MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Uso de da Red e Internet

Proceso:

Gestión de Servicios de Información y Soporte Tecnológico

Versión 02

20/10/2022

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente documento especifica los lineamientos mínimos para la implementación de controles necesarios para respaldar y asegurar la operación de la red en el **Ministerio de Ambiente y Desarrollo Sostenible (ENTIDAD)**, permitiendo fortalecer mediante un proceso de mejora continua la prestación de servicios de red.

Se establece el uso de internet como herramienta de trabajo y a su vez caracterizar los diferentes usuarios que pertenecen al Ministerio, con el propósito de definir permisos de accesibiliad de acuerdo a la clasificación de cada grupo de usuarios.

GUIA DE RED DE DATOS DEL MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

1 OBJETIVO

Establecer y divulgar los lineamientos a implementar para fortalecer a nivel institucional, el servicio de red y navegación hacia internet de los usuarios de la Entidad, instaurando las condiciones de uso para un manejo correcto, efectivo y responsable, dentro de un marco de legalidad.

2 ALCANCE

Aplica a toda la infraestructura de red corporativa del Ministerio de Ambiente y Desarrollo Sostenible. Inicia con la definición de los diferentes grupos de usuarios caracterizados en el área de Infraestructura y termina en la desabilitacion de cada cuenta cuando el usuario (Funcionario o Contratista) termina su vinculo laboral con la Entidad.

3 BASE LEGAL

- Ley 1581 de 2012, dicta disposiciones para la protección de datos personales, la cual tiene como objeto "desarrollar el derecho constitucional que tiene todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos…"
- Ley 527 de 1999, Define y reglamenta el acceso y uso de mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen en las entidades de certificación.
- Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1032 de 2006 (derechos de autor y conexos), Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital en Colombia - DNP
- Decreto 1078 de 2015, expide el decreto único reglamentario del sector de las TIC y de la Estrategia de Gobierno Digital

• ISO 27001/2013, Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo Integrado de Planeación y Gestión (MIPG).

4 RED SEGURA

La seguridad de las redes es una parte integral de las redes informáticas que hace referencia a protocolos, tecnologías, dispositivos, herramientas y técnicas que aseguran los datos y la infraestructura informática para prevenir o mitigar las amenazas y riesgos de acceso o mal uso de los recursos referidos.

La seguridad en las redes es implementada para proveer un marco donde los funcionarios, contratistas y demás colaboradores, realizan su trabajo diariamente en un entorno seguro. Por lo cual se hace necesario considerar tres elementos fundamentales según Figura 1.

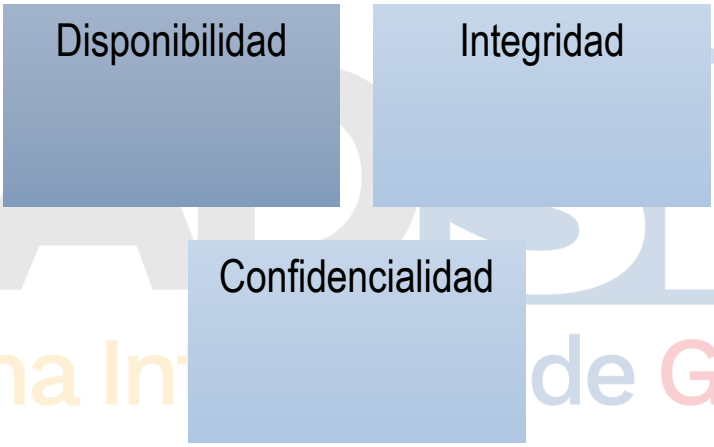

Figura 1. Pilares de la seguridad de la información Fuente: Elaboración propia

Para mejorar la seguridad de la información en la red, uno de los elementos fundamentales a tener en cuenta es el cumplimiento de los 3 pilares de la seguridad de información. A continuación, se describen cada uno de ellos y los aspectos para tener en cuenta en la red del ENTIDAD.

4.1 DISPONIBILIDAD

Define que la información esté disponible, accesible y utilizable para quienes estén autorizados a acceder a ella, así como la disponibilidad de los equipos la cual debe ser garantizada por el fabricante o proveedor.

4.1.1 Características

a. Los equipos que integran la infraestructura de TI deben poseer la robustez necesaria para respaldar la operación y ser de reconocida calidad.
b. Haber sido evaluados por un ente independiente y les haya otorgado una buena calificación (Por ejemplo, Gartner).
c. El equipo debe garantizar una robustez suficiente para que su tiempo medio de falla sea el mínimo posible (MTBF).
d. El fabricante debe garantizar que los equipos pueden operar 7x24x365.
e. El proveedor de servicio de red WAN e Internet debe garantizar una disponibilidad mínima del 99.9% al año[1].
f. Los dispositivos deben contar con soporte de fabricante para reemplazos, repuestos y soporte en general. Así, como la posibilidad de contar con consultorías que permitan adoptar buenas prácticas para optimizar el desempeño red.
g. Los contratos de soporte deben ajustarse a tiempos de respuesta moderados y acordes a los requerimientos del ENTIDAD.
h. Se debe contar con planes de continuidad de servicio en caso de:
    - Falla de Internet.
    - Falla de enlaces de subida (Centros de cableado a Datacenter)
    - Falla en los equipos activos. (Core ó Acceso)
    - Falla de los enlaces de Servidores.
    - Falla en las fuentes de alimentación de los equipos.
    - Falla de los enlaces de datos en general.
    - Falla en la red inalámbrica WIFI.
i. Contar con los recursos necesarios para ejecutar y mantener planes de continuidad.
j. Se debe verificar la estabilidad de la red después de cualquier implementación tecnológica en las instalaciones del ENTIDAD.
k. Contar con redundancia en:
    - Enlaces de datos: Todo enlace de datos hacia los dispositivos de comunicaciones, internet y hacia redes de terceros deben poseer por lo menos, un enlace adicional de respaldo en caso de falla.
    - Equipos: Los equipos de comunicación CORE y periféricos de red deben poseer por lo menos un equipo de respaldo que asuma la carga total de las comunicaciones en caso de falla.
    - Equipos de backup: Correspondientes a dispositivos de Acceso en caso de falla acordes con los planes de continuidad previamente definidos por la Entidad.
    - Energía eléctrica: Los equipos deben poseer como mínimo 2 fuentes de suministro eléctrico, respaldados por circuitos eléctricos independientes, soportados mediante UPS y planta eléctrica.

[1] Disponibilidad ofertada por Colombia Compra Eficiente, Anexo IT-C-CT-01 Enlaces Dedicados a Internet, Plan Plata.

l. Asegurar mediante copias periódicas las configuraciones de los dispositivos de red, los cuales deben integrarse fielmente a los planes de backups de la Entidad.
m. Asegurar un adecuado diseño, operación y cobertura de la red WIFI aumentando la disponibilidad de este servicio bajo un respaldo acorde a la infraestructura de TI.

4.2 INTEGRIDAD

Define que la información pueda ser modificada únicamente por las personas autorizadas y que la integridad de los equipos sea garantizada por el fabricante.

4.2.1 Características

a. Los equipos deben poseer la robustez necesaria y de reconocida calidad evaluadas por entes consultores de investigación en tecnologías de información independientes y les haya otorgado una buena calificación. Ejemplo: Gartner.
b. Garantizar y promover instalaciones adecuadas de cableado estructurado bajo los estándares nacionales e internacionales.
c. Los equipos deben ser instalados en su respectivo Rack de comunicaciones de acuerdo con las buenas prácticas recomendadas por los fabricantes.
d. Los racks de comunicaciones no deben mezclarse con dispositivos diferentes a los que permiten la comunicación de redes. (Servidores, call manager, cámaras. PC, KVM, etc.).
e. Los racks de comunicaciones deben tener una función definida y no mezclarla con otras, por ejemplo: el rack que recibe las últimas millas, no debe mezclarse con el rack que maneja los switch de borde. Se acepta colocar los switch de piso en el rack del switch CORE.
f. Los equipos deben estar instalados en un ambiente óptimo para su operación (Energía, Temperatura, Humedad, etc.), según las características técnicas de operación de los equipos entregadas por el fabricante.
g. El acceso físico a los dispositivos de red, se deben encontrar restringidos mediante el uso de control de acceso físico electrónico (tarjeta de proximidad, biométricos, cámaras, puertas de seguridad, etc.).
h. Se debe llevar un registro auditable del acceso al Data Center y centros de cableado.
i. El lugar destinado a los dispositivos de red debe contar con los elementos de prevención y control de incendios correspondiente.
j. El lugar destinado a los dispositivos de red se debe encontrar señalizado para correcta observación de los funcionarios, contratistas y colaboradores de la Entidad, como Área Restringida.
k. El lugar destinado a los dispositivos de red debe cumplir con la norma de sismo resistencia aplicable en Colombia.
l. Los rack donde se ubican los equipos de comunicaciones y cableado deben ser instalados de acuerdo a las buenas prácticas de estos entornos.

m. Mantener los equipos de red cubiertos con respaldo de fábrica por un tiempo mínimo de 3 años que garantice la atención oportuna ante fallas presentadas en estos.
n. Evitar la operación de equipos de red sin soporte y en estado de obsolescencia por un tiempo superior a 5 años.

4.3 CONFIDENCIALIDAD

Define que la información y los dispositivos de red, solo pueda ser accesible por las personas autorizadas.

4.3.1 Características

a. Realizar segmentación de la red en capa 2.
b. La comunicación entre VLANs debe realizarse a través mecanismos de seguridad (Firewall, ACLs u otro elemento de control de acceso), que defina claramente origen, destino y protocolo. Por lo tanto, se debe identificar claramente el tipo de tráfico que contiene cada una de las VLANs definidas.
c. Implementar mecanismos de autenticación fuerte y control de acceso a la gestión de la red, por ejemplo: (Radius, TACACS+)
d. El acceso a la gestión de los equipos debe efectuarse mediante una VLAN exclusiva (VLAN de gestión), la cual sólo es accesible desde los PC de los administradores u operadores.
e. Las herramientas de monitoreo deben acceder a los dispositivos para recolectar información. Este debe ubicarse en un segmento aparte de todos los demás servicios (VLAN de monitoreo, o puede ser la misma VLAN de gestión).
f. Evitar el uso de protocolos inseguros (Telnet) que facilitan la fuga de información sensible. En caso de no poderse evitar el uso de dichos protocolos, se debe aislar en una VLAN aparte.
g. Se debe utilizar protocolos seguros (SSH, HTTPS, etc.) que cuenten con cifrado para el envío y manejo de información; para el acceso a la gestión de los dispositivos de la red corporativa del MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE.
h. Se debe implementar protección contra ataques a nivel de red que prevengan fuga de información y ataques de hombre en el medio (MitM), ARP Spoofing, DNS Spoofing, DHCP Spoofing, etc.
i. El acceso de los usuarios se realice con base en perfiles.
j. Para la conexión de usuarios remotos se debe realizar a través de canales con cifrado fuerte (VPN).
k. La conexión de sucursales u otras entidades autorizadas se debe realizar a través de canales con cifrado fuerte (VPN).
l. Al implementar servicios de acceso remoto tipo VPN para usuarios, la conexión debe ser tipo SSL de última generación y permitir únicamente escritorio remoto a la estación de trabajo del usuario.
m. Al dar de baja un dispositivo, se debe implementar un procedimiento e instructivo de borrado seguro de configuraciones e información del mismo.
n. Se debe generar controles de navegación mediante el uso de perfiles.
o. Deshabilitar/apagar los puertos físicos no utilizados en los dispositivos.

p. Restringir el acceso a los puertos de consola de los dispositivos a través de configuraciones de buenas prácticas.
q. La red WIFI no debe utilizar mecanismos de cifrado como WPA2/WPA3, en su remplazo utilizar autenticación por 802.1x.

4.4 SEGURIDAD Y PRIVACIDAD

Al realizar el monitoreo para analizar el comportamiento de los usuarios del Ministerio, se debe tener en cuenta lo que menciona el articulo 3 de la Ley 1581/2012, sobre protección de datos personales en lo referente a datos sensibles. De acuerdo a la norma lo define así: "*Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello~ que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos*"

Al igual se deben tener en cuenta los siguientes controles del anexo A de la norma ISO 27001/2013:

A.13 **Seguridad de las comunicaciones**

A.13.1.1 **Gestión de la seguridad de las redes:** Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

A.13.1.1 **Controles de redes:** Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

A.13.1.2 **Seguridad de los servicios de red** Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente

4.4.1 Como acceder a los sistemas de información de la Entidad

Acceder a la red interna de la organización desde una ubicación externa, como puede ser el hogar de los servidores públicos, para utilizar información de la Entidad y cualquier otra herramienta como el correo electrónico es vital para poder teletrabajar. Para realizarlo de manera segura y que la información se transmita respetando su confidencialidad **es recomendable utilizar una red privada virtual o VPN** por sus siglas en inglés Virtual Private Network.

4.4.2 Red privada virtual o VPN

Una VPN crea una **conexión privada y cifrada** evitando que los ciberdelincuentes puedan espiar las comunicaciones. Las VPN, al igual que sucede con una página web, pueden contratarse como servicio a un proveedor externo o se pueden instalar y administrar internamente por la empresa.

Las **VPN como servicio** tienen como principal ventaja que toda la administración y gestión la realiza una empresa externa, por lo que los periodos para implantarla son muy reducidos. Sin embargo, se pierde en privacidad porque la información de la empresa se transmite por un tercero.

La otra opción es utilizar una **VPN propia de la Entidad**. De esta manera, en ningún momento la información es gestionada por un tercero, lo que ofrece un extra de privacidad. No obstante, instalar un servicio de VPN propio lleva más tiempo que contratarlo. Además, se requiere personal especializado para que lo haga, ya que si no se configura correctamente puede convertirse en la puerta de entrada de los ciberdelincuentes a la organización.

4.4.3 Conexión al servicio de VPN institucional

Acceder remotamente a algunos de los servicios de la Entidad, como ULISES, SIFAME o a la intranet, es una situación frecuente pero que, a su vez, puede ser una acción de alto riesgo, por temas de Confidencialidad, Integridad y Disponibilidad de la Información.

Si el funcionario o contratista se encuentra fuera de las instalaciones del MADS, o en comisiones nacionales e internacionales o en la modalidad de trabajo en casa y tiene la necesidad de enviar un archivo o un documento y siente la necesidad de utilizar la wifi en un aeropuerto, hotel, o un centro comercial, no es una buenas práctica. lo recomendable es utilizar el servicio de conexión por VPN.

4.5 BUENAS PRÁCTICAS

4.5.1 Trazabilidad

Para garantizar una adecuada administración, gestión y control de incidentes en los servicios de red, se hace necesario contar con una adecuada documentación que proporcione como mínimo:

a. Topología de red.
b. Planos de distribución actualizados piso a piso que permita identificar los puntos de red LAN e inalámbricos.

c. Contar con los planos arquitectónicos actualizados piso a piso de la edificación que facilite como insumo al mejoramiento de la red inalámbrica WIFI.
d. Tener mapas de cableado detallado en data center, centros de cableado y puntos de usuarios final.
e. Generar diagramas de Ingeniería de detalle asociados a los servicios de TI que se implementen.
f. Elaborar un esquema de direccionamiento IP.
g. Elaborar diagramas y esquemas de conexión de los centros de cableado y data center.
h. Tener un inventario de todos los dispositivos de red con una hoja de vida asociada a cada dispositivo de red.
i. Generar un procedimiento para el borrado seguro de los dispositivos de la red.
j. Tener los registros de eventos habilitados (niveles: Fatal, Error, Warning, e Info) y que se almacenen en un repositorio seguro dentro de la red (storage de logs).
k. Complementando lo anterior, los dispositivos de red deben tener la capacidad de almacenar (hasta donde sea posible) los registros de eventos.
l. Implementar y mantener un software de gestión de registro de eventos.
m. Se debe implementar y mantener un software de gestión robusto el cual permita visibilidad y control de la red.
n. Efectuar mantenimientos preventivos a los dispositivos de red de acceso al menos dos (2) veces al año y a los de CORE al menos una (1) vez al año.
o. El fabricante o en su defecto el proveedor de acuerdo al contrato vigente deberá realizar una visita para verificar el estado de sus dispositivos por lo menos una vez al año.

4.5.2 Usuarios

Definir los usuarios requeridos para el acceso a los dispositivos de red que respondan a un nombre identificable según el estándar del ENTIDAD. Estos usuarios deben ser configurados mediante un sistema de autenticación seguro.

Se debe mantener un usuario de emergencia configurado localmente en el dispositivo de red en caso de incidentes. Este usuario y contraseña deberá mantenerse en cadena de custodia, revisarse y cambiarse cada 6 meses.

No se debe permitir usuarios genéricos para acceder a los dispositivos de red, excepto si son utilizados por dispositivos de monitoreo o en caso de emergencia.

4.5.3 Configuraciones

a. En las configuraciones se debe eliminar todo uso de protocolos inseguros para su gestión y en caso de no ser posible, asegurarlos.

b. Tener en la medida de lo posible una descripción de cada una de las configuraciones realizadas, por ejemplo: Si se configura una ruta poner una descripción del objetivo o que hace esa ruta. En caso del que dispositivo no permita esto dicha descripción se debe colocar en las ingenierías de detalle.
c. Para las configuraciones realizadas en todos los dispositivos, se deberá hacer copias de seguridad acorde a los esquemas de Backup del ENTIDAD.
d. Se debe configurar los dispositivos de red acorde con las buenas prácticas de seguridad del fabricante de los dispositivos.
e. Tener un plan (incluye procedimiento e instructivo) de restauración de configuración probado y listo para ser ejecutado en caso de incidentes.
f. Los dispositivos deben generar u ofrecer un registro de eventos, los cuales se registren en un dispositivo externo para monitoreo y análisis.

4.5.4 Protocolos /Servicios

a. Permitir carpetas compartidas (puerto 445) única y exclusivamente hacia file server implementados con tecnologías NAS o SAN.
b. Documentar todos y cada uno de los protocolos ya sea TCP, UDP, ICMP y cualquier otro autorizado para transitar por la red.
c. Permitir únicamente los protocolos autorizados para transitar en la red.

4.5.5 WI-FI

d. La plataforma de WIFI deben ofrecer la flexibilidad necesaria para propagar SSIDs con parámetros de visibilidad e invisibilidad en las conexiones inalámbricas.
e. Se debe implementar, preferencialmente, que los usuarios operen bajo la banda de 5Ghz sobre la de 2.4Ghz y que los usuarios Invitados cuente con un canal dedicado con ancho de banda acordado. El desempeño del servicio dependerá igualmente de las características técnicas del equipo del usuario.
f. No utilizar mecanismos de cifrado como WPA2/WPA3, en su remplazo utilizar un método de autenticación basado en 802.1x.
g. Se debe implementar un mecanismo que permita el acceso de usuarios Invitados empleando un portal cautivo que garantice el control de los mismos.
h. Se debe considerar el otorgamiento de permisos de acceso de navegación para usuarios invitados por máximo 8 horas.

4.5.6 Perfiles de Navegación

Se estipulan los siguientes perfiles como parte del servicio LAN y WLAN.

- NAV_VIP: Este perfil de navegación provee acceso casi ilimitado a los sitios de internet y está perfilado para las altas gerencias de la Entidad y demás servidores públicos que por funciones u obligaciones tengan autorización del Jefe Inmediato o Supervisor de contrato.

- NAV_ Comunicaciones: Este perfil de navegación está enfocado a la Oficina de Comunicaciones y todo el grupo que requiera acceso al mismo dado que la fortaleza de sus accesos está en sitios de interés del sector y redes sociales.

- NAV_OTIC: Este perfil de navegación está enfocado a la Oficina TIC dado que su alcance involucra temas netamente técnicos, perfiles de acceso a plataformas y servicios globales, así como funciones de descarga de software, aplicaciones, utilitarios y soluciones de gestión tecnológica.

- NAV_Administrativo: Este perfil de navegación es el general y aplica para todos los usuarios de red de la Entidad a menos que éste sea parte de alguna de las políticas anteriormente descritas. Los accesos son restringidos por asuntos de seguridad de la información y su alcance está en permanente gestión para habilitar/deshabilitar nuevas funcionalidades.

4.5.7 SSIDs

Se estipulan los siguientes SSID como parte del servicio WLAN.

- VIP: Este perfil de navegación provee acceso casi ilimitado a los sitios de internet y está perfilado para las altas gerencias de la Entidad y demás servidores públicos que por funciones u obligaciones tengan autorización del Jefe Inmediato o Supervisor de contrato. Esta red sugiere tener una característica de SSID oculto.

- Funcionarios: Este perfil de navegación es el general y aplica para todos los usuarios de red de la Entidad a menos que éste sea parte de alguna de las políticas anteriormente descritas. Los accesos son restringidos por asuntos de seguridad de la información y su alcance está en permanente gestión para habilitar/deshabilitar nuevas funcionalidades.

- Visitantes: Este perfil de navegación aplica para todos los usuarios de paso o eventuales en la entidad. Los accesos son restringidos por asuntos de seguridad de la información y su alcance está controlado.

- WIFI Libre: Este perfil aplica según la reglamentación vigente para las entidades del Estado Colombiano. Los accesos son restringidos por asuntos de seguridad de la información y su alcance está controlado para los ciudadanos.

Si la Entidad requiere implementar más SSID, se debe analizar la necesidad, verificar su viabilidad técnica previo a un plan de implementación.

4.5.8 MONITOREO WLAN

Se debe implementar las siguientes características:

a. La solución WIFI debe permitir el monitoreo WLAN integral de la conexión de usuarios.
b. Visualizar los niveles de señal y alertar anomalías (por ejemplo, ataques de suplantación, inyección de paquetes, ataques de fuerza bruta).
c. El sistema debe permitir ubicar dispositivos en la red utilizando la dirección MAC y el Access Point al que está asociado.
d. Disponer de un registro de actividades (logs).

4.5.9 PERFILES

a. Se debe utilizar un mecanismo de autenticación fuerte para el ingreso a la red de la entidad, considerando las siguientes características:

- Garantizar exclusivamente el ingreso a la red de los dispositivos y usuarios autorizados, por lo tanto, se debe autenticar el usuario y/o el equipo.
- Con base en el perfil del usuario, asignarlo a la Vlan correspondiente mediante la integración del directorio activo u otros servicios de autenticación, asegurando el acceso confiable a la red de los usuarios internos y externos.
- El sistema permita desconectar usuarios de la red WIFI.
- Los perfiles de usuario solamente deberán ingresar a la información autorizada.

4.5.10 PUERTOS FÍSICOS

a. Los equipos dispuestos en los puestos de trabajo y conectados a un punto de red, deben realizar una asociación de dirección MAC.
b. Limitar la cantidad de direcciones MAC que acepte por puerto.

4.5.11 GESTIÓN DE VULNERABILIDADES

a. Se debe realizar análisis de vulnerabilidades a los dispositivos de red por lo menos dos (2) veces al año, diseñar y ejecutar planes de remediación.

b. Se debe realizar pruebas que incluyan ataques de hombre en el medio (MitM) para la LAN.
c. Se debe realizar despliegues de actualizaciones automáticas en los equipos registrados en el controlador de red; estas deben desplegarse en horario nocturno para garantizar continuidad en el negocio y contar con ventanas de mantenimiento autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones.

4.6 SANCIONES

El uso inapropiado del acceso a internet proporcionado por el Minambiente puede ocasionar la desactivación temporal o permanente de las cuentas de red.

El tráfico particular de un usuario puede ser monitoreado sin notificación previa, por la Oficina de Tecnologías de la Información - TIC, para efectos de garantizar el buen uso del servicio en cumplimiento de las condiciones y uso del servicio establecidas en el presente documento. Si existe evidencia de que el usuario está haciendo mal uso del servicio, incumpliendo los lineamientos establecidos en este documento o está incurriendo en actividades ilícitas mediante el servicio de acceso a internet, la Entidad se reserva el derecho de tomar acciones disciplinarias, incluyendo las medidas pertinentes, de acuerdo con la normativa y legislación vigente.

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos se toman de la Ley 1273 de 2009 los siguientes artículos haciendo parte de las sanciones que tendrán los usuarios que incumplan las políticas de uso del servicio de navegación de Internet del Ministerio de Ambiente y Desarrollo Sostenible:

> Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
>
> Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

5 GLOSARIO.

Acceso: Equipo encargado de proporcionar acceso a los grupos de trabajo o usuarios de red, normalmente se encuentran ubicados en los centros de cableado.

Access Point o Punto de Acceso Inalámbrico: conocido por las siglas **WAP** o **AP**), es un dispositivo de red que interconecta equipos de comunicación inalámbrico para formar una red inalámbrica interconectando dispositivos móviles o tarjetas de red inalámbricas.

Centro de cableado: Puede ser una habitación o un gabinete diseñado especialmente para ello. Por lo general, incluye: paneles de conexión, espejos de cableado, switches, routers, puentes.

Core: Equipo encargado de proporcionar conectividad entre los distintos puntos de acceso (router, switch, etc). Nos permite enlazar diferentes servicios, como internet, redes privadas, redes LAN o telefonía entre otros.

Datacenter: Centro de datos que alberga los recursos tecnológicos que permiten procesar una gran cantidad de información.

HTTPS: Es un protocolo de aplicación que se basa en el protocolo http, que está destinado a la transferencia segura de datos de hipertexto. O sea es la versión segura de http. Este protocolo lo utilizan entidades bancarias, tiendas en línea y cualquier servicio que solicite el envío de datos personales o contraseñas a través de la web.

ICMP: El protocolo de control de mensajes de Internet es parte del conjunto de protocolos IP. Es utilizado para enviar mensajes de error e información operativa indicando, por ejemplo, que un host no puede ser localizado o que un servicio que se ha solicitado no está disponible.

Ingeniería de detalle: planos, planillas, croquis, memorias de cálculo, especificaciones técnicas, en forma tal que permitan realizar al contratista los trabajos indicados

LAN: Red de área local (por sus siglas en inglés Local Area Network), interconexión de varios ordenadores y periféricos

MAC (siglas en inglés de Media Access Control) es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (8 bits)) que corresponde de forma única a una tarjeta o dispositivo de red.

NAS: El almacenamiento conectado en red, Network Attached Storage, es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador/ordenado

Rack: Estante metálico cuya finalidad principal es la de alojar equipamiento electrónico, informático y de comunicaciones donde las medidas para la anchura están normalizadas para que sean compatibles con el equipamiento de cualquier marca o fabricante.

SAN: Una red de área de almacenamiento, en inglés Storage Area Network, es una red de almacenamiento integral.

Servidor: Un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software.

SSH: Es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

TCP: Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP).

Topología de Red: se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.

UDP: El protocolo de datagramas de usuario es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

UPS: Una UPS (Uninterruptible Power Supply) es una fuente de suministro eléctrico que posee una batería con el fin de seguir suministrando energía a un dispositivo en el caso de interrupción eléctrica.

VPN: Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

WAN: (Wide Area Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

WIFI: es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información

WPA2: En español «Acceso Wi-Fi protegido 2», es un sistema para proteger la red inalámbrica creado para corregir las deficiencias del sistema previo en el nuevo estándar 802.11i

WPA3: en español «Acceso Wi-Fi protegido 3», es el sucesor de WPA2 que fue anunciado en enero de 2018, por la Wi-Fi Alliance. El nuevo estándar utiliza cifrado de 128 bits en modo WPA3-Personal y confidencialidad de reenvío.