**CAJA COSTARRICENSE DE SEGURO SOCIAL**
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

**AS-AATIC-130-2022**
6 de julio de 2022

Máster
Idannia Mata Serrano, subgerente a.i.
**DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150**

Estimada señora:

**ASUNTO: Oficio de asesoría referente a la gestión del Directorio Activo**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo del Área de Tecnologías de Información y Comunicaciones de esta Auditoria, para el período 2022, y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa sobre diversos aspectos a considerar durante la gestión del Directorio Activo de la Caja Costarricense de Seguro Social en aras de coadyuvar en el fortalecimiento del control interno y la minimización de posibles vulnerabilidades de seguridad.

**Antecedentes**

La empresa tecnológica multinacional Microsoft Corporation define el Directorio Activo (AD) como una estructura jerárquica que almacena información sobre objetos como servidores, cuentas de usuario, impresoras, computadoras y otros dispositivos en una red, facilitando a los administradores y usuarios la búsqueda y organización de los datos.

Adicionalmente, en el directorio supra se localiza la estructura lógica conformada por bosques[1], los cuales proporcionan límites de seguridad, servicios de autonomía de datos y su aislamiento en una organización, de manera que puedan reflejar las identidades del sitio y del grupo, así como eliminar las dependencias de la topología física.

Además, el AD y su arquitectura de almacenamiento están compuestos por cuatro elementos esenciales, los cuales se indican a continuación:

- **Dominios[2] y bosques:** Constituyen los elementos principales de la estructura lógica del directorio activo.
- **Compatibilidad con el sistema de nombres de dominio (DNS):** Proporciona un servicio de resolución de nombres para la ubicación del Controlador de Dominio y un diseño jerárquico que el AD puede usar para proporcionar una convención de nomenclatura donde se refleje la estructura organizacional.
- **Esquemas:** Proporcionan la definición de objetos que son utilizados para crear otros objetivos que se almacenaran en el AD.

[1] Un bosque es una construcción lógica que Active Directory Domain Services (AD DS) usa para agrupar uno o más dominios. Estos dominios almacenan objetos para los usuarios o grupos, y proporcionan servicios de autenticación. Microsoft Corp.
[2] El dominio es un componente fundamental de la estructura lógica de Active Directory. Por definición, se trata de un conjunto de objetos de tipo equipo, usuario y otras clases de objetos que comparten una base de datos de directorio común.

- **Almacenamiento de datos:** Es la parte del directorio que administra el almacenamiento y la recuperación de datos en cada controlador de dominio.

**Ciberataque al Directorio Activo**

El AD es el encargado es el encargado de proporcionar autenticación y acceso de usuarios a la red e información de una organización mediante controladores[3] de dominio, por lo tanto, se ha convertido en uno de los objetivos principales de cibercriminales, quienes han incrementado los intentos de vulnerar su seguridad.

A continuación, se presenta el detalle de los mecanismos de ataques más utilizados por los criminales cibernéticos para tratar de acceder de forma fraudulenta al AD:

- Búsqueda de credenciales en Internet: Los cibercriminales utilizan este tipo de ataque sin ser detectados, buscando en internet credenciales de usuarios de una organización o empresa de su interés para intentar acceder a la red.

- Envenenamiento del protocolo de Resolución de nombres de multidifusión local de vínculos (LLMNR): Este tipo de ataque se centra en la recolección o retransmisión de identidades de autenticación de host al momento de iniciar sesión de un usuario, envenenando el servicio para que las víctimas se comuniquen con un sistema controlado por los cibercriminales y posteriormente, obtener las contraseñas.

- Secuestro del Sistema de Nombres de Dominio o DNS Takeover: El atacante silencia al servidor DNS legítimo por medio de algún ataque de denegación de servicio. Una vez silenciado, lo reemplaza funcionalmente por un servidor fraudulento bajo su dominio.

- Ataque de retransmisión del Protocolo de intercambio de archivos de red o Relay SMB Attack: SMB Relay y SMB Relay2 son programas informáticos utilizados para llevar a cabo ataques cibernéticos, su propósito es atacar remotamente equipos creando una nueva dirección IP virtual y la firma SMB debe estar deshabilitada como requisito para que funcione dicho ataque.

- Pass the hash y Pass the Password: Ataque donde un ciberdelincuente extrae o roba credenciales de usuario, en este caso contraseñas, luego las utiliza para engañar el sistema de autenticación y crear una nueva sesión en la red.

- Kerberoasting: La autenticación del AD se realiza a través del Protocolo Kerberos, el cual se encarga de proporcionar tiquetes a los usuarios para verificar su permiso, por lo tanto, el objetivo de este ciberataque es obtener mayor acceso a objetivos adicionales mediante el escalamiento de privilegios en el AD, lo anterior modificando los métodos de autenticación de las contraseñas mediante el uso del sistema de tiquetes.

- Ataque Golden Ticket: Este tipo de ataque se basa en la generación de tiquetes para poder acceder a todos los recursos de internet.

[3] Un controlador de dominio es el servidor que almacena la información de las cuentas de usuario y se encarga de permitir su acceso de conformidad con las políticas de seguridad del dominio al que se desea ingresar.

- Bloodhound: Herramienta tecnológica utilizada para correlacionar usuarios, computadoras y privilegios, con el objetivo de identificar posibles rutas de ataque.

- Ataque MS14-025: Los cibercriminales llevan a cabo este ataque mediante el robo de contraseñas aprovechándose de formas antiguas de Windows para almacenar credenciales.

**La gestión del Directorio Activo y la seguridad**

La administración del AD de las organizaciones a través de buenas prácticas vinculadas con la configuración de credenciales, otorgamiento y monitoreo de los privilegios de usuario, revisión de eventos, ejecución de respaldos y restauración de copias de seguridad en un ambiente adecuado podría reducir el impacto ocasionado ante un ciberataque y minimizar brechas de ciberseguridad que los criminales utilizan para vulnerar la red, ocasionar daños y sustraer datos sensibles administrados por el negocio para posteriormente realizar extorsiones a sus víctimas.

En virtud de lo expuesto anteriormente, la empresa Microsoft Corporation en su página web señala los siguientes aspectos técnicos a considerar para minimizar la superficie expuesta a ataques del AD:

- Implementación de least Privilege modelos administrados: Se centra en identificar los posibles riesgos en torno al uso de cuentas con privilegios elevados y proporciona recomendaciones a considerar para reducir el riesgo.

- Implementación de hosts administrativos seguros: Se realiza la descripción de los principios para la implementación de sistemas administrativos dedicados y seguros, así como diversos enfoques para implementar hosts de forma segura.

- Protección de controladores de dominio contra ataques: Se describe las directivas y configuración donde se incluyen algunas recomendaciones específicas para ayudar a garantizar la protección de los controladores de dominio y sistemas utilizados para su administración.

**Observaciones**

Esta Auditoría en aras de coadyuvar con el fortalecimiento del control interno y minimizar posibles vulnerabilidades referentes a la seguridad de la información administrada por la Institución, así como el impacto en la prestación de servicios durante la recuperación de un ciberataque, menciona los siguientes aspectos relacionados con la gestión del AD, lo anterior con el objetivo de que sean valorados y analizados por la administración:

- Definición de procesos que permita el cambio periódico de contraseña de la cuenta de servicio del Centro de Distribución de Claves (KRBTGT), asimismo, es aconsejable efectuar la modificación de la credencial dos veces con el objetivo de modificar el historial almacenado y de esa forma evitar que un controlador de dominio se replique con una contraseña antigua.

- Establecimiento de políticas para cambiar periódicamente la contraseña de la cuenta de administrador del Modo de restauración de servicios de directorio (DSRM), la cual tiene como función la reparación o restauración de la base de datos de AD.

- Implementación de planes de respaldo y restauración de copias de seguridad de los Controlares de Dominio, Protocolo de Configuración del Host Dinámico (DHCP), Sistema de Nombre de Dominio (DNS), infraestructura de clave pública y otros elementos según se consideren convenientes de conformidad con las políticas de respaldo institucionales. Adicionalmente, es importante que se valore el almacenamiento de respaldos en servidores que no se encuentre conectados a la red ni incluidos en el AD.

- Revisiones de Listas de Control de Acceso (ACL) en aras de identificar oportunidades de mejora asociadas a configuraciones de objetos del AD, delegación de permisos en la Unidad Organizativa del Controlador de Dominio o en dispositivos tecnológicos incluidos en la red, aspecto relevante debido a que si un atacante accediera a cuentas y las vinculara al Administrador del Grupo de Directivas de Objeto (PGO)[4] podría debilitar los mecanismos de seguridad implementados.

  Además, es importante analizar habitualmente las justificaciones emitidas para el otorgamiento de permisos registrados en la ACL y de considerarse oportuno, eliminar los que representen un posible riesgo de vulnerabilidad de la seguridad del AD.

  Al respecto, la práctica constante de esta recomendación coadyuvaría en la detección de permisos otorgados erróneamente a usuarios y la identificación de riesgos de forma preventiva.

  Por otra parte, se debe prestar atención a las cuentas de usuario que tienen todos los permisos activados en los objetos de la red, lo anterior por cuanto podría presentar amenazas que logren vulnerar la seguridad de AD y/o la posibilidad de un ataque por delegación restringida para la obtención del código del Controlador de Dominio.

- Verificación de la ubicación de las cuentas de administrador con nivel de privilegio alto a cargo de la gestión de servidores críticos y la activación de las opciones de confidencialidad, tarjeta inteligente y limitación de delegación de la cuenta.

- Ejecución de comprobaciones de seguridad que permitan verificar el bloqueo del acceso desde y hacía internet de Controladores de Dominio, en caso de no contar con dicha restricción, resulta importante que se valore su implementación a partir de mecanismos técnicos y de directiva.

- Valoración de riesgos a los que se expone la Caja Costarricense de Seguro Social, para determinar la pertinencia de establecer la directiva de auditoría en estaciones de trabajo y servidores que permita identificar eventos, generación de alertas, así como el correspondiente monitoreo.

- Establecimiento de políticas de contraseñas de usuarios con privilegios elevados que sean detalladas y cumplan con los aspectos de seguridad mínimos requeridos, además, promover la concientización en la organización respecto a buenas prácticas sobre gestión de credenciales.

- Análisis de configuración de los servidores con delegación de restricciones, lo anterior considerando los riesgos de seguridad que implica tener ese tipo de equipos conectados a la red y las acciones a efectuar en caso de determinar posibles vulnerabilidades de seguridad.

[4] Grupo de Directivas de objeto o Group Policy Object en inglés, es la infraestructura que le permite especificar configuraciones administradas para usuarios y equipos a través de la configuración de directivas de grupo y las preferencias de directivas de grupo.

- Limitar la delegación de permisos en el AdminSDHolder y mantenerlo monitoreado constantemente para verificar la ejecución de actividades anómalas tales como asignación o modificación de derechos de usuarios o grupos en ese objeto de AD.

- Establecimiento de mecanismos de control sobre la actividad de grupos con privilegios, lo anterior con el objetivo de monitorear eventos y detectar posibles riesgos que puedan afectar la seguridad del AD y de la organización.

- Elaboración de un análisis que permita determinar la factibilidad respecto a utilizar servicios en la nube para la gestión del directorio activo de la CCSS, en apego al marco normativo vigente, las posibilidades institucionales y las buenas prácticas en esa materia.

**Consideraciones normativas**

La Ley General de Control Interno No.8292, en el artículo No. 10 —Responsabilidad por el sistema de control interno, establece lo siguiente:

> *"**Artículo 8 Artículo 10. —Responsabilidad por el sistema de control interno.***
>
> *Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento."*

Las Normas técnicas para la gestión y control de las TIC, en el apartado 1.4.7 —Continuidad de los servicios de TI, menciona lo siguiente:

> *"**1.4.7 Continuidad de los servicios de TI***
>
> *La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.*
>
> *Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad."*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en los apartados XI. Seguridad y ciberseguridad y XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos, señala:

> *"**XI. SEGURIDAD Y CIBERSEGURIDAD***
>
> *La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*

*La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…).*

*Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*

*La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información (…)"*

***(…) XIII. CONTINUIDAD Y DISPONIBILIDAD OPERATIVA DE LOS SERVICIOS TECNOLÓGICOS***

*La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estratega viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*

*La institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*

*La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción."*

La Guía para la elaboración de respaldos (TIC-GPR-0001), en los incisos *"3. Dispositivos"* y *"8 Recuperación",* indica lo siguiente:

*"3. Dispositivos*

*La política de copias de seguridad debe garantizar la reconstrucción de los archivos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.*

*Es recomendable contar con un sitio externo al sitio para guardar copias de respaldos como contingencia en caso de desastre.*

*8. Recuperación*

*Se deben definir mecanismos de comprobación de las copias de seguridad, aunque los propios programas que las efectúan suelen disponer de ellos para verificar el estado de la copia, es conveniente planificar dentro de las tareas de seguridad la restauración de una parte de la copia o de la copia completa periódicamente, como mecanismo de prueba y garantía."*

**Conclusiones**

El Directorio Activo es el encargado de almacenar información de objetos que conforman la red de una organización, autenticando el acceso de usuarios según las políticas de seguridad establecidas y los privilegios asignados, por lo tanto, ese componente tecnológico se ha vuelto una herramienta importante para obtener el ingreso a sistemas informáticos y datos gestionados por el negocio.

En virtud de su función e importancia, los cibercriminales han incrementado el interés en lograr el control de sus diversos componentes para infiltrarse de manera fraudulenta en la red, causar daños irremediables y extorsionar a sus víctimas.

Por lo tanto, resulta importante que la Institución analice los mecanismos de control interno implementados, la configuración y administración del Directorio Activo, con la finalidad de detectar oportunamente aspectos de mejora y minimizar así las brechas de ciberseguridad que puedan ocasionar la materialización de riesgos en torno a la vulneración de sistemas y datos sensibles, más aun considerando los recientes ciberataques ocurridos meses atrás a la Caja Costarricense de Seguro Social y otras instituciones públicas en Costa Rica, los cuales han sido ocasionados presuntamente por cibercriminales como CONTI y HIVE que utilizan entre sus mecanismos de ataque intentos de vulnerar la seguridad y configuración de sistemas como el AD.

Al respecto, este Órgano de Fiscalización y Control en su rol de asesor, informa sobre los aspectos esbozados en el presente oficio con el objetivo de que sean revisadas y analizadas por la administración activa y de considerarse conveniente, se efectúen las acciones para minimizar la materialización de riesgos asociados a ataques cibernéticos que afecten el Directorio Activo Institucional, perdida de información y detrimento en la prestación de los servicios brindados a través de tecnologías de información y comunicaciones.

Atentamente,

**AUDITORÍA INTERNA**

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.06 12:11:14 -06'00'

Lic. Olger Sánchez Carrillo
**Auditor**

OSC/RJS/RAHM/GMP/lbc

C. Auditoría