CONTENIDO

1. INTRODUCIÓN

El presente documento presenta una serie de recomendaciones de seguridad y privacidad de la información, para fortalecer los diferentes componentes de la infraestructura tecnológica TIC de la entidad.

Entendiendo hardening o bastionado, las acciones realizadas para disminuir la superficie de ataque, realizando acciones que aseguren las configuraciones de los diferentes componentes de la infraestructura tecnológica.

De manera predeterminada los fabricantes configuran sus productos en función de la facilidad de uso sobre la seguridad, esto significa funciones o configuraciones por defecto potencialmente peligrosas o funciones innecesarias. Cada función o configuración es un vector para un potencial ataque, por lo que asegurar la adecuada configuración de los sistemas es una tarea fundamental para mitigar las amenazas y vulnerabilidades y evitar su materialización.

2. OBJETIVOS

Establecer las pautas de hardening para asegurar la infraestructura crítica de TI de la UAESP, con el objetivo de preservar su confidencialidad, integridad y disponibilidad, con un enfoque granular, diferenciando el tipo de componente por sus características como; funcionalidad, rol, fabricante, versión, entorno, etc., y atendiendo a la normatividad vigente establecida por el MinTic y buenas prácticas del mercado como las establecidas por el CCN-CERT en sus guías de hardening, NIST (CSF y SP), PCI DSS, HIPAA, CIS, DISA STIG o 150/IEC15408.

2.1 Objetivos específicos

- Reemplazar las configuraciones de fábrica de la infraestructura de TI por unas seguras o en ocasión de un reseteo que regrese el dispositivo a su configuración de fábrica.
- Implementar mejoras de seguridad sobre la infraestructura TI, asegurando que esta se encuentre protegida del acceso físico no autorizado que pudiesen comprometer su seguridad e interrumpir su operación.
- Administrar las configuraciones de la infraestructura TI de acuerdo con las recomendaciones de los fabricantes y las buenas prácticas asociadas.
- Realizar las actualizaciones periódicas de la infraestructura, que incluyan firmware y software, teniendo en cuenta los últimos parches de seguridad liberados por el fabricante.
- Monitorear la infraestructura TI para implementar y actualizar las pautas de hardening cuando sea necesario.

3. ALCANCE

Aplica a la infraestructura crítica de TI e incluye sus sistemas operativos, hardware y firmware de la entidad.

Aplica a todos a los servidores(as) públicos(as) y contratistas de la Unidad Administrativa Especial de Servicios Públicos que administran la infraestructura crítica de TI de la entidad. Inicia con la identificación, valoración, revisión y aplicación de las recomendaciones entregadas en el presente documento.

4. NORMATIVA

Resolución 0500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

NTC-ISO/IEC 27001:2013: Norma Técnica Colombiana Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

5. SIGLAS

- API: Application programming interface – (Interfaz de programación de aplicaciones).
- CMS: Content management system - Sistema de gestión de contenidos.
- CIS: Center for Internet Security – Centro para la seguridad en Internet.
- CISA: Cybersecurity & infraestructure security agency – Agencia de seguridad de ciberseguridad e infraestructura.
- DAST: Dynamic Application Security Testing – Pruebas de seguridad de aplicaciones dinámicas.
- DISA: Defense information Systems Agency – Agencia de sistemas de información de defensa.
- DoS: Denial of service attack – Ataque de denegación de servicio.
- DDoS Distributed denial of service attack Ataque de denegación de servicio distribuido.
- ISO: International Organization for Standardization – Organización internacional de normalización.
- MSPI: Modelo de Seguridad y Privacidad de la Información.
- NINTIC: Ministerio de las tecnologías de la información y las comunicaciones.
- NIST: National Institute of Standards and Technology – Instituto nacional de normalization y tecnología.
- OTIC: Oficina de tecnologías de la información y las comunicaciones.
- OWASP: Open web application Security Project – Proyecto abierto de seguridad de aplicaciones web.
- SAMM: Software Assurance Maturity Model.
- SANS: Escal Institute of Advanced Technologies.
- SAST: Static application security testing.
- S-SDLC: Secure Software Development Live Cicle.
- STIGs: Security Technical Implementacion Guides.
- SSID: Service Set Identifier.
- UAESP: Unidad Administrativa Especial de Servicios Públicos.
- VCS: Version Control System.

6. DEFINICIONES

Activo: Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Aplicación: programa informático desarrollado para facilitar o llevar a cabo ciertas tareas automáticamente.

Autenticación: Acto o proceso de confirmar que algo o alguien es quien dice ser.

Autorización: proceso mediante el que el usuario obtiene los privilegios necesarios para poder acceder a los recursos o información.

CMS: Un sistema de gestión de contenidos o CMS es un programa informático que permite crear un entorno de trabajo para la creación y administración de contenidos, principalmente en páginas web, por parte de los administradores, editores, participantes y demás usuarios.

Confidencialidad: capacidad de preservar que la información o recursos, están ocultos a usuarios no autorizados.

Dast: herramientas y técnicas para analizar la seguridad de aplicaciones de manera dinámica.

Disponibilidad: capacidad que garantiza que el software es operativo y accesible por los usuarios.

Fabricante (Vendor): Son las compañías encargadas de diseñar, fabricar, distribuir los productos que presten algún tipo de servicio tecnológico, tales como elementos de comunicación, elementos de usuario final, etc.

Firmware: Es un programa informático que establece la lógica de bajo nivel para el funcionamiento de un dispositivo electrónico, este programa es diseñado para que se efectúen las actividades más básicas en el funcionamiento de una máquina, desde el mismo encendido hasta las interrupciones que le permiten en intercambio de datos entre dos usuarios.

Fiabilidad: se define en términos estadísticos como la probabilidad de operación libre de fallos de un programa de computadora. Característica fundamental de los sistemas informáticos por la que se mide el tiempo de funcionamiento sin fallos.

GET: El método GET envía la información en la propia URL, estando limitada a 2000 caracteres. La información es visible por lo que con este método nunca se envía información sensible. No se pueden enviar datos binarios (archivos, imágenes...).

Hardware: Conjunto de componentes físicos de un sistema informático.

Hardening, Bastionado o Endurecimiento: En seguridad informática es el proceso de asegurar un sistema de información mediante la reducción de la superficie de ataque, esto se logra mediante el uso de configuraciones recomendadas de acuerdo con el tipo de dispositivo tecnológico.

Hash: son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado

HTTPS: (HyperText Transfer Protocol Secure), Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web.

Incidente: cualquier evento que tenga el potencial de afectar la preservación de la confidencialidad, integridad, disponibilidad o valor de la información

Infraestructura tecnológica: Son los elementos de hardware (servidores, redes de comunicación, elementos de seguridad informática, etc.) y software (bases de datos, aplicativos, desarrollos, etc.) que integran y dan soporte a la ejecución de todos los sistemas de información del instituto.

Interfaz de línea de comando (CLI): Interfaz en modo texto para el usuario final que le permite mediante la ejecución de comandos de configuración para algún dispositivo electrónico.

Integridad: capacidad que garantiza que el código del software, activos utilizados, configuraciones no puedan ser o no hayan sido modificados o alterados sin autorización.

Log: registro de un evento ocurrido durante la operación de un sistema de información

LVM: Logical volumen manager, es una implementación de un gestor de volúmenes lógicos para el núcleo Linux

POST: método que introduce los parámetros en la solicitud HTTP para el servidor. Por ello, no quedan visibles para el usuario. Además, la capacidad del método POST es ilimitada.

Red de datos: Conjunto de computadores y otros elementos que están conectados a través de una red (comparte mismo medio), ubicados en la misma o diferente ubicación geográfica, que permiten compartir información entre los usuarios a través del recurso tecnológico.

Resiliencia: es la habilidad de un software para recuperarse y ajustarse a sí mismo en escenarios de estrés o interrupción, logrando ejecutar la tarea para la cuál ha sido diseñado.

Sast: pruebas de seguridad de aplicaciones estáticas utilizadas para proteger el software mediante la revisión del código fuente del software para identificar las fuentes de vulnerabilidades.

Software: Programas y documentación de apoyo que permiten y facilitan el uso de la computadora además de automatizar procesos. El software controla el funcionamiento del hardware y el procesamiento de datos.

SSL: (Secure Sockets Layer), capa de sockets seguros, es un protocolo para navegadores y servidores web que permite autenticar, cifrar y descifrar la información enviada a través de Internet.

Switch (dispositivo activo capa 2): Elemento que sirve para conectar varios elementos dentro de una red con la finalidad de compartir información entre ellos mediante el uso de un dispositivo final tipo computador, celular, tablet, etc.

UAESP: Unidad Especial de Servicios Públicos, entidad adscrita a la secretaria del Hábitat en la Ciudad de Bogotá Distrito Capital.

7. CONSIDERACIONES GENERALES

A continuación, se lista una serie de recomendaciones de carácter general que pueden implementarse a los diferentes activos sujetos al alcance de este documento.

- La oficina TIC debe contar con inventario actualizado y mantener control sobre el software y la infraestructura tecnológica.
- Eliminar los servicios y aplicaciones innecesarias, debido a que; por error humano o mediante un ataque se pueden modificar las configuraciones y activar arbitrariamente los servicios deshabilitados que pueden llegar a ser explotados.
- La oficina TIC debe determinar los servicios, protocolos y aplicaciones permitidas, establecer los que se deshabilitarán o eliminarán de los servidores.
- La instalación de servicios críticos, protocolos, o componentes adicionales a los necesario para la adecuada prestación del servicio en ambientes de producción, deben ser aprobados por el grupo de gestión de cambios TIC.

- La infraestructura crítica de TI debe ser sujeta de hardering y testeada previo paso a producción.
- Se debe extraer y almacenar copia de la configuración de los activos previo a manipulaciones como actualizaciones o reseteos.
- Todo software y firmware debe ser descargado de las páginas oficiales de los desarrolladores y de ser posible confirmar su integridad mediante la verificación de su hash.
- Se debe monitorear y estar en contacto con los diferentes fabricantes para implementar de primera mano las recomendaciones entregadas por éstos con respecto a configuraciones y actualizaciones.
- Todo activo debe contar con las últimas actualizaciones de software y firmware estables y se debe contar con mecanismos para realizar rollback de ser necesario.
- Se deben establecer los mecanismos de seguridad física necesarios para endurecer los activos contra accesos físicos no autorizados o en ocasión de un accidente o desastre natural.
- Se deben establecer configuraciones que aseguren la alta disponibilidad y permitir la continuidad de las operaciones en escenarios adversos.
- Se debe realizar backup a los activos críticos que aseguren la menor perdida de información en el escenario de la materialización de una amenaza.
- Se deben cerrar los puertos de aquellos servicios de escucha por defecto y que no son requeridos por el servidor.
- Se deben fortalecer las configuraciones de los servicios activos mediante la restricción de: usuarios, ordenes que puedan realizar control y filtrado de datos que son enviados al servidor (XSS, SQL injection, etc.).
- Se debe establecer una red DMZ, mediante un firewall restringiendo el acceso de las conexiones externas hacia ésta para los casos en los que aplique.
- Se debe evitar que un servidor DMZ disponga de herramientas de desarrollo como compiladores, interpretes SHELL, BASH, desensambladores, etc.
- Cada servicio de los servidores debe ejecutarse con un usuario/grupo propio y único para dicho servicio, y que éste tenga asignado los permisos estrictamente necesarios.
- Todo software descargado desde Internet debe ser almacenado y testeado en un ambiente de prueba antes de su despliegue en producción y el sistema debe ser escaneado por el antivirus después de testear el software.

8. HARDENING SISTEMA OPERATIVO LINUX

A continuación, se presenta una serie de recomendaciones para aplicar sobre la infraestructura crítica de TI con sistema operativo Linux. Adicionalmente, en el anexo No. 1 se encuentra la lista de chequeo que se debe diligenciar de acuerdo con el alcance del presente documento.

Previo a la instalación:

- Descargue las distribuciones o software únicamente de la página oficial de los fabricantes y compruebe mediante hash la integridad del sistema operativo o software descargado.
- Se deben planear los requerimientos de hardware asociados considerando que estos son limitados y se debe hacer el mejor uso de estos.
- Se debe planear el particionado, previo a la instalación para evitar instalaciones que presenten: perdida de rendimiento al momento de acceso de los datos, facilitar la recuperación ante desastres, problemas de disponibilidad de espacio en disco o espacios sobredimensionados sin utilizar.

- Configure las contraseñas de acuerdo con el manual de políticas de seguridad y privacidad de la entidad.

Durante la instalación:

- Se debe establecer una contraseña de arranque.
- Establecer los permisos del archivo de configuración de arranque.
- Forzar al uso de contraseñas en el modo Single User.
- Se deben realizar instalaciones básicas limitando el conjunto de funcionalidades solo a las necesarias para su instalación y funcionamiento inicial, y posteriormente de acuerdo con los requerimientos instalar solo los componentes necesarios.
- En las distribuciones que lo permitan usar LVM.
- Se debe configurar adecuadamente el uso del bit suid y guid en especial los permisos de administración root, debido que estos permisos pueden ser utilizados para escalar privilegios.

Después de la instalación:

- Se debe realizar la actualización completa y upgrade del sistema tan pronto finalice la instalación.
- Se debe realizar revisión de vulnerabilidades y la instalación de sus respectivos parches.
- Se debe prevenir la combinación de reinicio.
- Se debe limitar la información sobre el activo de información.
- Se deben configurar solo los servicios necesarios y el resto se deben deshabilitar.
- Se debe limitar el acceso como root a las terminales.
- Se debe forzar el logout de los usuarios.
- Se debe limitar el acceso a los recursos.
- Antes de pasar un sistema operativo o software a producción, se deben realizar test de seguridad y rendimiento en ambientes de prueba controlados.
- Se deben instalar y configurar los controles de seguridad establecidos por la entidad, los cuales incluyen:
    - Software de antivirus
    - Firewall
    - Software de gestión de actualizaciones y parches
    - Tecnologías de cifrado de disco
    - Aplicaciones de monitoreo.

9. HARDENING SISTEMAS OPERATIVOS WINDOWS

A continuación, se presentan una serie de recomendaciones específicas a realizar sobre los activos que cuentan con sistema operativo Windows Server en cualquiera de sus versiones. Adicionalmente en el anexo No. 1 se encuentra la lista de chequeo que se debe diligenciar de acuerdo con el alcance del presente documento.

- Firmar el protocolo SMB.
- Configure la sincronización de hora automática, algunos servicios y protocolos no funcionan si se evidencian diferencias de tiempo significativas.
- Inicie con una instalación con los mínimos componentes y luego agregue solo los necesarios.
- De acuerdo con las recomendaciones de la NIST 800-123, el servidor debe estar en un host dedicado y de un solo uso.
- Se deben deshabilitar los servicios, aplicaciones y protocolos que no sean necesarios.

- Elimine o desactive componentes innecesarios los cuales se listan a continuación:
  - Microsoft store.
  - Uso compartido de archivos e impresoras (NetBIOS, NFS, FTP)
  - Servicios de redes inalámbricas
  - Programas de acceso remoto inseguros (Telnet)
  - Servicios de directorio activo (LDAP)
  - Sistemas de información de red (NIS)
  - Servidores web y servicios asociados
  - Servicios de correo electrónico (SMTP)
  - Compiladores de idiomas y bibliotecas
  - Herramientas de desarrollo del sistema
  - Utilidades y herramientas de administración de redes y sistemas (SNMP).
- Se deben deshabilitar o restringir el acceso de cuentas predeterminadas innecesarias como, por ejemplo: cuenta invitada, cuentas administrador a nivel raíz y las cuentas asociadas con servicios locales y de red.
- En caso de no poder realizar las acciones del punto anterior se deben cambiar las contraseñas por defecto de estas cuentas y configurar contraseñas fuertes.
- Se deben crear grupos de usuarios, asigne los usuarios a los grupos asociados y luego asigne los permisos a los grupos, este enfoque es más seguro y fácil de administrar, que asignar permisos a usuarios individuales.
- Debe limitarse el privilegio de ejecución de las herramientas relacionadas con el sistema.
- Se debe restringir al máximo los accesos de lectura a archivos y directorios.
- Se deben instalar y configurar los controles de seguridad establecidos por la entidad, los cuales incluyen:
  - Software de antivirus
  - Firewall
  - Software de gestión de actualizaciones y parches
  - Tecnologías de cifrado de disco
  - Aplicaciones de monitoreo.

10. HARDENING REDES CABLEADAS

10.1 Recomendaciones para el aseguramiento de servicios para un dispositivo capa 2 (switch).

En este numeral se describirán de manera general las recomendaciones para la configuración de las características básicas en seguridad que deben ser implementadas en los dispositivos activos de red capa 2 de la entidad.

Todos los elementos de red (switches) tienen por defecto en su funcionamiento diario servicios activos o no activos, de acuerdo con las especificaciones del fabricante, esto puede habilitar nuevas superficies en la configuración que puedan ser utilizadas por un atacante para causar un perjuicio en la infraestructura de red de la entidad.

A continuación, se enumeran cuáles son los servicios por defecto recomendados que debe ser habilitados o que deben ser deshabilitados para este tipo de dispositivos.

Tabla 1 SERVICIOS POR DEFECTO – ESTE CHECKLIST ESTÁ BASADO EN EL LINUX HARDENING CHECKLIST PROPUESTO POR LA UNIVERSITY COLLEGE DUBLIN Y EN LA ALCALDÍA DE BOGOTÁ.

Estado	Servicio	Descripción
Activar	SSHv2	Protocolos de comunicación recomendados para interactuar con los dispositivos tipo switch.
	TLSv1.2	
	SSLv3.0	

Estado	Servicio	Descripción
Desactivar	IP icmp redirects	Mensajes generados para verificar conectividad que habilitan superficie de ataque y no son necesario tenerlos habilitados.
	IP proxy-arp	
	IP icmp unrechables	
	IP directed-broad	
Desactivar	IP source routing	Servicio que habilita el reconocimiento de rutas, puede ser utilizado para reemplazar rutas de origen.
Desactivar	Discard protocol	Protocolo que utiliza paquetes muy pequeños UDP para la transmisión de información de la máquina.
	Chargen protocol	Protocolo que utiliza paquetes muy pequeños UDP para la transmisión de información de la máquina.
Desactivar	Daytime protocol	Puede ocasionar que por medio de secuencias ASCII se consiga acceso al dispositivo
Desactivar	FTP protocol	Protocolos para transferencia de datos entre terminales de usuario final y dispositivo, solo deben estar activos para temas de respaldo.
	TFTP	
	SCP	
Desactivar	Telnet	Protocolo para la comunicación sin cifrado entre una estación y un dispositivo switch no se debe utilizar, se pueden presentar ataques de hombre en el medio, se debe utilizar SSH mínimo en versión 2.
Desactivar	Bootp Service	Antiguo protocolo que permitía asignar dinámicamente una dirección IP al dispositivo.
Desactivar	HTTP Server	Se debe habilitar el protocolo HTTPS o no utilizarlo para acceso a la máquina.
Desactivar	SNMP protocol	Protocolo para la administración del dispositivo, se debe utilizar mínimo la versión 2, se recomienda la versión 3.

Estado	Servicio	Descripción
Desactivar	Discovery protocol	Protocolo para el descubrimiento de vecinos, es recomendable solo habilitarlo en las interfaces necesarias.
Desactivar	IP mask reply	Genera información de la red que no debe ser enunciada a todo el público.

10.2 Recomendaciones para la configuración de las interfaces (puertos) de un dispositivo (switch).

A continuación, las configuraciones mínimas que se recomiendan para reducir la superficie de ataque en las interfaces (puertos) de red en los dispositivos activos de red capa 2 (switches).

Activar:

- Configuración de la seguridad de puerto (port Security) de acuerdo con las mejores prácticas para cada uno de los fabricantes de los dispositivos activos de red capa 2 (switch) de la entidad.
- Configurar en modo apagado (shutdown/disable), las interfaces del dispositivo activos capa 2 que no se encuentren en uso.
- Limpiar la configuración de las interfaces que no están en uso y asignarlas a una VLAN tipo Carrier.
- Cambiar la VLAN nativa de los puertos troncales en los dispositivos activos capa 2 de la entidad.
- Configurar solo las VLANS permitidas en los puertos troncales en los dispositivos capa 2 de la infraestructura de red de la entidad.
- Configurar correctamente el protocolo de árbol de extensión (spanning-tree) en los dispositivos activos de red capa 2 de la entidad.
- Habilitar las opciones de configuración ‘dhcp snooping, dhcp6 snooping, Dynamic ARP protection’
- Habilitar las opciones para la protección en IPv6 de ND (neighbor Discovery flags)
- Habilitar las opciones de protección para la publicación de prefijos SLAAC en IPv6.

Desactivar:

- Protocolos de enrutamiento no necesarios, estas máquinas solo deberán ser utilizadas para la transmisión de datos en la capa 2.
- La negociación automática para los puertos troncales entre dispositivos de capa2 de la entidad.
- No permitir la asignación automática de la interfaz de administración del switch por medio de protocolo DHCP.

10.3 Recomendaciones para la configuración de acceso seguro a un dispositivo (switch).

Los dispositivos activos de red capa 2 (switches) tienen varias formas para ser administrados de manera remota, entre estos podemos encontrar la interfaz de administración fuera de banda (OoBM - Out-of-Band Management), las líneas VTY por medio del protocolo SSH o TELNET, las líneas de consola local y el acceso web mediante los protocolos HTTP/HTTPS. Las configuraciones en seguridad (hardening) deben ser implementadas para limitar el acceso a las maquina mediante el uso de estos protocolos.

Controles de acceso:

- Out-of-Band Management port (interfaz de administración fuera de banda): En lo posible utilizar esta interfaz de administración fuera de banda para la administración del dispositivo mediante el uso del protocolo SSH mínimo en su versión 2.0.
- Management VLAN (vlan de administración): Es recomendable restringir la administración remota de los dispositivos mediante el uso de una red virtual (VLAN) aislada.
- Authorized IP managers (direcciones IP de administración): Es recomendable restringir el acceso remoto a los dispositivos desde un rango especial de direcciones IP de administración dedicadas para este fin.
- Access Control list (listas de acceso): permite restringir el acceso remoto a los dispositivos de manera granular mediante el uso de rangos de direcciones IP o protocolos de comunicación.

Controles de Autenticación, Autorización y Auditoria (Authetication, Authorization, Accounting):

- Local password authetication (autenticación de usuarios local): este método debe ser utilizado como último recurso o como alternativa en la autenticación de los usuarios para el ingreso a los dispositivos, este debe ser configurado de acuerdo con las recomendaciones que cada uno de los fabricantes, entre las cuales se pueden mencionan algunas:
    - Complejidad de la clave del usuario
    - Número mínimo de caracteres en la clave de usuario.
    - Historial de la clave del usuario.
    - Vencimiento en tiempo de la clave del usuario.
    - Cifrado local de las claves de usuario.
    - Mensaje al fallo del ingreso de la clave de usuario.
    - Tiempo de consola inactivo.
- Role-Based Access Control (RBAC): se debe en lo posible configurar los roles de control de acceso para cada uno de los usuarios administradores en los dispositivos, la configuración de estos roles depende directamente del tipo de fabricante de la maquina tipo switch.
- RADIUS authetication (autenticación por radius): Es altamente recomendado utilizar un sistema de autenticación centralizado tipo Radius que permita a los usuarios administradores de los dispositivos la gestión de contraseñas, roles y privilegios.

Recomendaciones para la prevención de ataques en el plano de control (Control Plane Policy):

- Se deben establecer políticas para la prevención de ataques a nivel de plano de control, estas configuraciones deben ser establecidas de acuerdo con las recomendaciones que facilite cada fabricante de los dispositivos que actualmente se encuentren en producción en la red de la UAESP.

Recomendaciones seguridad física:

- Evitar la manipulación de los paneles frontales de los dispositivos activos de red siempre y cuando no sea necesario, si es posible habilitar las opciones de control en el firmware de las maquinas.
- Restringir físicamente el acceso a los puertos seriales, auxiliares, USB a los usuarios no permitidos mediante la implantación de los controles necesarios.

10.4 Recomendaciones generales en seguridad para un dispositivo capa 2 (switch)

- La entidad debe contar con un sistema de monitoreo para los dispositivos de red que le permita tener visibilidad del funcionamiento y capacidad que se está utilizando actualmente en la red de datos y los servicios que se ejecutan por este medio de transmisión.
- Instalar en todos los dispositivos que con previo estudio se avale el correcto funcionamiento la última actualización en firmware para las máquinas de red capa 2.
- Implementar, configurar un sistema de backup que respalde las configuraciones de las maquinas en forma manual y automática, si es posible que también cifre estas configuraciones.
- No compartir las configuraciones de los dispositivos de red por medio de protocolos inseguros como TFTP, TELNET, FTP o realizar la publicación de esta información en sitios web públicos.

11. HARDENING EN REDES INALÁMBRICAS

Para la configuración inicial y hardening de las redes inalámbricas tenga en cuenta las siguientes consideraciones:

- Cambie las contraseñas predeterminadas, la mayoría de los dispositivos de red incluidos los access point, están preconfigurados con contraseñas de administración por defecto las cuales son fáciles de encontrar en línea, representando una brecha de seguridad. El uso de contraseñas complejas se constituye en la primera línea de defensa.
- Acceso restringido. Solo permita que los usuarios autorizados accedan a su red. Todo hardware conectado a la red tiene una dirección de control de acceso a medios (MAC). Puede restringir el acceso a su red filtrando estas direcciones MAC.
- Configure una cuenta de "invitado", esta función le permite otorgar acceso inalámbrico a los invitados en un canal inalámbrico separado con una contraseña diferente, mientras mantiene la privacidad de sus credenciales principales.
- Cifre los datos de su red. El cifrado de sus datos inalámbricos evita que cualquier persona que pueda acceder a su red los vea.
- Utilice protocolos de cifrado fuertes y asegúrese que son los recomendados por el fabricante y buenas prácticas.
- Oculte los (SSID), para evitar que personas ajenas accedan fácilmente a su red, evite publicar su SSID
- Considere instalar un firewall directamente en sus dispositivos inalámbricos (un firewall basado en host).
- Verifique y mantenga el software y firmware de los access point actualizado.
- Realicé monitoreo constante sobre los dispositivos de red en busca de comportamientos sospechosos.
- La entidad debe contar con un portal cautivo, que permita mediante un sistema de autenticación centralizada usando ad-dc, tener la gestión de los accesos, la auditoria de los ingresos realizados, entre otros, para los usuarios que utilicen los servicios de la red inalámbrica de la entidad.

12. HARDENING FIREWALL

A continuación, se presentan una serie de recomendaciones específicas a realizar sobre el Firewall de la entidad. Adicionalmente se encuentra la lista de chequeo que se debe diligenciar de acuerdo con el alcance del presente documento.

- En el apartado administración, seleccione la complejidad mínima para las contraseñas atendiendo la política de seguridad de la información y las buenas prácticas, esto le permitirá establecer varios parámetros, como la longitud mínima de la contraseña, el número mínimo de caracteres superiores / inferiores, numéricos y especiales. Bloquear la repetición de caracteres. Puede requerir que los administradores cambien su contraseña en el primer inicio de sesión y establezcan un período de tiempo durante el cual será válida cada contraseña.
- Una de las primeras tareas que se debe realizar es cambiar la contraseña de administrador “admin” predeterminada por una más segura que cumpla con las políticas de seguridad de la información de la entidad.
- Segregue a las cuentas de administración en diferentes grupos y proporcióneles accesos diferentes, está tarea la puede realizar en el apartado roles de administrador y creando un nuevo rol. Por ejemplo, si se cuenta con un grupo de administradores que solo necesitan tener acceso a ciertos registros, se deben desactivar las demás partes a las que no necesita acceso. Deshabilitar políticas, objetos, redes, si no queremos que esta cuenta pueda ver las direcciones IP completas o los nombres de usuarios adjuntos en los registros asegurando de paso la privacidad.
- Crear una cuenta de administrador “basado en roles” asignándole el perfil “log-admin”, se debe cerrar sesión e iniciarla con la cuenta recién creada.
- Se recomienda crear un perfil de reenvío de logs del sistema, previendo que, si algo sucede mal, alguien cambia la configuración o sucede alguna acción irregular, los logs se reenviarán a un correo seleccionado.
- Asegúrese que la interfaz de administración esté ubicada en una red segregada o una VLAN separada, a la que solo tenga acceso los administradores.

13. HARDENING DE DATOS

A continuación, se presentan una serie de recomendaciones para proteger las bases de datos de la entidad, previniendo la perdida de datos, fuga o el acceso no autorizado:

Seguridad física del servidor de base de datos:

- Los servidores físicos donde se encuentran alojadas las bases de datos deben contar con un entorno seguro, cerrado, supervisado y monitoreado para evitar el acceso físico no autorizado.
- Los servidores web de aplicaciones no deben estar alojados en la misma máquina que el servidor de base de datos.
- Se deben instalar en el servidor los mecanismos de seguridad con los que cuenta la Entidad (antivirus, Firewall, IPS, IDS, etc.)
- El servidor de la base de datos debe estar ubicado detrás del firewall con reglas predeterminadas para controlar el tráfico de red.
- Los administradores de bases de datos e infraestructura deben revisar y actualizar periódicamente las reglas de filtrado del firewall, respondiendo a las nuevas amenazas y vulnerabilidades.

Software de base de datos:

- Se debe mantener actualizado el software de bases de datos y validar que las versiones actuales cuentan con soporte por parte del fabricante.
- Todas las funciones o servicios no utilizados o innecesarios de la base de datos se deben eliminar o desactivar.

- Las cuentas predeterminadas innecesarias se deben desactivar o cambiar las contraseñas predeterminadas por unas fuertes de acuerdo con lo estipulado en el manual de políticas de seguridad de la información.
- Se deben eliminar los archivos temporales generados en el proceso de instalación que pueden contener contraseñas.
- El software de bases de datos debe estar actualizado y configurado para incluir los parches de seguridad actuales de manera oportuna.

Aplicación / Servidores web / Código de aplicación

- Los diferentes componentes con los que interactúan las bases de datos (aplicaciones / servidores web) deben asegurar la protección de la información mediante controles criptográficos.
- Los servidores, componentes, aplicaciones y herramientas que acceden a la base de datos deben estar documentados.
- Los archivos de configuración y el código fuente deben estar protegidos y solo se pueden acceder a ellos las cuentas de administrador.
- Se debe revisar el código y funcionamiento de las aplicaciones, para detectar vulnerabilidades de inyección de SQL.
- No se permite la instalación de ningún Spyware - "software espía" en los servidores de aplicaciones, web o bases de datos.
- Cuentas de administrador / Permisos / Contraseñas
- El DBA debe revisar todos los cambios solicitados en la base de datos para mantener la seguridad del sistema
- Las cuentas con privilegios de administración del sistema se otorgarán a la menor cantidad de funcionarios o contratistas que así lo requieran de acuerdo con las necesidades.
- Todos los desarrolladores, proveedores, DBAs y contratistas deben firmar un acuerdo de no divulgación.
- Las cuentas de inicio de sistema operativo utilizadas por el personal de DBA para iniciar sesión en máquinas de servidor de bases de datos para tareas administrativas deben ser cuentas individuales y no una cuenta de grupo compartida.
- Se deben auditar las cuentas, asegurando deshabilitar las de los funcionarios y contratistas que se desvinculan de la entidad.

Protección de datos personales

- Se debe atender la normatividad vigente sobre la protección de datos personales.
- En caso de requerir copia de una base de datos de producción a un ambiente de desarrollo o pruebas, los datos deben ser anonimizados o enmascarados a fin de tener una estructura similar a la original, pero con datos sensibles alterados.

Gestión del cambio

- Los procedimientos de gestión de cambios están documentados y cumplen con los requisitos del propietario de los datos.
- Existen controles de administración de cambios para registrar todos los cambios en la base de datos de producción.
- Se tienen identificaos todos los programas y procesos que leen o modifican los datos de producción.

Auditoría de bases de datos

Para efectos de auditoría y trazabilidad de las transacciones o movimientos en las bases de datos, se recomienda tener en cuenta los siguientes ítems:

- Los inicios de sesión exitosos o fallidos; en servidores, sistemas operativos y bases de datos, se deben registrar. Estos registros se conservan durante el tiempo estipulado en la normatividad y buenas prácticas vigentes.
- Las bases de datos que contengan datos personales deben tener activada la auditoría siempre que sea técnicamente posible.
- Los registros de auditoría son revisados regularmente para verificar la seguridad de las bases de datos y el cumplimiento normativo.
- Las actividades irregulares sobre la base de datos deben activar una notificación automática de los administradores responsables del sistema.

Copia de seguridad y recuperación de bases de datos

- Se debe contar con procedimientos de backup y recuperación, los cuales deben estar documentados y cumplir con los requisitos legales y buenas prácticas.
- Se deben realizar pruebas periódicas a los procedimientos de copia de seguridad y recuperación.
- Los intervalos de retención de los Backups están documentados y son suficientes para cumplir con los requisitos de recuperación del negocio y la normatividad vigente.

Cifrado de bases de datos

- Los datos que reportan en la base de datos se cifran durante la transmisión a través de la red utilizando medidas de cifrado lo suficientemente fuertes como para minimizar el riesgo de exposición de los datos o captura de información si se interceptan o se enrutan mal.
- Si se implementa el cifrado a nivel de base de datos, se debe documentar los procedimientos para la administración segura de claves.
- Se recomienda que todas las capas de aplicación (red, aplicación, estación de trabajo cliente) estén cifradas.
- Las copias de seguridad de las bases de datos deben ser cifradas.
- Se debe atender al manual de políticas de seguridad de la información y los procedimientos de cifrado establecidos por la entidad.

14. PAGINA Y APLICATIVOS WEB

A continuación, se presentan una serie de recomendaciones específicas a realizar a la página y aplicaciones:

- Si la entidad decide hacer uso de un CMS, se debe elegir uno que se desarrolle activamente y tenga el respaldo de una comunidad numerosa de desarrolladores o por una empresa de reconocimiento, esto garantiza que, al momento de encontrarse una vulnerabilidad, sea rápidamente publicada y corregida.
- El CMS instalado debe estar en su última versión estable disponible y de una rama que tenga actualmente soporte.
- Se debe verificar que el CMS junto con sus componentes sean compatibles con el sistema operativo del servidor.
- Se debe verificar que el historial de vulnerabilidades críticas del CMS elegido sea el más bajo posible.
- Tanto el CMS, el sistema operativo y sus diferentes componentes deben ser descargados de la web oficial comprobando los hashes.

- Se debe instalar en un sistema operativo moderno, con soporte y actualizado.
- Realizar la instalación de la mínima cantidad de componentes y software necesaria tanto en el CMS como en el sistema operativo, se deben deshabilitar los módulos innecesarios que, por defecto, vienen activos, es importante conocer bien que módulos necesita la aplicación para su funcionamiento.
- Se debe instalar en el servidor los mecanismos de seguridad con los que cuenta la Entidad (antivirus, WAF, IPS, IDS, etc.)
- Se deben abrir solo los puertos que son relevantes para el desempeño y administración de la página web (TCP: 80 (HTTP), 443(HTPPS), 22(SSH), etc.)
- Se debe seleccionar un servidor web con respaldo y condiciones de seguridad óptima.
- Se debe realizar el análisis del tráfico HTTP/HTTPS mediante herramientas de análisis y monitoreo.
- Se debe realizar monitoreo a las alertas y noticias sobre ciberseguridad relacionadas a los diferentes componentes web (CMS, sistema operativo, PHP, servidor web, etc.).
- Se recomienda no revelar la versión del servidor web o mostrar otra versión o tecnología de forma deliberada.
- Se debe deshabilitar el listado de directorios. Esta acción previene el acceso a los archivos del directorio web a través de la URL.
- Se debe deshabilitar la navegación fuera del directorio web. Esto previene ataques tipo “directory traversal”.
- Configurar la cabecera HTTP X-FRAME-OPTIONS para asegurar que la página de la entidad sea contenida dentro de un iframe desde la propia página sameorigin.
- Se deben restringir los métodos HTTP que no sean de utilidad para las aplicaciones.
- Se debe habilitar la protección contra Cross-site scripting (XSS), sanitizando el código.
- Se debe deshabilitar el método TRACK/TRACE.
- Se debe ejecutar el proceso Apache desde un usuario no privilegiado.
- Se debe tener en cuenta lo recomendado por OWASP top 10.

15. LISTAS DE CHEQUEO

Para la adecuada gestión de las configuraciones recomendadas, se deben diligenciar las listas de chequeo correspondientes a cada activo gestionado, las cuales complementan el presente documento.

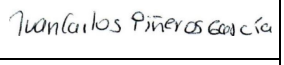
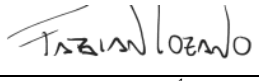
16. FUENTES BIBLIOGRAFICAS

- Cisco Systems. (4 de September de 2020). Cisco Guide to Harden Cisco IOS Devices. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- Cybersecurity Infraestructure Secutiy Agency. (21 de june de 2018). Security Tip (ST18-001). Obtenido de Securing Network Infrastructure Devices: https://us-cert.cisa.gov/ncas/tips/ST18-001
- National Security Agency. (18 de 8 de 2018). Hardening Network Devices. Obtenido de https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF
- Steven Piliero, L. (2007). Center for Internet Security Benchmark for Cisco IOS. New Jersey: cisecurity.org.
- https://security.berkeley.edu/education-awareness/database-hardening-best-practices

17. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	23/02/2023	Creación del documento

18. AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Carlos Piñeros García	Profesional Universitario - Oficina TIC	
	Héctor Gonzalo Cifuentes Hernández	Profesional Especializado – Oficina TIC	
	Fabian Lozano Aguilar	Contratista – Oficina TIC	
	Mauricio Suárez Mayorga	Profesional Universitario	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina de Tecnologías de Información y las Comunicaciones	
	Luz Mary Palacios Castillo	Profesional Universitario – Oficina Asesora de Planeación	
Aprobó	Yesly Alexandra Roa	Jefe Oficina Asesora de Planeación	Alexandra Roa Mendoza Firmado digitalmente por Alexandra Roa Mendoza Fecha: 2023.02.24 07:21:11 -05'00'