo sólo a los usuarios designados, mantener todos los activos útiles para el almacenamiento de la información en un ambiente seguro.

Cada usuario designado al acceso de la información deberá asegurar su conservación, no ocasionar daños, manejo inadecuado, no permitir alteraciones, pérdidas o consultas realizadas por usuarios no autorizados de acuerdo con la responsabilidad que le fue designada.

5.4.4. Política de gestión de medios de almacenamiento

Todas las unidades de almacenamiento y dispositivos removibles útiles para el almacenamiento de la información deberán ser asignado a un colaborador, estos activos deberán ser utilizado exclusivamente para el resguardo de la información y deberán ser conectados solo a los dispositivos electrónicos definidos, estos a su vez deben ser monitoreados, al ser utilizados deberán ser resguardados en un ambiente seguro. Al darse de baja o reclasificado deberá seguir un proceso de borrado seguro, dentro de esta política se debe especificar el procedimiento de destrucción apropiado definido por la Junta directiva.

5.5. Política de prevención

Para poder mitigar las vulnerabilidades identificadas es necesario establecer políticas de seguridad preventiva en todos los recursos que forman parte de la infraestructura de red, esto incluye mantenimiento de equipo físico y del *software*, realizar escaneos periódicamente y documentar, al igual que realizar monitoreos de seguridad, así como lo sugiere el estándar O-ISM3.

5.5.1. Política de uso de controles criptográficos

Esta política busca garantizar y proteger la integridad, disponibilidad y confidencialidad de la información a través de la aplicación de controles criptográficos.

Aquí se debe definir las técnicas criptográficas y herramientas que garanticen la integridad, disponibilidad y confiabilidad de la información, las herramientas elegidas se deben ajustar a las necesidades de la organización.

Garantizar que los controles definidos no obstaculicen otros controles de filtrado como el filtrado *web*, *antimalware* y *antispyware*. Además, se deben definir los procedimientos para la gestión de llaves públicas o privadas y comunicar los procedimientos a los interesados.

5.5.2. Política de respaldo

La política de respaldo busca asegurar la información que se resguarda en medios de almacenamiento externo y que cumpla con los principios de la seguridad.

- Se debe garantizar que los respaldos se realicen de manera periódica con las disposiciones de seguridad acordadas.

- Las copias de seguridad deberán de tener un control de acceso, almacenadas en un lugar seguro libre de amenazas físicas y cibernéticas

- Realizar revisiones periódicas de los respaldos de tal manera que estos se puedan restaurar correctamente.

- Definir el tipo de respaldo según las necesidades de la organización.

5.5.3. Política de gestión de vulnerabilidades técnicas

El objetivo de esta política es proporcionar técnicas para la prevención o reducción de posibles amenazas que se pueden dar.

- Identificar las amenazas, por ejemplo, las descritas en la tabla 7 formular un plan de monitoreo según las amenazas encontradas.

- Realizar un reporte de actualizaciones a instalar en el *software.*

- Contratar herramientas de seguridad como antivirus, *antimalware*, entre otros.

- Reportar a los usuarios las posibles vulnerabilidades de los activos que tienen a su cargo, y guiarlos en la implementación de la solución o tratamiento antes o después del ataque.

- Definir el ente encargado de instalar cualquier tipo de *software* en los dispositivos de red y en el equipo de cómputo.

- Verificar el licenciamiento del *software* y aplicaciones instaladas en los equipos.

- La administración remota del equipo solo podrá realizarse por personal autorizado

- Mantener al día las actualizaciones de los programas o aplicaciones utilizados.

Esta política va de la mano con la política de uso del internet, ya que existe una alta probabilidad que los ataques se den fuera de la red.

5.5.4. Política de uso de internet

Mediante esta política se busca proteger la información en el uso adecuado del servicio de internet por los usuarios.

- Fomentar entre los colaboradores el uso adecuado del internet, evitando malas prácticas que puedan poner en riesgo la seguridad de la información.

- Usar el servicio para envío y descarga de información permitida.

- Revisar y vigilar que el uso del servicio de internet sea el adecuado.

- Cada usuario con acceso al servicio de internet será el responsable de la información que envíe o descargue.

- No se debe permitir descargas realizadas desde sitios poco fiables, como música, películas, juegos, imágenes, películas o archivos ejecutables.

- Monitorear y evaluar las actividades y páginas visitadas por los usuarios que presenten un comportamiento sospechoso.

- Filtrar el contenido que ingrese o que se envíe desde la red.

5.5.5. Política de protección contra código malicioso

Esta política busca establecer medidas de prevención y detección frente a las amenazas que son causadas por código malicioso, entre ellas están:

- Tener un sistema de detección de intrusos, herramientas antispam, antivirus y sistemas de control de navegación con el fin de que no se ejecuten virus o gusanos en los dispositivos de red.

- Instalar programas para analizar y verificar código malicioso, virus, gusanos, troyanos en los equipos y a nivel de red.

- Las herramientas definidas para la detección deberán ser instaladas por el ente definido.

- Mantener las actualizaciones de las herramientas de protección al día.

- Instalar y actualizar los parches creados para los sistemas operativos, motores de detección, bases de datos y para el *software* instalado del lado del servidor y del cliente.

- Crear controles para detectar y restringir el código malicioso o virus provenientes de descargas no autorizadas, sitios *web* de dudosa reputación, archivos infectados en dispositivos de almacenamiento externo y contenido infectado en correos electrónicos.

- No permitir que usuarios sin autorización puedan desinstalar o desactivar las herramientas para la detección y protección contra virus, código malicioso o troyanos.

- Realizar actividades prácticas sobre lectura de correos con archivos adjuntos infectados o links de sitios dudosos.

- Definir el filtrado del tráfico de sitios poco fiables, mediante la implementación de un proxy u otra herramienta de *software*.

5.5.6. Política de seguridad física

Esta política se centra en proteger todo el *hardware* que conforma la red de la organización.

- Definir los mecanismos de protección a los dispositivos de red, como por ejemplo usar tarjetas de acceso al área de red de la organización.

- Supervisar y registrar a todos los usuarios autorizados que ingresen al área de red.

- Definir las medidas de protección física y eléctrica para el equipo de red.

- Proteger la infraestructura de red mediante contratos de soporte y mantenimiento.

- Llevar un control o inventario de todo el equipo físico.

- Definir un control de seguridad con el equipo que deba retirarse de las instalaciones de la organización.

5.5.7. Política de gestión de seguridad de la red

Esta política busca proteger la información que viaja a través de la red interna y a través de la conexión hacia terceros.

- Controlar el acceso a la red mediante la segmentación a través de vlans.

- Mantener un control de conexiones a la red mediante la dirección MAC de los equipos.

- Controlar el acceso a servidores mediante el uso de claves.

- Acceso remoto a los servicios mediante el uso de VPNs, túneles encriptados.

- Acceso interno a los servicios mediante listas de acceso.

- Establecer tiempos de conexión en los equipos de red como corta fuegos, enrutadores, conmutadores o servidores.

- Definir usuarios y roles para el acceso a los equipos de red.

5.6. Política de respuesta

Una respuesta es la acción ante una posible amenaza o ataque, al no tener una política de respuesta de seguridad se produce un retraso en el cual la red está expuesta a una violación de la seguridad. En esta política se debe establecer una lista de prioridades ante el ataque, plan correctivo, evaluación e identificación del grado de violación, y llevar un registro en la bitácora.

5.6.1. Lista de prioridades

Una lista de prioridades está conformada por los dispositivos de red y por el equipo informático, estos son variables ya que dependen de la infraestructura con la que la organización cuenta y de los servicios que ésta ofrece.

Entre los equipos que son de prioridad alta ante cualquier ataque se registran; los equipos de comunicación como los enrutadores, conmutadores y los cortafuegos, servidores de bases de datos, y los servidores que se utilizan para resguardar las copias de seguridad. El equipo considerado de prioridad media son los servidores de directorio activo, servidores de correo y el equipo de prioridad baja es todo el equipo de informática que los usuarios de la organización utilizan.

5.6.2. Plan correctivo

Un plan correctivo involucra aquellas acciones que se deben de realizar en medio de un ataque, el objetivo es dar restablecer la continuidad a los servicios que ofrece la organización, definir los roles antes los incidentes presentados a fin de actuar con orden y de manera eficaz.

Dentro del plan correctivo se encuentra la des habilitación de servicios y puertos que no son necesarios, monitorear la infraestructura de red con el fin de detectar y limitar el impacto de los efectos colaterales producidos por el ataque, bloquear la acción de la amenaza bloqueando dominios o direcciones IP, desconexión de equipos de la red para revisión, identificar el punto inicial del ataque, revisión de los sistemas y sitios que se sospecha que fueron atacados, servidores, copias de seguridad y ejecución de herramientas de escaneo.

Una de las formas de determinar un ataque es mantener en constante monitoreo el tráfico de la red, revisando registros sospechosos e inusuales, aumento de archivos sospechosos, presencia de ventanas emergentes de publicidad donde no debería de existir.

5.6.3. Evaluación e identificación del grado de violación

Aquí se valoran los daños con toda la información recopilada del ataque, esto se debe realizar con el menor tiempo posible ya que se debe contener el daño y evitar que se propague y comprometa la integridad de la información y de todos los dispositivos de red, ya que es necesario recuperar aquellos dispositivos comprometidos.

El grado de identificación de los servicios comprometidos busca perfilar cada uno de estos:

- Grado 1. Aplicación con tolerancia mínima que requiere recuperarse de forma inmediata (8 horas).

- Grado 2. aplicación que debe levantarse en menos de 12 horas después de la declaración del desastre.

- Grado 3. Aplicación que puede levantarse en menos de 24 horas.

- Grado 4. Aplicación que puede levantarse después de 24 horas.

5.6.4. Registros del ataque

Una vez se resuelva el ataque y se garantice que el incidente ha sido resuelto, se deben reactivar los servicios y equipo , esto conlleva realizar nuevas copias de seguridad, cambio de contraseñas en los equipos, servidores y servicios, monitorear la red, instalar antivirus y herramientas de seguridad, además de elaborar un informe final en el que se detalle el tipo de ataque, los servicios y equipos comprometidos, posibles vulnerabilidades que dieron origen

al ataque con el fin de corregir, parchar y mejorar la seguridad de la infraestructura de la red.

5.7. Mejora continua

Se define mejora continua como una actividad repetitiva cuyo fin es aumentar la capacidad de los procedimientos y controles sobre la base de los resultados identificando oportunidades de mejora donde se busca la eficiencia y eficacia de los recursos utilizados.

Dependiendo del nivel de madurez que tenga la organización en cumplir con sus políticas de seguridad, así se propone la mejora continua es decir al medir el logro de sus políticas se establecerán nuevos tiempos de escaneo, un mejor control sobre el control de accesos y la documentación.

El protocolo O-ISM3 es una buena referencia para implementar por primera vez un Sistema de Gestión de Seguridad ya que se enfoca en los objetivos de la seguridad y calidad con los objetivos del negocio, además de mejorar la disponibilidad de los servicios que la organización ofrece con el fin de gestionar de manera continua la seguridad a la red, este marco propone procesos de seguridad según el modelo de seguridad O-ISM3. En este capítulo se propone un modelo de seguridad según el definido por The Open Group, este modelo de madurez parte del área de IT.

5.7.1. Objetivos del negocio

Los objetivos del negocio se entrelazan con los objetivos de seguridad.

5.7.1.1. Gestión del conocimiento

Este proceso busca recopilar información referente a la seguridad de la información, con el fin de manejar información actualizada sobre nuevas amenazas en el área de tecnología, asegurando que los procesos se realicen de la forma correcta.

Este proceso se debe implementar en el área de sistemas y recursos humanos, mediante reuniones y capacitaciones donde el personal de TI es quien exponga la manera de realizar los procesos y procedimientos correctos.

5.7.1.2. Diseño y evolución de la gestión de seguridad de la información

En esta sección se busca seleccionar los procesos estratégicos para lograr el objetivo de la seguridad, analizar el nivel de madurez actual para luego elaborar un modelo de madurez, el propietario de este proceso es el personal de TI.

5.7.2. SSP-1 informes

El personal de TI es el encargado de informar mediante reuniones semestrales sobre el cumplimiento de la implementación del modelo de madurez para la toma de decisiones en temas de seguridad por parte de la gerencia.

5.7.3. SSP-2 coordinación

Este proceso busca establecer una buena comunicación entre el área de TI y el área encargada de la implementación del modelo O-ISM3, las

herramientas utilizadas para gestionar la comunicación quedan a discreción de las partes interesadas.

5.7.4. SSP-6 asignar recursos para la seguridad de la información

Este proceso busca brindar recursos monetarios, de personal e instalaciones para que los procesos que lo necesiten se ejecuten de manera ininterrumpida.

5.7.5. Objetivos de seguridad

Dentro de los objetivos de seguridad según el modelo de seguridad de O-ISM se detalla un plan bien elaborado partiendo de lo que se tiene hacia dónde se quiere llegar.

5.7.5.1. TSP-1 reporte a gerencia

Este proceso tiene con fin presentar un reporte periódicamente sobre la seguridad de la información y sobre la asignación de recursos, este reporte debe contemplar actualizaciones en el detalle de los activos y la operatividad de estos, distribución de licencias y actualizaciones de *software*.

5.7.5.2. TSP-2 administrar los recursos

En este proceso se debe elaborar un presupuesto anual sobre los costos que implican mantener la seguridad de la información, esto incluye renovación de equipo, licencias y actualizaciones y mantenimiento operativo, al mismo tiempo

se debe tener un control sobre la distribución de los recursos para asegurar la correcta gestión de la seguridad de la información.

5.7.5.3. TSP-3 definir objetivos de seguridad

Este proceso debe definir lo que se desea lograr dentro del dominio administrado por TI, tomando como base el modelo de seguridad O-ISM3, brindar soporte adecuado ante algún incidente de seguridad, y asegurar los principios de la seguridad del sistema de información.

5.7.6. Procesos ISM3

Los procesos ISM3 son un conjunto de operaciones que se ajustan a las necesidades de la organización dependiendo de las necesidades de ésta.

5.7.6.1. OSP-5 parcheo de dominio administrativo por TI

Este proceso se debe realizar de manera continua la cual incluye actualizaciones del sistema y de sistemas operativos con el fin de prevenir posibles vulnerabilidades, tener en cuenta que las actualizaciones pueden generar fallas que afectan la disponibilidad de la información por lo que se deben crear respaldos antes de las actualizaciones realizadas.

5.7.6.2. OSP-10 gestión de copias de seguridad

Este proceso busca que se realicen copias de seguridad periódicas de servidores, sistemas, código fuente, bases de datos y servidor de archivos, el tipo de copia de seguridad debe estar definido en la política de respaldo.

5.7.7. OSP-11 control de accesos

Este proceso debe de verificar el acceso a la información digital o física, sea accedida por personal autorizado, así como a los dispositivos de red y servidores.

5.7.8. OSP-12 registro de usuarios

Este proceso cubre la gestión de registro de usuarios, creación, modificación y baja según los niveles de acceso definidos en la política de control de accesos.

5.7.9. OSP-14 gestión de protección del medio ambiente

Este proceso cubre la gestión de registro de usuarios, creación, modificación y baja según los niveles de acceso definidos en la política de control de accesos.

5.7.10. OSP-17 gestión de protección contra *malware*

Este proceso busca implementar y ejecutar reglas de seguridad contra malware, haciendo uso de las herramientas existentes dentro de la organización o instalando las necesarias para resguardar la integridad de la información.

5.7.11. OSP-21 calidad de la información y sondeo de cumplimiento

En este proceso se debe realizar una evaluación trimestral de la información y de los procesos implementados. Con la información obtenida se debe establecer el nivel de madurez que la organización ha alcanzado.

5.8. Modelo de madurez

El nivel de madurez es un método para establecer el nivel en el que se encuentra una organización en los procesos de seguridad de la información.

COBIT propone 5 niveles para evaluar la madurez de los procesos implementados.

- 0 – no se aplican procesos
- 1 – los procesos que existen están desorganizados
- 2 – los procesos siguen un patrón regular
- 3 – los procesos se documentan y se comunican
- 4 – los procesos se monitorean y se miden
- 5 – las buenas prácticas se siguen y se automatizan

Además, establece criterios para definir esos niveles basados en los siguientes atributos:

- Conciencia y comunicación (CC), es el grado de conciencia respecto a los objetivos del negocio

- Políticas, estándares y procedimientos (PP); este atributo busca entender el nivel de seguridad sobre los activos definidos, si se tienen políticas, estándares o procedimientos para proveer seguridad a la red.

- Herramientas y automatización (HA), entender si existen herramientas estandarizadas de apoyo a los procesos existentes

- Responsabilidad y rendición de cuentas (RE), entender el nivel de compromiso para cada involucrado en el área de TI

- Establecimiento y medición de metas (ME), determinar si se implementan herramientas o sistemas de medición de desempeño de los procesos

- Habilidades y experiencia (HE), entender si se conocen y se tienen las habilidades necesarias en el área de seguridad.

CONCLUSIONES

1. Las políticas de seguridad son pautas que ayudan a mejorar la seguridad de la información, estas no aseguran que exista un entorno 100 % libre de amenazas y ataques.

2. Crear una cultura de seguridad entre los colaboradores de la organización para que se puedan crear políticas claras y cuyo objetivo esté enfocado en los objetivos de la organización.

3. Los procesos que se manejen o implementen deben ser conocidos por todos los colaboradores.

4. La familia de estándares ISO/IEC 27000 son un conjunto de buenas prácticas para la gestión de seguridad de la información que abarcan todo el ciclo de vida de una política de seguridad.

5. El análisis de riesgo busca identificar las vulnerabilidades y amenazas a las que está expuesta la red de una organización, y con base a este análisis se busca establecer una valoración del impacto y riesgo potencial de cada una de estas.

6. El protocolo O-ISM3 es una buena referencia para implementar un modelo de seguridad de la información.

7. El modelo de madurez es un método repetitivo que se debe realizar antes y después de crear e implementar las políticas de seguridad.

RECOMENDACIONES

1. Contar con la absoluta colaboración y participación de la alta gerencia ya que ellos pueden contratar asesores en el tema de seguridad y con ello capacitar a los colaboradores.

2. Revisar todo lo elaborado por los colaboradores de la mano de un experto en el tema o bien alguien que tenga experiencia en el tema de seguridad.

3. Identificar activos o amenazas pueden variar según la valoración que la organización le dé, al igual que la valoración de probabilidad de ocurrencia ya que esto dependerá de las experiencias pasadas o la ocurrencia con que se hayan dado.

4. Crear políticas claras, fáciles de alcanzar y de fácil comprensión para los colaboradores, ajustándose a las políticas existentes.

5. Documentar las políticas creadas y establecer periodos de revisión al estarlas creando, así mismo establecer periodos de evaluación y cumplimiento de estas y aplicar sanciones en caso de que no se cumplan.

REFERENCIAS

Baltazar, J., y Campuzano, J., (2011). *Diseño e implementación de un esquema de seguridad perimetral para redes de datos. Caso práctico: Dirección General del Colegio de Ciencias y Humanidades.* [Tesis de Pregrado, Universidad Nacional Autónoma de México]. Archivo digital. https://ru.dgb.unam.mx/handle/20.500.14330/TES01000669103

Cifre, S. (2018). *Marco de trabajo estructurado para la seguridad de la información en servidores Web basado en estándares internacionales.* [Tesis de especialización, Universidad Tecnológica Nacional]. Archivo digital. https://ria.utn.edu.ar/handle/20.500.12272/5964

Cisco. (12 de marzo de 2023). *¿Qué es la seguridad de red? https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#:~:text=La%20seguridad%20de%20red%20es%20cualquier%20actividad%20dise%C3%B1ada,red%20eficaz%20administra%20el%20acceso%20a%20la%20red.*

Lasso, C. (2015). *Auditoría en seguridad informática en base de datos del grupo de trabajo de Infraestructura y soporte de tecnologías de la información del departamento para la prosperidad social – DPS – de Bogotá, sede principal.* [Tesis de Especialización, Universidad Abierta y a Distancia]. Archivo digital. https://repository.unad.edu.co/handle/10596/3717

Stallings, W. (2004). *Comunicaciones y Redes de Computadores.* Pearson Prentice Hall. http://biblioteca.univalle.edu.ni/files/original/85855280ef3d43c77781a423a892de58d36aae0a.pdf

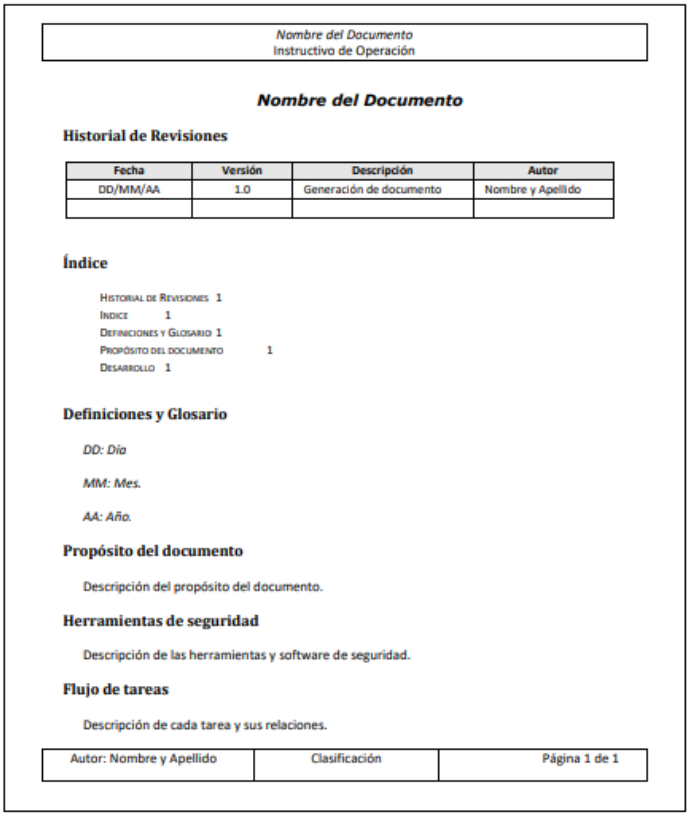
Tanenbaum, A., & Wetherall, D., (2012). *Redes de Computadoras.* Pearson Educación. https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf

Vieites, Á. G. (2013). *Auditoria de seguridad informática.* Editorial RA-MA.

ANEXOS

Anexo 1.

Formato de documentos de instructivos de operación



Nombre del Documento
Instructivo de Operación

Nombre del Documento

Historial de Revisiones

Fecha	Versión	Descripción	Autor
DD/MM/AA	1.0	Generación de documento	Nombre y Apellido

Índice

Definiciones y Glosario

DD: Día

MM: Mes.

AA: Año.

Propósito del documento

Descripción del propósito del documento.

Herramientas de seguridad

Descripción de las herramientas y software de seguridad.

Flujo de tareas

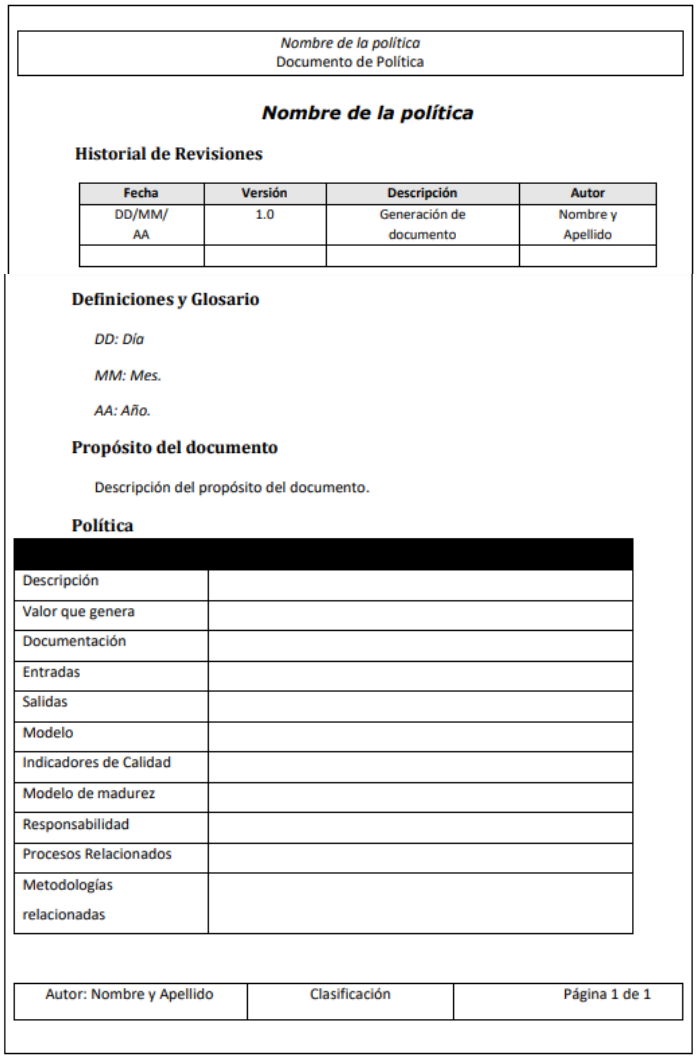
Descripción de cada tarea y sus relaciones.

Autor: Nombre y Apellido	Clasificación	Página 1 de 1

Nota. Propuesta de la estructura para la realización de documentos de instructivos de operación. Obtenido de S. Cifre (2020). *Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas* [Tesis de maestría, Universidad Tecnológica Nacional]. (p. 55). Archivo digital. https://ria.utn.edu.ar/xmlui/bitstream/handle/20.500.12272/6050/Tesis%20de%20Maestri%cc%81a%20-%20Cifre%20Simo%cc%81n.pdf?sequence=1&isAllowed=y

Anexo 2.

Plantilla documento de política



Nombre de la política
Documento de Política

Nombre de la política

Historial de Revisiones

Fecha	Versión	Descripción	Autor
DD/MM/ AA	1.0	Generación de documento	Nombre y Apellido

Definiciones y Glosario

DD: Día

MM: Mes.

AA: Año.

Propósito del documento

Descripción del propósito del documento.

Política

Descripción	
Valor que genera	
Documentación	
Entradas	
Salidas	
Modelo	
Indicadores de Calidad	
Modelo de madurez	
Responsabilidad	
Procesos Relacionados	
Metodologías relacionadas	

Autor: Nombre y Apellido	Clasificación	Página 1 de 1

Nota. Propuesta de la realización de un documento de Política de seguridad. Obtenido de S. Cifre (2020). *Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas* [Tesis de maestría, Universidad Tecnológica Nacional]. (pp. 51-52). Archivo digital. https://ria.utn.edu.ar/xmlui/bitstream/handle/20.500.12272/6050/Tesis%20de%20Maestri%cc%81a%20-%20Cifre%20Simo%cc%81n.pdf?sequence=1&isAllowed=y