
# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
# INSTITUTO DE POSTGRADO

## TÍTULO

PRINCIPALES VULNERABILIDADES Y ACCIONES DE MITIGACIÓN RECOMENDADAS EN LA ADMINISTRACIÓN DEL ACTIVE DIRECTORY DE MICROSOFT

**AUTOR**

**Torres Alvarez Bernardo Miguel**

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

**TUTORA**

**Ing. Ana Eva Chacón Luna, Ph.D.**

**Santa Elena, Ecuador**

**Año 2024**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
# INSTITUTO DE POSTGRADO

## TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

**Ing. Alicia Andrade Vera, Mgtr.**
**COORDINADORA DEL PROGRAMA**

Firmado electrónicamente por:
ANA EVA CHACON LUNA

**Ing. Ana Eva Chacón Luna, Ph. D.**
**TUTOR**

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

**Ing. Jorge Zambrano Martínez, Ph. D.**
**DOCENTE ESPECIALISTA**

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

**Ing. Cesar Moreira Zambrano, Ph. D.**
**DOCENTE ESPECIALISTA**

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

**Abg. María Rivera González, Mgtr.**
**SECRETARIO GENERAL UPSE**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
# INSTITUTO DE POSTGRADO

## CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por TORRES ALVAREZ BERNARDO MIGUEL, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

**TUTORA**

Firmado electrónicamente por:
ANA EVA CHACON LUNA

**Ing. Ana Eva Chacón Luna, Ph.D.**

**Santa Elena, 14 de octubre de 2024**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
# INSTITUTO DE POSTGRADO

## DECLARACIÓN DE RESPONSABILIDAD

Yo, **TORRES ALVAREZ BERNARDO MIGUEL**

**DECLARO QUE:**

El trabajo de Titulación, Principales vulnerabilidades y acciones de mitigación recomendadas en la Administración del Active Directory de Microsoft, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 14 de octubre de 2024

## EL AUTOR

Firmado electrónicamente por:
BERNARDO MIGUEL
TORRES ALVAREZ

**Bernardo Miguel Torres Alvarez**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE CIENCIAS DE LA INGENIERÍA
# INSTITUTO DE POSTGRADO

## CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Principales vulnerabilidades y acciones de mitigación recomendadas en la Administración del Active Directory de Microsoft", presentado por el estudiante, TORRES ALVAREZ BERNARDO MIGUEL fue enviado al Sistema Antiplagio Compilatio, presentando un porcentaje de similitud correspondiente al 2%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

BernardoTorres_tesis

2%
Textos sospechosos

1% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos

Nombre del documento: BernardoTorres_tesis.pdf
ID del documento: ceafec9a9d9b4e359a0495768bc0eb36fd916440
Tamaño del documento original: 429,84 kB
Autores: []

Depositante: ANA EVA CHACON LUNA
Fecha de depósito: 14/10/2024
Tipo de carga: interface
fecha de fin de análisis: 14/10/2024

Número de palabras: 6039
Número de caracteres: 42.899

**TUTORA**

Firmado electrónicamente por:
ANA EVA CHACON LUNA

**Ing. Ana Eva Chacón Luna, Ph.D.**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
# INSTITUTO DE POSTGRADO

## AUTORIZACIÓN

Yo, **TORRES ALVAREZ BERNARDO MIGUEL**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo de Examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este trabajo de Examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, 14 de octubre de 2024

## EL AUTOR

Firmado electrónicamente por:
BERNARDO MIGUEL
TORRES ALVAREZ

**Bernardo Miguel Torres Alvarez**

# AGRADECIMIENTO

Deseo expresar mi más profundo agradecimiento a todas las personas que, de alguna manera, han sido esenciales para este logro académico. En primer lugar, agradezco a mi pareja y a mi familia, quienes siempre han sido mi apoyo y fuente de inspiración. Su respaldo incondicional me ha impulsado a seguir adelante.

A mis profesores, quienes con su orientación y conocimientos me han ayudado a ampliar mis habilidades y perspectiva en el campo de estudio, les estoy profundamente agradecido. Su dedicación y compromiso fueron cruciales para el desarrollo de esta investigación.

A mi directora de tesis, por su valiosa guía, paciencia y conocimientos compartidos. Su orientación fue fundamental para mantener el enfoque adecuado y mejorar la calidad de esta investigación.

*Bernardo Miguel Torres Alvarez*

# DEDICATORIA

A mi esposa, por su amor incondicional y su apoyo constante, que me han dado la fuerza para seguir adelante. A mis padres y hermanos, por ser siempre mis guías y haberme hecho quien soy, a mi tío que me verá terminar este proyecto desde donde esté y a mis abuelos que me han enseñado a ser fuerte y no rendirme. Gracias a todos por estar siempre a mi lado.

*Bernardo Miguel Torres Alvarez*

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS



# ÍNDICE DE TABLAS

## Resumen.

La investigación tiene como objetivo identificar y analizar las principales vulnerabilidades en la administración de Active Directory (AD) de Microsoft, derivadas de configuraciones incorrectas o malas prácticas de administración y proponer acciones de mitigación específicas para cada vulnerabilidad. Se emplea una metodología cualitativa que combina una revisión exhaustiva de literatura técnica reciente y el análisis de vulnerabilidades clasificadas en el sistema Common Vulnerabilities and Exposures (CVE) y evaluadas mediante Common Vulnerability Scoring System (CVSS). Como resultado, se identificaron 104 vulnerabilidades documentadas en los últimos cuatro años relacionadas con Active Directory, de las cuales 12 fueron calificadas como críticas u con una puntuación CVSS de 9.8 y 10. Entre las conclusiones destaca la necesidad de aplicar parches en tiempos específicos, implementar controles basados en ISO 27001:2022 y usar mapas de calor para priorizar vulnerabilidades según su impacto. Estas medidas buscan optimizar la seguridad de AD, garantizar la continuidad operativa y fortalecer la protección de las redes empresariales.



**Palabras clave:** Directorio Activo, Vulnerabilidades, ISO 27001:2022, Mitigación de riesgos.

# Abstract

The research aims to identify and analyze the main vulnerabilities in the administration of Microsoft's Active Directory (AD), arising from incorrect configurations or poor management practices, and to propose specific mitigation actions for each vulnerability. A qualitative methodology is employed, combining a thorough review of recent technical literature and the analysis of vulnerabilities classified in the Common Vulnerabilities and Exposures (CVE) system and evaluated using the Common Vulnerability Scoring System (CVSS). As a result, 104 documented vulnerabilities related to Active Directory were identified over the past four years, of which 12 were rated as critical with a CVSS score of 9.8 and 10. The conclusions highlight the need to apply patches within specific timeframes, implement controls based on ISO 27001:2022, and use heat maps to prioritize vulnerabilities according to their impact. These measures aim to optimize AD security, ensure operational continuity, and strengthen the protection of enterprise networks.



**Keywords:** Active Directory, Vulnerabilities, ISO 27001:2022, Risk Mitigation.

# 1. Introducción.

El Active Directory (AD) de Microsoft es una herramienta clave para la administración centralizada de usuarios, recursos y políticas en redes empresariales. Su importancia lo convierte en un blanco atractivo para atacantes, especialmente cuando no se gestiona adecuadamente. Este trabajo aborda vulnerabilidades críticas de AD, documentadas en los últimos 4 años y derivadas de configuraciones incorrectas, errores humanos y o aplicaciones desactualizadas que utilizan AD para su funcionamiento. Además, propone acciones de mitigación específicas para cada vulnerabilidad, La investigación incluye un análisis detallado de vulnerabilidades recientes clasificadas por CVE y evaluadas con CVSS, y se apoya en herramientas visuales como mapas de calor para priorizar riesgos. Este enfoque busca contribuir al fortalecimiento de la seguridad de AD, promoviendo buenas prácticas y una administración proactiva para prevenir ataques y garantizar la continuidad operativa de las organizaciones por lo que recomienda incluir la norma ISO 27001:2022 en la construcción e implementación del sistema de gestión de seguridad de la información.

## Objetivos

### Objetivo General

Determinar las principales vulnerabilidades en Active Directory de Microsoft derivadas de una administración incorrecta y medidas específicas de mitigación para optimizar la seguridad de la herramienta en entornos empresariales.

### Objetivos Específicos

- Investigar las vulnerabilidades detectadas en Active Directory en los últimos cuatro años, utilizando fuentes de la industria y reportes técnicos relevantes.
- Analizar las vulnerabilidades de mayor impacto en la seguridad tomando en cuenta su calificación CCVS.
- Proponer un conjunto de acciones preventivas y correctivas para mitigar las vulnerabilidades más peligrosas, con base en estándares de seguridad y buenas prácticas recomendadas por Microsoft y organizaciones internacionales.

## Alcance

Este estudio se enfoca en la identificación y análisis de las vulnerabilidades más significativas en Active Directory de Microsoft que resultan de configuraciones incorrectas o descuidos por parte de los administradores al no aplicar actualizaciones y parches de seguridad. El alcance abarca el análisis de vulnerabilidades documentadas en los últimos cuatro años y que han tenido un impacto crítico en la seguridad de redes empresariales. La investigación se limita a la revisión de informes técnicos, publicaciones académicas y vulnerabilidades documentadas por organizaciones internacionales. No se pretende ofrecer una revisión exhaustiva de todas las vulnerabilidades posibles, sino centrarse en aquellas que presentan los mayores riesgos debido a errores en la administración. Además, se propondrán medidas concretas para mitigar las vulnerabilidades más críticas, proporcionando un marco de referencia útil para administradores de sistemas y profesionales de TI.

## Importancia del estudio

La relevancia de este estudio radica en la necesidad creciente de garantizar la seguridad en la infraestructura tecnológica de las empresas, donde Active Directory juega un papel fundamental. Dado que AD es responsable de la administración centralizada de usuarios, equipos y recursos de red, cualquier vulnerabilidad no mitigada puede tener graves repercusiones en la integridad, confidencialidad y disponibilidad de los datos. La explotación de estas vulnerabilidades podría permitir ataques que comprometan la seguridad de toda la organización.

La importancia del estudio también reside en su contribución a la comprensión y mitigación de los riesgos asociados a una configuración inadecuada de Active Directory. A pesar de las guías y recomendaciones existentes, es frecuente que los administradores de sistemas cometan errores o no consideren adecuadamente las implicaciones de ciertas configuraciones o riesgos en la relación entre aplicaciones externas que utilizan a AD como administrador de credenciales de autenticación. Este estudio no solo identifica estas vulnerabilidades, sino que también propone acciones concretas para mitigarlas, sirviendo como una herramienta valiosa para mejorar la ciberseguridad en las organizaciones.

Al ofrecer una guía clara y basada en datos recientes, la investigación aportará al cuerpo de conocimiento en seguridad informática y ayudará a los profesionales de TI a mejorar la administración de sus entornos de Active Directory, fortaleciendo así la protección de sus redes.

### 1.1. Metodología.

La presente investigación sobre Active Directory de Microsoft es de carácter cualitativo y se desarrollará en dos fases principales:

Primero se realizará la revisión de la literatura, se llevará a cabo una revisión exhaustiva de la literatura académica y técnica disponible. Esto incluirá el análisis de informes de seguridad, guías de mejores prácticas y estudios previos sobre vulnerabilidades en Active Directory. Se prestará especial atención a las publicaciones de los últimos cuatro años para garantizar la relevancia y actualidad de los datos utilizados. Esta revisión permitirá contextualizar las vulnerabilidades más comunes y los riesgos asociados a una configuración incorrecta de Active Directory.

Luego se realizará una búsqueda de las vulnerabilidades publicadas en los últimos 4 años con un identificador del sistema CVE relacionadas con AD, estas vulnerabilidades se clasificarán según la puntuación dada por CVSS y se analizarán las que tienen una puntuación de 9.8 y 10. Este proceso permitirá priorizar las vulnerabilidades según su nivel de impacto y facilitará el desarrollo de propuestas de mitigación basadas en la naturaleza de la vulnerabilidad.

## 2. Marco Teórico.

### 2.1. Active Directory (AD)

Un directorio es un conjunto de datos ordenados de forma jerárquica, que facilita el acceso, administración y búsqueda de información.

Active Directory almacena información de los objetos y cuentas de una red, facilita su búsqueda y uso por parte de los usuarios y administradores, los objetos

incluyen recursos compartidos como servidores, volúmenes, impresoras, etc. (Foulds, Microsoft Learn, 2023)

Es una herramienta muy potente que permite desplegar políticas administrativas a diferentes grupos según corresponda, pudiendo dividir la infraestructura en departamentos, jerarquías, etc. Esto es imprescindible para evitar que cuentas tengan más privilegios de los que corresponde, “De cualquier forma un producto altamente tecnológico no es simple de poner en producción” (Francis, 2021),

### 2.1.1. Almacén de datos de directorio.

Active Directory utiliza cuatro tipos de particiones, estas contienen datos de dominio, configuración, esquema y aplicación, esta información se almacena en controladores de dominio, servidores esenciales en una red, encargado de gestionar y organizar todos los recursos, como usuarios, grupos y permisos. Este servidor proporciona servicios de autenticación y autorización, asegurando que solo los usuarios autorizados puedan acceder a los recursos de la red. El controlador de dominio utiliza Active Directory para almacenar y organizar la información de los objetos de la red en una base de datos distribuida, garantizando redundancia y alta disponibilidad de los datos.

- **Datos de dominio.**
  Contienen información sobre los objetos de un dominio, contactos de correo electrónico, atributos de equipos y cuentas de usuario.

- **Datos de configuración.**
  Datos que describen la topología del directorio, incluyen una lista de todos los dominios, árboles y bosques, ubicaciones de los controladores de dominio y catálogos globales.
- **Datos de esquema.**
  Los datos de esquema son la definición formal de todos los objetos y atributos que puede almacenar el directorio. Los administradores

pueden ampliar y modificar el esquema, definiendo nuevos tipos de objetos y atributos. Los objetos de esquema están protegidos por listas de control de acceso, garantizando que solo los usuarios autorizados puedan modificar el esquema.

- **Datos de la aplicación.**
  Los datos de esta partición están pensados para información que debe replicarse, pero no a escala global, los datos de la aplicación no forman parte del almacén de datos del directorio de forma predeterminada, sino que deben ser creados y configurados por el administrador.

### 2.1.2. Replicación de datos.

Los datos del directorio deben residir en más de un lugar de la red, esto garantiza el acceso eficiente para todos los usuarios, reduciendo la carga de los demás controladores de dominio. Active Directory usa un modelo de replicación maestro, esto permite realizar cambios para de directorio en cualquier controlador y no solo en el principal.

Todos los controladores de dominio de un bosque contienen una réplica del esquema, las particiones de configuración del bosque, los datos de dominio y el catálogo global.

Active Directory utiliza un comprobador de coherencia de conocimientos (KCC), este proceso se ejecuta en cada controlador de dominio e identifica automáticamente la topología de replicación más eficaz para la red. El KCC vuelve a calcular periódicamente la topología de replicación para ajustarla a los posibles cambios que se hayan producido, este proceso determina la topología de replicación entre sitios.

### 2.1.3. Controladores de dominio.

Un controlador de dominio es un servidor, físico o virtual, que ejecuta una versión de Windows Server y tiene instalados los servicios de Active Directory.

Cada controlador de dominio almacena los objetos y particiones del directorio qué serán replicados en otros controladores en el mismo dominio. El dominio puede tener cualquier cantidad de controladores de dominio como necesite, dependiendo del tamaño de la infraestructura, ubicación geográfica o segmentación de red.

Antes de Windows NT, aunque podían existir múltiples controladores de dominio, solo uno podía tener el rol de maestro de esquema, esto significa que los cambios en el directorio solo podían hacerse en un controlador en específico, actualmente pueden coexistir varios maestros de esquema en el mismo dominio. (Francis, 2021)

### 2.1.4. Árbol y bosque.

El esquema de Active Directory se puede describir como un árbol, donde la raíz es el dominio, de él nacen diferentes nodos y de ellos salen los objetos como grupos, usuarios y equipos esto se puede observar en la Ilustración 1.

Un bosque es la agrupación de varios árboles de dominio.

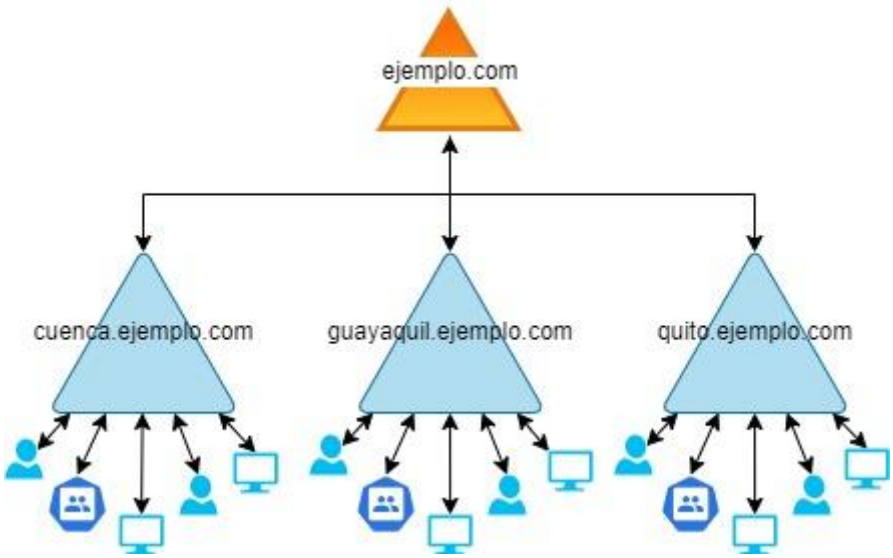


**Ilustración 1. Estructura árbol de dominio**

### 2.1.5. Roles FSMO.

Los roles son permisos especiales que se reparten entre uno o varios controladores de dominio para administrar acciones específicas. Estos roles pueden afectar las acciones cotidianas como la replicación. (Han, 2024)

Podemos utilizar el comando Netdom query FSMO en el power Shell del controlador de dominio para visualizar los roles que tienen ese controlador de dominio, esto se observa en la Ilustración 2.

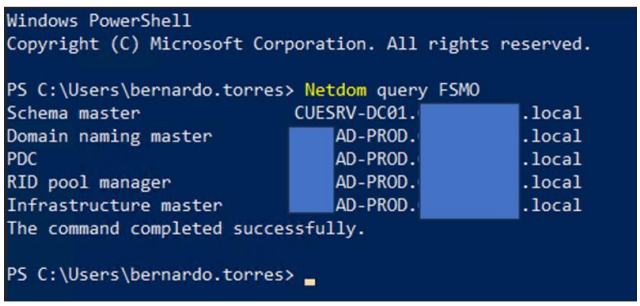


**Ilustración 2. Roles FSMO en un controlador de dominio**

A continuación, se describe los roles que se encuentran asignados al controlador de dominio en la Ilustración 2:

**Maestro de Esquema:** Es el controlador de dominio que realiza las actualizaciones en el esquema del directorio, es decir modifica la nomenclatura del esquema, una vez completada la actualización del esquema, este se réplica del maestro hacia los demás controladores de dominio del directorio, solo existe uno por cada bosque. (Ruiz-Ibáñez, 2019)

**Maestro de nombres del dominio:** Este controlador de dominio es el encargado de dar seguimiento a los nombres de los objetos en todo el bosque, garantizando que sean únicos, así mismo rastrea referencias cruzadas a objetos en otros dominios.

**Emulador PDC:** Este controlador de dominio emula tener compatibilidad con sistemas Windows NT.

**Maestro RID:** Este rol permite que un controlador de dominio de seguimiento a la asignación de Identificadores de Seguridad (SIDs).

### 2.1.6. Objetos en Active Directory.

Los objetos de Active Directory son representaciones lógicas de usuarios, departamentos, computadores, etc. Que conforman la organización.

**Usuarios:** Son aquellos miembros del dominio que son capaces de acceder a los sistemas miembro de la infraestructura corporativa de Active Directory.

Los usuarios pueden ser de personas físicas o genéricos para la ejecución de tareas específicas.

**Grupos:** Son unidades que permiten recopilar cuentas de usuario, computadores, etc. Para facilitar su administración, existen varios tipos de grupos:

- **Grupos de Seguridad:** Grupos que pueden proporcionar mecanismos de acceso a recursos compartidos de red de forma controlada. Permite asignar permisos y derechos de usuario (Rights User). Los derechos de usuario se asignan para determinar las acciones que están permitidas para los miembros de cierto grupo dentro de un dominio o bosque. Algunos derechos se asignan por defecto al instalar Active Directory.
- **Grupos de Distrubución:** Grupos utilizados para crear listas de distribución de correo electrónico.

**Unidades organizativas:** Las unidades organizativas (OU) son una subdivisión dentro de Active Directory, pueden contener usuarios, grupos, equipos y otras unidades organizativas. Permiten implementar permisos y directivas de grupo a múltiples objetos simultáneamente y de forma jerárquica.

**ACL: Las listas de control de acceso almacenan las entradas de control de acceso (ACE), cada ACE identifica un administrador y especifica sus derechos de acceso permitidos, denegados o auditados.**

## 2.2. Seguridad en Active Directory

Los ataques contra infraestructura informáticas aumentan constantemente en todo el mundo, a la par las técnicas para mitigar estas amenazas se ven obligadas a transformarse y evolucionar de forma similar, se debe tener siempre en cuenta que ninguna infraestructura tecnológica es totalmente inmune a los ataques.

Es imprescindible identificar las vulnerabilidades de nuestros sistemas para implementar acciones preventivas de mitigación, reduciendo así el área de ataque o minimizando el impacto en caso de que una vulnerabilidad llegue a ser explotada.

### 2.2.1. Vulnerabilidades Comunes.

#### 2.2.1.1. Puntos de entrada comunes

Los objetivos iniciales suelen ser aquellas áreas de la infraestructura de TI donde los atacantes pueden penetrar con mayor facilidad, por lo general son brechas de seguridad o actualizaciones que se pueden aprovechar para conseguir acceso a un sistema dentro de una infraestructura. (Foulds, Microsoft Learn, 2023)

Las vulnerabilidades más comunes son:

- Lagunas en la implementación del antivirus y antimalware.
- Aplicación de revisiones incompletas.
- Aplicaciones y sistemas operativos obsoletos.
- Errores de configuración.
- Falta de buenas prácticas de seguridad en el desarrollo de aplicaciones.

#### 2.2.1.2. Robo de credenciales

Los atacantes obtienen acceso mediante el uso de herramientas que permiten extraer credenciales de las sesiones de cuentas que tienen iniciada sesión en ese momento, por lo general se dirigen a cuentas que tienen ya privilegios elevados, evitando tener que realizar una escalada de privilegios para obtener acceso al sistema. (Mokhtar, Jurcut, ElSayed, & Azer, 2022)

- Los ataques suelen centrarse en los tipos de cuentas listados a continuación:
- Cuentas con privilegios permanentes.
- Cuentas VIP.

- Cuentas de Active Directory conectadas con privilegios.
- Controladores de dominio.

Los usuarios cuyas cuentas tienen privilegios elevados corren riesgo de robo de credenciales cuando realizan los estos comportamientos:

- Inicio de sesión en sus cuentas con privilegios en equipos no protegidos
- Exploración de Internet mientras tienen una sesión iniciada en una cuenta con privilegios

Otras prácticas que ponen en riesgo las credenciales del sistema son:

- Configuración de cuentas con privilegios locales con las mismas credenciales en todos los sistemas.
- Asignación de demasiados usuarios a grupos de dominio con privilegios, lo que fomenta el uso excesivo.
- Administración insuficiente de la seguridad del controlador de dominio.

### 2.2.2. Planeamiento de respuesta.

Aunque se implementen múltiples medidas preventivas de mitigación es importante elaborar planes de respuesta ante posibles escenarios de ataque y vulnerabilidades explotadas.

#### 2.2.2.1. Detección y contención inmediata:

**Monitoreo y Detección:** Se debe utilizar herramientas de monitoreo que permitan identificar actividades sospechosas, revisar registros de eventos y buscar inicios de sesión o cambios anormales.

**Aislamiento:** Aísla los sistemas comprometidos para evitar la propagación del ataque, desconecta de la red los controladores de dominio afectados si es necesario.

#### 2.2.2.2. Evaluación del Daño:

**Identificación de cuentas comprometidas:** Revisa constantemente el entorno de AD para detectar cuentas de usuario no reconocidas y otros indicadores.

**Revisión de cambios:** Revisa cambios en la configuración del AD, considerando cambios en las políticas de grupo o pertenencias a grupos de administradores.

#### 2.2.2.3. Recuperación y restauración:

**Restauración de controladores de dominio:** Es importante tener copias de seguridad de los controladores de dominio por si es necesario restaurarlos luego de un ataque.

**Reforzamiento de permisos:** Es necesario auditar y reforzar privilegios de las cuentas para restringir el acceso a cuentas no autorizadas.

#### 2.2.2.4. Prevención de futuros ataques:

**Implementación de políticas de seguridad:** Establece el uso de contraseñas seguras y políticas de autentificación multifactor.

**Actualización de Seguridad:** Es imprescindible mantener todos los sistemas y aplicaciones actualizados.

**Capacitación y concienciación:** Mantener capacitado al personal sobre las mejores prácticas de seguridad y como identificar posibles amenazas ayuda a mitigar múltiples vulnerabilidades en un entorno tecnológico cambiante.

## 2.3. Corporación MITRE, CVE y CVSS

### 2.3.1. Organización MITRE

MITRE es una organización sin fines de lucro fundada en 1958, con sede en McLean, Virginia, y Bedford, Massachusetts, en los Estados Unidos. Su misión es resolver problemas para un mundo más seguro a través de la innovación y la colaboración en áreas como la ciberseguridad, la defensa, la salud y la aviación. MITRE gestiona varios centros de investigación y desarrollo financiados por el gobierno federal de los Estados Unidos, conocidos como Federally Funded Research and Development Centers (FFRDCs).

La iniciativa de MITRE nace de la necesidad de proporcionar soluciones tecnológicas avanzadas y asesoramiento estratégico al gobierno de los Estados Unidos. A lo largo de los años, MITRE ha expandido su alcance para abordar desafíos globales en múltiples sectores, trabajando en estrecha colaboración con agencias gubernamentales, la industria y el mundo académico

### 2.3.2. Vulnerabilidades y exposiciones comunes (CVE)

El sistema Common Vulnerabilities and Exposures (CVE) es un esfuerzo internacional iniciado en 1999 para identificar y catalogar vulnerabilidades de seguridad en software y hardware. Cada vulnerabilidad recibe un identificador único conocido como número CVE, lo que facilita la comunicación y el intercambio de información entre organizaciones y profesionales de la seguridad.

### 2.3.3. Autoridades de Numeración de CVE (CNA)

Las CNA son organizaciones autorizadas para asignar identificadores CVE y realizar publicaciones de vulnerabilidades de seguridad, estas entidades son responsables de identificar vulnerabilidades, asignarles un número CVE único y documentar la información relevante para su publicación.
Entre las CNE se encuentran fabricantes de software como Microsoft, Google y Oracle, organizaciones de seguridad como INCIBE-CERT de España, MITRE a más de coordinar el sistema CVE también es una CNA.

### 2.3.4. Sistema común de puntuación de vulnerabilidades (CVSS)

El Common Vulnerability Scoring System (CVSS) es un marco estandarizado para evaluar la gravedad de las vulnerabilidades en sistemas informáticos y software, lanzado por primera vez en 2005, implementa un método coherente y objetivo para calificar vulnerabilidades, permitiendo priorizar esfuerzos de remediación en función de la gravedad de las vulnerabilidades.

El CVSS está bajo la custodia del Foro de Respuesta a Incidentes y equipos de Seguridad (FIRST), una organización internacional que promueve la cooperación y coordinación en la respuesta a incidentes de seguridad en sistemas informáticos y software.

CVSS utiliza 3 métricas para calcular la puntuación de una vulnerabilidad:
Métrica base: Son las características intrínsecas de la vulnerabilidad que son constantes en el tiempo y en el entorno del usuario.
Métricas temporales: Reflejan las características de la vulnerabilidad que puede cambiar con el tiempo, debido entre otras a la disponibilidad de parches.
Métricas ambientales: Consideran el entorno específico del usuario y como la vulnerabilidad afecta a la organización.

## 2.4. Autentificación mediante Kerberos.

Kerberos es un protocolo de autentificación de red que mediante un tercero de confianza permite a los usuarios y sistemas comprobar su identidad, fue desarrollado inicialmente en el Instituto Tecnológico de Massachusetts (MIT) (Ibáñez & López-Fuentes, 2017).

Como parte del proceso de autentificación se puede identificar claramente las siguientes partes:

**Cliente:** Es el usuario o sistema que solicita acceso a un servicio.

**Servidor de Aplicaciones (AS):** Es quien proporciona el servicio al que quiere acceder el cliente.

**Centro de Distribución de Claves (KDC):** Este es el componente central del protocolo, se divide en Servidor de Autentificación (AS) que verifica las credenciales del cliente y emite un Ticket de Concesión de Tickets (TGT) y servidor de concesión de Tiquetes (TGS) que emite los tickets de servicio basados en el TGT.

El proceso de autentificación de Kerberos es:

**Solicitud de Autenticación Inicial (AS-REQ):**
El cliente envía una solicitud de autenticación al AS, incluyendo su identidad.

**Respuesta del Servidor de Autenticación (AS-REP):**
El AS verifica las credenciales del cliente y, si son válidas, envía un TGT cifrado con la clave secreta del cliente.

**Solicitud de Tiquete de Servicio (TGS-REQ):**
El cliente descifra el TGT y lo usa para solicitar un tiquete de servicio al TGS, especificando el servicio al que desea acceder.

**Respuesta del Servidor de Concesión de Tiquetes (TGS-REP):**
El TGS verifica el TGT y, si es válido, emite un tiquete de servicio cifrado con la clave secreta del servidor de aplicaciones.

**Solicitud de Servicio (AP-REQ):**
El cliente envía el tiquete de servicio al servidor de aplicaciones para solicitar acceso al servicio.

**Respuesta del Servidor de Aplicaciones (AP-REP):**
El servidor de aplicaciones verifica el tiquete de servicio y, si es válido, concede acceso al cliente.

## 2.5. Autentificación SAML SSO (Single Sign-On).

SALM son las siglas para referirse a Lenguaje de marcado de aserción de seguridad, es un sistema basado en XML y se usa para intercambiar datos de autentificación y autorización.

Podemos identificar dos partes, el proveedor de identidad (IdP) y el proveedor de servicios (SP), el IdP realiza la autenticación del usuario y envía la información de identidad y nivel de autorización al SP, el SP confía en el proveedor de identidad y autoriza al usuario para acceder al recurso o servicio solicitad.

El servicio SSO permite que el usuario solo necesite iniciar sesión una vez para acceder a múltiples aplicaciones.

## 2.6. ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos

La norma ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta norma se centra en la seguridad de la información, la ciberseguridad y la protección de la privacidad. (International Organization for Standardization, 2022)

Para la implementación de la norma es imprescindible contar con compromiso de la alta dirección, puesto que se requerirá de la asignación de recursos.

Una vez socializado con la alta dirección se debe definir el alcance del sistema de gestión de seguridad de la información (SGSI), especificando límites y aplicabilidad dentro de la organización, en base a este alcance se desarrollará y aprobará políticas de seguridad de la información en la que se definirá categorías de riesgo desde aceptables hasta críticos y los criterios de evaluación.

Con las políticas aprobadas se realizará una evaluación de riesgos y se establecerá un plan de tratamiento de riesgos donde se debe incluir medidas para gestionarlos.

En base a los controles que la norma plantea en el Anexo 2, se debe establecer un documento de declaración de aplicabilidad, donde se liste los controles seleccionados para aplicar en la organización, se justifique su necesidad, se describa el estado de implementación de los controles en los diferentes procesos y finalmente una guía para las auditorías internas y externas.

Una vez redactados y aprobados estos documentos se procede a la implementación de los controles de seguridad necesarios para mitigar los riesgos según la prioridad determinada durante su evaluación. Es imprescindible realizar campañas de formación y concienciación en la organización para capacitar al personal sobre las políticas, procedimientos y controles de seguridad de la información.

Es importante establecer procedimientos de monitoreo y revisión del SGSI, asegurando su efectividad continua, realizando auditorías internas periódicas, así como revisiones por parte de la alta dirección en intervalos planificados para evaluar la conformidad del SGSI con los requisitos de la norma y su correcta implementación en la organización.

En base a los resultados de estas auditorías y revisiones periódicas se deberán tomar acciones de mejora continua, que permitan al SGSI estar actualizado y

vigente en conformidad con la naturaleza cambiante de las organizaciones y el entorno tecnológico.

# 3. Desarrollo.

## 3.1. Vulnerabilidades de Active Directory con identificador CVE de los últimos 4 años.

Al desarrollar una búsqueda de vulnerabilidades en la página web de CVE y utilizando como palabras clave Active Directory arroja 259 resultados de los cuales 104 han sido publicadas desde 2020, en el Anexo 1 se presenta un listado de las vulnerabilidades con identificador CVE publicadas desde el año 2020 con su calificación CVSS.

En la Ilustración 3 se observa un mapa de calor de la relación entre los puntos CVSS y la severidad de las vulnerabilidades. (Instituto Nacional de Ciberseguridad (INCIBE), 2015)

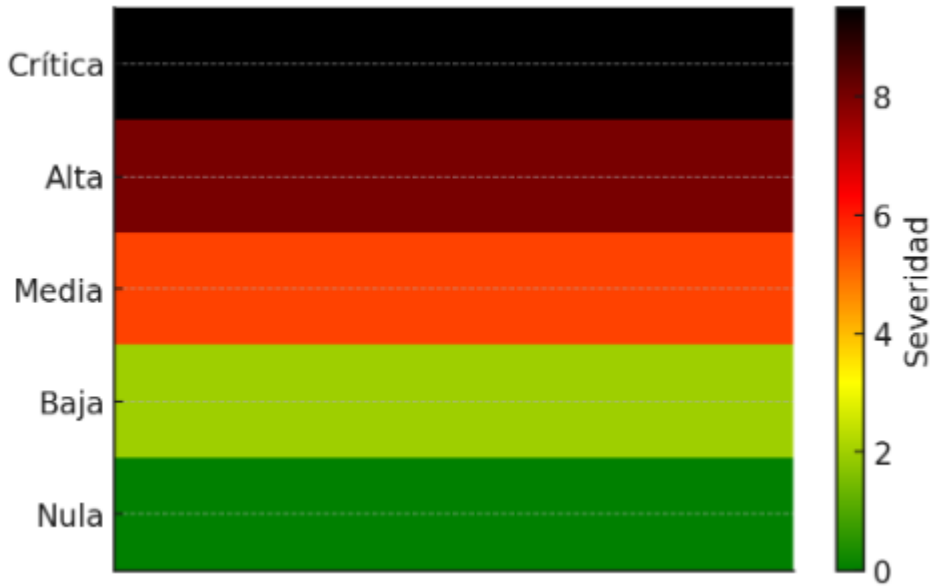


**Ilustración 3 Mapa de calor Puntuación vs Severidad**

A continuación, se describen las 12 vulnerabilidades que están consideradas como críticas y tienen calificaciones mayores o iguales a 9,8 y las acciones de mitigación recomendadas.

### 3.1.1. CVE-2023-48654, severidad crítica, calificación 9.8 (MITRE, CVE-2023-48654)

Esta vulnerabilidad se encuentra en versiones anteriores a la 5.13.1 de One Identify Password Mananger, aplicación que se integra a Active Directory y permite a los usuarios reestablecer sus propias contraseñas en la pantalla de inicio de sesión.

Para proporcionar esta funcionalidad se ejecuta un navegador basado en Chromium en modo kiosco del que el atacante logra escapar.

El atacante accede a la sección de Google ReCAPTCHA, que es parte del proceso para reestablecer la contraseña, hace clic en el enlace de privacidad abriendo una nueva ventana del navegador, utilizando esta ventana navega hacia cualquier otra que permita subir archivos, desde la ventana del explorador de archivos navega hasta cmd.exe y lo lanza con privilegios NT AUTHORITY\SYSTEM.

Esta vulnerabilidad permite al atacante obtener acceso al sistema afectado con privilegios elevados.

**Mitigación:**

- Actualizar One Identity Password Mananger a una versión superior 5.13.1.

### 3.1.2. CVE-2023-39069, severidad crítica, calificación 9.8. (MITRE, CVE-2023-39069)

Esta vulnerabilidad aprovecha como las aplicaciones TheHive y Cortex manejan la autentificación en Active Directory, estas herramientas están diseñadas para mejorar y documentar la respuesta a incidentes de seguridad.

Durante el proceso de configuración inicial en estas aplicaciones es necesario ingresar detalles del dominio, incluyendo direcciones de los controladores de dominio y el nombre del dominio, cuando el usuario intenta iniciar sesión las aplicaciones envían una solicitud de autentificación a Active Directory, en caso de que las credenciales sean válidas Active Directory responde con un token de autentificación que permite al usuario acceder.

Para realizar la explotación el atacante necesita tener acceso remoto a los sistemas donde se ejecutan las aplicaciones, el atacante envía una solicitud de autentificación a través de las API utilizando una cuenta existente, pero sin proporcionar la contraseña, debido a la vulnerabilidad AD responde con éxito a la solicitud incluso sin la contraseña válida.

Esto proporciona acceso con privilegios elevados a las aplicaciones, en el caso de TheHive al gestionar y coordinar actividades de respuesta a incidentes de seguridad un atacante podría manipular casos de incidentes o tener acceso a información sensible, así mismo en Cortex, que al analizar datos de amenazas y ejecutar respuestas automatizadas podría un atacante alterar las respuestas programadas, ejecutando comandos maliciosos o anulando la respuesta a incidentes.

**Mitigación:**

- Actualizar TheHive a la versión 5.0.8 o posterior y Cortex a la versión 3.1.6 o posterior.

### 3.1.3. CVE-2023-36655, severidad crítica, calificación 9.8. (MITRE, CVE-2023-36655)

Esta vulnerabilidad aprovecha la forma en la que ProLion CryptoSpike 3.0.15P2 maneja el proceso de autentificación, esta aplicación es una solución de seguridad diseñada para proteger sistemas de almacenamiento contra ataques de ransomware y proporcionar transparencia en el acceso a datos.

Esta aplicación se integra con Active Directory para manejar las credenciales y cuentas de usuario.

Para la explotación de esta vulnerabilidad el atacante va a realizar el proceso de autentificación para un usuario que se encuentre bloqueado, ingresando diferentes combinaciones de mayúsculas y minúsculas, el sistema interpretará como un usuario válido pero diferente del usuario que se encuentra bloqueado, generando un token de autentificación y permitiendo el acceso al sistema.

La naturaleza de la aplicación hace que un acceso no autorizado tenga un alto impacto, permitiendo al atacante desactivar la gestión de ataques de ramsonware.

**Mitigación:** Actualizar a una versión posterior de la ProLion CryptoSpike 3.0.15P2 o aplicar los parches lanzados por el fabricante.

### 3.1.4. CVE-2022-47966, severidad crítica, calificación 9.8. (MITRE, CVE-2022-47966)

La vulnerabilidad afecta a múltiples productos de Zoho ManageEngine que utilizan la biblioteca Apache Santuario xmlsec 1.4.1.

Entre los productos afectados se encuentran ServiceDesk Plus, ADManager Plus, entre otros.

La biblioteca Apache Santuario xmlsec 1.4.1 se utiliza para la seguridad XML, especialmente para la firma y cifrado de documentos XML.

Para explotar la vulnerabilidad es necesario que SAML SSO haya sido configurado alguna vez en el producto, y permite que un atacante no autenticado ejecute código arbitrario en el sistema.

La vulnerabilidad permite a los atacantes enviar aserciones SAML manipuladas que se aceptan como válidas, en este caso Active Directory puede ser utilizado como IdP para el sistema.

Una vez el atacante logra la autenticación tiene acceso a las aplicaciones que confían en Active Directory, comprometiendo potencialmente toda la infraestructura de TI, pudiendo ejecutarse movimientos laterales y obtener nuevas credenciales de los sistemas comprometidos.

**Mitigación:**

- Actualizar todos los productos Zoho ManageEngine a las versiones más recientes.

- Verificar que SAML SSO esté configurado correctamente.

- Implementar Autentificación Multifactor.

**3.1.5. CVE-2022-45141, severidad crítica, calificación 9.8.** (MITRE, CVE-2022-45141)

Esta vulnerabilidad afecta al protocolo SAMBA de Active Directory, aprovechando la debilidad del algoritmo RCA-HMAC para cifrar tickets de Kerberos para poder interceptarlos y manipularlos, consiguiendo así acceso con privilegios elevados al sistema.

Mitigación:

- Actualizar Samba a una versión que no utilice RC4-HMAC para cifrar los tickets de Kerberos, las versiones afectadas son hasta la 4.15.13 y desde la 4.16.0 hasta la 4.16.8, por lo que se debe actualizar a versiones superiores.

- Configurar el servidor para utilizar cifrados más seguros como AES256-CTS-HMAC-SHA1-96 para los tickets de Kerberos.

- Monitorear y auditar cualquier actividad sospechosa.

**3.1.6. CVE-2022-43400, severidad crítica, calificación 9.8.** (MITRE, CVE-2022-43400)

Esta vulnerabilidad afecta al sistema Siveillance Video Mobile Server V2022 R2, esta aplicación está diseñada por Siemens para la gestión y monitoreo de sistemas de videovigilancia, permitiendo a los usuarios acceder y gestionar al sistema de forma remota a través de sus dispositivos móviles.

La explotación de esta vulnerabilidad permite a un atacante remoto no autenticado acceder a la aplicación sin una cuenta válida.

Cuando un usuario intenta iniciar sesión en el aplicativo, el sistema en lugar de validar las credenciales del usuario únicamente verifica si pertenece al grupo administrador y en caso de ser afirmativo permite el acceso sin verificar que las credenciales sean correctas.

**Mitigación:**

- Actualizar Siveillance Video Mobile Server a la versión V22.2a (80) o superior.

- Revisa que las configuraciones de inicio de sesión en Active Directory estén correctamente implementadas y que solo las cuentas necesarias pertenezcan al grupo de administradores.

- Implementar autenticación multifactor.

- Monitorear y auditar para detectar cualquier acceso no autorizado.

**3.1.7. CVE-2021-37153, severidad crítica, calificación 9.8.** (MITRE, CVE-2021-37153)

Esta vulnerabilidad afecta a ForgeRock Access Management antes de su versión 7.0.2, esta aplicación permite una administración integral de autentificación para diferentes plataformas, siendo fácilmente integrable con Active Directory y otras plataformas que puedan cumplir el rol de almacén de identidad.

Esta vulnerabilidad requiere que ForgeRock AM se configure para utilizar Active Directory como su almacén de identidad.

Durante el proceso habitual el usuario intenta autenticarse en el sistema que utiliza ForgeRock AM, proporcionando las credenciales, esta aplicación envía una solicitud a Active Directory para verificar las credenciales, recibiendo como respuesta si las credenciales son o no validas, en este punto ForgeRock AM debería validar si la respuesta es legítima, es en este punto donde se presenta la vulnerabilidad, al no realizarse una correcta verificación un atacante podría enviar una respuesta maliciosa y la aplicación la aceptaría como auténtica.

Una vez autorizado el inicio de sesión el atacante tendría acceso a todos los sistemas donde se encuentre implementado ForgeRock AM.

**Mitigación:**

Actualizar ForgeRock AM a la versión 7.0.2 o superior.

Revisar configuraciones de seguridad entre Active Directory y ForgeRock AM para garantizar que se sigan las mejores prácticas, incluyendo la validación adecuada de respuestas de autenticación.

### 3.1.8. CVE-2021-23008, severidad crítica, calificación 9.8. (MITRE, CVE-2021-23008)

Esta vulnerabilidad compromete la autenticación en el sistema BIG-IP Access Policy Manager (APM), este sistema controla el acceso a aplicaciones y datos implementando políticas de acceso basadas en identidad.

El proceso de explotación puede realizarse interceptando la conexión KDC de Kerberos y el cliente mediante técnicas como el ataque de hombre en el

medio, también puede ejecutarse cuando el atacante tiene control de un servidor de AD.

El ataque se basa en enviar respuestas falsificadas al proceso de autenticación que la aplicación no valida correctamente y acepta como legítimas.
Una vez explotada la vulnerabilidad el atacante tiene acceso a todos los sistemas donde se encuentra implementado el sistema BIG-IP Access Policy Manager.

**Mitigación:**

- Actualizar BIG-IP, según la versión debe aplicarse la actualización:
    - BIG-IP APM 16.x: Corregido en la versión 16.1.0.
    - BIG-IP APM 15.x: Corregido en la versión 15.1.3.
    - BIG-IP APM 14.x: Corregido en la versión 14.1.4.
    - BIG-IP APM 13.x: Corregido en la versión 13.1.4.
    - BIG-IP APM 12.x: Corregido en la versión 12.1.6

- Implementar la validación KDC en el recurso de autenticación de AD para asegurar que las respuestas sean legítimas.

**3.1.9. CVE-2020-26542, severidad crítica, calificación 9.8.** (MITRE, CVE-2020-26542)

Esta vulnerabilidad se encuentra en el Plugin simple de LDAP para MongoDB, cuando se utiliza con Active Directory.

Esta vulnerabilidad permite que la autenticación se complete cuando se pasa un valor en blanco para la contraseña de la cuenta, es decir un atacante puede

autenticarse sin proporcionar una contraseña válida y obteniendo acceso con los privilegios asignados a la cuenta autenticada.

Durante el proceso de autenticación la vulnerabilidad se presenta en el momento en que Active Directory responde a la solicitud de autenticación, pero debido a una falla en el Plugin Simple LDAP, esta respuesta no se maneja correctamente y permite que la autenticación se complete correctamente.

**Mitigación:**

- Actualizar Percona Server para MongoDB a una versión actual, a partir del 9 de octubre de 2020 se corrige esta vulnerabilidad.

- Monitorear y auditar comportamientos extraños de autenticación.

**3.1.10. CVE-2020-2300, severidad crítica, calificación 9.8.** (MITRE, CVE-2020-2300)

Esta es una vulnerabilidad que afecta el plugin Active Directory de Jenkins, esta es una aplicación utilizada para el desarrollo de software y el plugin permite autenticarse desde el Active Directory.

La vulnerabilidad se presenta cuando está habilitada la opción ADSI, al permitir el plugin una contraseña en blanco y aprovechando que la operación de enlace no autenticado está habilitada en Active Directory el plugin puede tomar este enlace como una autentificación válida.

Esto permite que un usuario sin credenciales válidas se autentifique, obteniendo los privilegios de la cuenta autenticada.

**Mitigación:**

- Actualizar la versión del Jenkins Active Directory Plugin a una versión superior a la 2.19.

- Deshabilitar enlaces no autenticados.

- Monitoreo y auditoría para detectar intentos de acceso no autenticado.

**3.1.11. CVE-2020-2299, severidad crítica, calificación 9.8.** (MITRE, CVE-2020-2299)

Esta vulnerabilidad afecta al mismo Jenkins Active Directory Plugin, conde con una "Constante Mágica" utilizada como contraseña se puede autenticar con cualquier usuario, pese a no proporcionar una contraseña válida.

La documentación oficial de la vulnerabilidad no registra cual es el valor real de esta constante por razones de seguridad.

Estas constantes son comunes en el proceso de desarrollo de las aplicaciones, pero no deben estar en el código que será puesto en producción.

**Mitigación:**

- Actualizar el plugin a una versión superior a la 2.19.

- Monitoreo y auditoría para detectar inicios de sesión extraños.

**3.1.12. CVE-2021-37705, severidad crítica, calificación 10.** (MITRE, CVE-2021-37705)

Esta vulnerabilidad afecta a OneFuzz, una plataforma de Microsoft que permite realizar pruebas de seguridad a software en desarrollo, esta vulnerabilidad permite que un usuario autenticado en OneFuzz utilizando Azure Active Directory en cualquier inquilino, una incorrecta gestión de la autenticación por parte de OneFuzz permite que, aunque no se encuentre en el mismo inquilinio este usuario pueda hacer consultas API, esto puede generar acceso a lectura y manipulación de datos privados.

**Mitigación:**

- Actualizar OneFuzz a la versión 2.31.0 o superior.

- Como solución temporal los usuarios pueden restringir el acceso al inquilino de una instancia desplegada de OneFuzz en una versión vulnerable.

## 3.2. Controles que se deben incluir en el SGSI por su relación con AD

Como medida de mitigación general se recomienda de forma enfática basar el desarrollo e implementación del SGSI de la organización en la norma ISO/IEC 27001:2022, en la tabla a continuación se describe los controles que tienen relación con AD y deberán tenerse en cuenta en organizaciones que tengan implementada esta herramienta, según la naturaleza de cada organización se deberá definir las acciones de implementación específicas para cada control.

| Control | Descripción |
|---|---|
| **A.5.7 Inteligencia sobre amenazas** | Implementar mecanismos para recopilar y analizar información sobre amenazas que puedan afectar a AD. |
| **A.8.9 Gestión de configuración** | Asegurar que las configuraciones de AD sean gestionadas de manera segura y documentadas adecuadamente. |
| **A.8.10 Eliminación de información** | Garantizar que la información sensible en AD se elimine de manera segura cuando ya no sea necesaria. |
| **A.8.11 Enmascaramiento de datos** | Proteger la información sensible en AD mediante técnicas de enmascaramiento de datos. |
| **A.8.12 Prevención de fugas de datos** | Implementar controles para prevenir la fuga de información desde AD. |
| **A.8.15 Inicio de sesión** | Se almacenará y monitoreará continuamente actividades de inicio de sesión en busca de actividades o eventos relevantes. |
| **A.8.16 Actividades de monitoreo** | Monitorear continuamente las actividades en AD para detectar y responder a incidentes de seguridad. |
| **A.8.23 Filtrado web** | Controlar el acceso a sitios web desde sistemas que interactúan con AD para prevenir accesos no autorizados. |
| **A.8.28 Codificación segura** | Asegurar que las aplicaciones y scripts que interactúan con AD sigan prácticas de codificación segura. |

**Tabla 1 Controles de la ISO/IEC 27001:2022 relacionados con AD**

# 4. Análisis y Discusión de los resultados

El presente trabajo de titulación identificó 104 vulnerabilidades relacionadas con Active Directory (AD) documentadas en los últimos cuatro años, de las cuales 12 fueron catalogadas como críticas, con calificaciones CVSS de 9.8 y 10. Este hallazgo evidencia una preocupante recurrencia de fallos en la seguridad de una herramienta fundamental para la administración de usuarios, recursos y políticas en redes empresariales. A continuación, se analizan las implicaciones más relevantes de estos resultados y su relación con las estrategias propuestas para mitigar riesgos.

## Vulnerabilidades Identificadas y su Impacto

El hallazgo de vulnerabilidades críticas pone de manifiesto cómo configuraciones incorrectas, aplicaciones externas mal gestionadas y la falta de actualizaciones oportunas continúan siendo los principales factores que comprometen la seguridad de AD. Se observa que 8 de las 12 vulnerabilidades analizadas es decir el 67% se relaciona con la forma en que las aplicaciones externas interactúan con AD, lo que refuerza la importancia de una administración proactiva y el monitoreo continuo de estas integraciones.

Un ejemplo significativo es la vulnerabilidad CVE-2023-39069, que permite el acceso no autorizado a sistemas sensibles debido a fallos en la autenticación con aplicaciones como TheHive y Cortex. Este tipo de vulnerabilidades ilustra cómo los atacantes pueden explotar las dependencias de AD para obtener acceso elevado y causar daños significativos.

## Eficiencia de las Acciones de Mitigación Propuestas

Las acciones de mitigación recomendadas, como la actualización de sistemas vulnerables, la implementación de controles basados en ISO/IEC 27001:2022 y la autenticación multifactor, se alinean con las mejores prácticas de seguridad y abordan las causas raíz

de estas vulnerabilidades. En particular, el uso de mapas de calor para priorizar vulnerabilidades permite una asignación eficiente de recursos y fortalece las capacidades de respuesta ante incidentes.

Por ejemplo, la aplicación de parches en versiones obsoletas de software vulnerable, como One Identity Password Manager y Zoho ManageEngine, no solo mitiga riesgos inmediatos, sino que también contribuye a prevenir futuros ataques. Sin embargo, la implementación efectiva de estas medidas depende de la adopción de una cultura organizacional orientada hacia la ciberseguridad y el compromiso de la alta dirección.

**Rol de la Norma ISO/IEC 27001:2022**

La inclusión de controles basados en la norma ISO/IEC 27001:2022 destaca como un enfoque integral para gestionar riesgos y fortalecer la seguridad de AD. Los controles específicos, como la gestión de configuraciones (A.8.9), la prevención de fugas de datos (A.8.12) y el monitoreo continuo (A.8.16), son esenciales para abordar vulnerabilidades sistémicas y promover una administración más robusta.

Sin embargo, la implementación de estos controles puede enfrentar barreras significativas, como la falta de recursos especializados y la resistencia al cambio dentro de las organizaciones. Por lo tanto, es crucial acompañar estas iniciativas con capacitación al personal y la integración de soluciones tecnológicas que simplifiquen la aplicación de medidas de seguridad.

**Limitaciones y Recomendaciones Futuras**

Aunque el estudio proporciona un análisis exhaustivo de vulnerabilidades críticas, se reconoce que no abarca todas las posibles vulnerabilidades de AD. Además, las recomendaciones se centran en medidas reactivas, por lo que futuras investigaciones podrían explorar enfoques más proactivos, como el uso de inteligencia artificial para la detección temprana de amenazas.

Otra limitación radica en la dependencia de datos provenientes de fuentes externas, lo que podría omitir vulnerabilidades menos documentadas, pero igualmente relevantes. Por ello, se recomienda complementar este tipo de investigaciones con pruebas de penetración

personalizadas y auditorías internas que reflejen mejor el entorno específico de cada organización.

# 5. Conclusiones

Las vulnerabilidades identificadas en Active Directory (AD) resaltan la importancia de una administración activa y preventiva. La constante revisión de vulnerabilidades publicadas y el uso de herramientas como CVE y CVSS son esenciales para anticiparse a posibles incidentes de seguridad y priorizar los esfuerzos de mitigación según el nivel de impacto.

El 67% de las vulnerabilidades críticas identificadas están relacionadas con aplicaciones externas que interactúan con AD. Esto demuestra que no solo es importante gestionar adecuadamente AD, sino también monitorear y actualizar las aplicaciones que dependen de este para evitar posibles brechas de seguridad.

La integración de controles específicos basados en la norma ISO/IEC 27001:2022 fortalece significativamente la postura de seguridad de AD. Estos controles abarcan desde la gestión de configuraciones hasta la prevención de fugas de datos, y deben adaptarse a las necesidades específicas de cada organización.

El administrador de Active Directory debe ir más allá de la gestión técnica básica, documentando integraciones, supervisando configuraciones y fomentando una cultura de ciberseguridad que incluya monitoreo constante y actualización de sistemas.

Las medidas de mitigación propuestas deben ir acompañadas de programas de formación y sensibilización, tanto para el personal técnico como para los usuarios finales, con el fin de fomentar buenas prácticas de ciberseguridad y minimizar el riesgo humano.

# 6. Recomendaciones

Para mantener una actualización continua se debe implementar un cronograma de revisión periódica de vulnerabilidades publicadas en CVE y CVSS.

Para mantener una actualización proactiva se debe garantizar la aplicación oportuna de parches de seguridad tanto en Active Directory como en las aplicaciones que interactúan con este.

Basar las estrategias de seguridad en la norma ISO/IEC 27001:2022, priorizando controles como la gestión de configuraciones (A.8.9), la prevención de fugas de datos (A.8.12) y el monitoreo continuo (A.8.16).

Realizar auditorías internas frecuentes para evaluar la implementación y efectividad de estos controles.

Documentar todas las integraciones con AD y realizar pruebas regulares de seguridad en estas aplicaciones.

Implementar autenticación multifactor en todas las interacciones con AD.

Diseñar programas de capacitación enfocados en identificar amenazas y responder a incidentes de seguridad.

Evaluar la incorporación de herramientas basadas en inteligencia artificial para detectar anomalías en tiempo real.

Implementar mapas de calor como herramienta para priorizar la atención a las vulnerabilidades más críticas.

# 7. Bibliografía


Foulds, I. (03 de 08 de 2023). *Microsoft Learn*. Obtenido de https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Foulds, I. (15 de 10 de 2023). *Microsoft Learn*. Obtenido de https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Francis, D. (2021). *Mastering Active Directory Design, deploy, and protect Active Directory.* Birmingham: Packt Publishing.

Gopal, K. (10 de Febrero de 2022). *Exploiting the CVE-2021-42278 (sAMAccountName spoofing) and CVE-2021-42287 (deceiving the KDC) Active Directory vulnerabilities.* Obtenido de 4sysops - The online community for SysAdmins and DevOps: https://4sysops.com/archives/exploiting-the-cve-2021-42278-samaccountname-spoofing-and-cve-2021-42287-deceiving-the-kdc-active-directory-vulnerabilities/#:~:text=CVE-2021-42278%20%E2%80%93%20sAMAccountName%20spoofing.%20By%20default,%20a%20standard%20doma

Han, L. (19 de 02 de 2024). *Microsoft Learn*. Obtenido de https://learn.microsoft.com/es-es/troubleshoot/windows-server/active-directory/fsmo-roles

Ibáñez, J. A., & López-Fuentes, F. (2017). Autenticación para acceso a datos distribuidos. *Research in Computing Science*, 142.

International Organization for Standardization. (2022). *Information security management systems—Requirements with guidance for use* . ISO/IEC Standard No. 27001:2022: https://www.iso.org/standard/27001

MITRE. (04 de 11 de CVE-2020-2299). *CVE-2020-2299.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2020-2299

MITRE. (04 de 11 de CVE-2020-2300). *CVE-2020-2300.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2020-2300

MITRE. (09 de 11 de CVE-2020-26542). *CVE-2020-26542.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2020-26542

MITRE. (10 de 05 de CVE-2021-23008). *CVE-2021-23008.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2021-23008

MITRE. (25 de 08 de CVE-2021-37153). *CVE-2021-37153.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2021-37153

MITRE. (13 de 08 de CVE-2021-37705). *CVE-2021-37705.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2021-37705

MITRE. (21 de 10 de CVE-2022-43400). *CVE-2022-43400.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2022-43400

MITRE. (06 de 03 de CVE-2022-45141). *CVE-2022-45141.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2022-45141

MITRE. (18 de 01 de CVE-2022-47966). *CVE-2022-47966.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2022-47966

MITRE. (06 de 12 de CVE-2023-36655). *CVE-2023-36655.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2023-36655

MITRE. (11 de 09 de CVE-2023-39069). *CVE-2023-39069.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2023-39069

MITRE. (25 de 12 de CVE-2023-48654). *CVE-2023-48654.* Obtenido de https://www.cve.org/CVERecord?id=CVE-2023-48654

Mokhtar, B., Jurcut, A., ElSayed, M., & Azer, M. A. (2022). Active Directory Attacks—Steps, Types, and Signatures https://doi.org/10.3390/electronics11162629. *Electronics*, 11(16).

NUÑEZ, O. (2017). Active Directory (Directorio Activo) Sistema De Seguridad, Control y Privacidad de la Información en la Gobernación del Tolima. Santa Marta, Colombia: Universidad del Magdalena.

Ruiz-Ibáñez, M.-T. (05 de 09 de 2019). Metodología Técnica De Revisión De Directorio Activo. Jaén, Andalucía, España: Universidad de Jaén.

# 8. ANEXOS

## ANEXO 1 VULNERABILIDADES RELACIONADAS CON ACTIVE DIRECTORY QUE TIENEN IDENTIFICADOR CVE DE MITRE

| ANEXO 1 VULNERABILIDADES RELACIONADAS CON ACTIVE DIRECTORY QUE TIENEN IDENTIFICADOR CVE DE MITRE | | | |
|---|---|---|---|
| **Identificador** | **Descripción** | **Calificación CVSS** | **Severidad** |
| CVE-2024-4332 | Se ha identificado una vulnerabilidad de omisión de autenticación en los componentes de REST y SOAP API de Tripwire Enterprise (TE) 9.1.0 cuando TE está configurado para utilizar la autenticación SAML LDAP/Active Directory y su función opcional "Sincronización automática de usuarios, roles y grupos LDAP" está habilitada. Esta vulnerabilidad permite a los atacantes no autenticados eludir la autenticación si se conoce un nombre de usuario válido. La explotación de esta vulnerabilidad podría permitir a los atacantes remotos obtener acceso privilegiado a las API y conducir a la divulgación o modificación no autorizada de la información. | 9,3 | Crítico |
| CVE-2024-4129 | Vulnerabilidad de autenticación incorrecta en Snow Software AB Snow License Manager en Windows permite a un atacante en red realizar una omisión de autenticación si la autenticación de Active Directory está habilitada. Este problema afecta a Snow License Manager: desde la versión 9.33.2 hasta la 9.34.0. | 8,8 | Alto |
| CVE-2024-41108 | FOG es un sistema gratuito de clonación/imagen/rescate/gestión de inventario de código abierto. La página hostinfo tiene un control de acceso faltante o incorrecto, ya que solo se requiere la dirección MAC del host para obtener la información de configuración. Estos datos solo se pueden recuperar si hay una tarea pendiente en ese host. De lo contrario, se devolverá un mensaje de error que contiene "¡Tareas no válidas!". La contraseña de dominio en el volcado de hostinfo está oculta incluso para los usuarios autenticados, ya que se muestra como una fila de asteriscos al navegar a la configuración de Active Directory del host. Esta vulnerabilidad se corrigió en 1.5.10.41. | 7,5 | Alto |
| CVE-2024-3781 | Vulnerabilidad de inyección de comandos en el sistema operativo. La neutralización incorrecta de elementos especiales en la integración de Active Directory permite que el comando previsto se modifique cuando se envía a un componente descendente en WBSAirback 21.02.04. | 9,1 | Crítico |
| CVE-2024-37393 | Existen múltiples vulnerabilidades de inyecciones LDAP en SecurEnvoy MFA antes de 9.4.514 debido a una validación incorrecta de la entrada proporcionada por el usuario. Un atacante remoto no autenticado podría exfiltrar datos de Active Directory a través de ataques de inyección LDAP ciegos contra el servicio DESKTOP expuesto en el punto de conexión HTTP /secserver. Esto puede incluir ms-Mcs-AdmPwd, que tiene una contraseña de texto no cifrado para la característica Solución de contraseña de administrador local (LAPS). | 7,5 | Alto |
| CVE-2024-37085 | VMware ESXi contiene una vulnerabilidad de omisión de autenticación. Un actor malintencionado con suficientes permisos de Active Directory (AD) puede obtener acceso completo a un host ESXi que se configuró previamente para usar AD para la administración de usuarios https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html volviendo a crear el grupo de AD configurado ("Administradores de ESXi" de forma predeterminada) después de que se haya eliminado de AD. | 6,8 | Medio |
| CVE-2024-23465 | Se descubrió que SolarWinds Access Rights Manager era susceptible a una vulnerabilidad de omisión de autenticación. Esta vulnerabilidad permite a un usuario no autenticado obtener acceso de administrador de dominio dentro del entorno de Active Directory. | 8,3 | Alto |
| CVE-2024-22245 | Las vulnerabilidades de retransmisión de autenticación arbitraria y secuestro de sesión en el complemento de autenticación mejorada (EAP) de VMware obsoleto podrían permitir que un actor malintencionado que podría engañar a un usuario de dominio de destino con EAP instalado en su navegador web solicite y retransmita tickets de servicio para nombres principales de servicio (SPN) de Active Directory arbitrarios. | 9,6 | Crítico |
| CVE-2024-21381 | Vulnerabilidad de suplantación de identidad de Microsoft Azure Active Directory B2C | 6,8 | Medio |
| CVE-2024-1573 | La vulnerabilidad de autenticación incorrecta en la función de monitoreo móvil de ICONICS GENESIS64 las versiones 10.97 a 10.97.2, Mitsubishi Electric GENESIS64 versiones 10.97 a 10.97.2 y Mitsubishi Electric MC Works64 todas las versiones permite a un atacante remoto no autenticado eludir la autenticación adecuada e iniciar sesión en el sistema cuando se cumplen todas las siguientes condiciones: * Se utiliza Active Directory en la configuración de seguridad. * “ Inicio de sesión automático” está habilitada en la configuración de seguridad. * El grupo de aplicaciones IIS de IcoAnyGlass se ejecuta bajo una cuenta de dominio de Active Directory. * La cuenta del grupo de aplicaciones IcoAnyGlass IIS está incluida en GENESIS64TM y MC Works64 Security y tiene permiso para iniciar sesión. | 5,9 | Medio |
| CVE-2023-51772 | One Identity Password Manager anterior a 5.13.1 permite Kiosk Escape. Este producto permite a los usuarios restablecer sus contraseñas de Active Directory en la pantalla de inicio de sesión de un cliente de Windows. Lanza un navegador basado en Chromium en modo quiosco para proporcionar la funcionalidad de reinicio. La secuencia de escape es: esperar a que se agote el tiempo de espera de la sesión, hacer clic en el icono de Ayuda, observar que hay una ventana del navegador para el sitio web de One Identity, navegar a cualquier sitio web que ofrezca carga de archivos, navegar a cmd.exe desde la ventana del explorador de archivos e iniciar cmd.exe como NT AUTHORITY\SYSTEM. | 8,8 | Alto |
| CVE-2023-51663 | Hail es una herramienta de análisis de datos de código abierto, de propósito general, basada en Python, con tipos de datos y métodos adicionales para trabajar con datos genómicos. Hail se basa en las direcciones de correo electrónico de OpenID Connect (OIDC) de los tokens de ID para verificar la validez del dominio de un usuario, pero dado que los usuarios tienen la capacidad de cambiar su dirección de correo electrónico, podrían crear cuentas y usar recursos en clústeres a los que no deberían tener acceso. Por ejemplo, un usuario podría crear una cuenta de Microsoft o Google y, a continuación, cambiar su correo electrónico a "test@example.org". A continuación, esta cuenta se puede usar para crear una cuenta de Hail Batch en clústeres de Hail Batch cuyo dominio de organización sea "example.org". El atacante no puede acceder a datos privados ni hacerse pasar por otro usuario, pero tendría la capacidad de ejecutar trabajos si los proyectos de facturación por lotes de Hail están habilitados y crear inquilinos de Azure si tienen acceso de administrador de Azure Active Directory. | 5,3 | Medio |
| CVE-2023-5003 | El plugin de WordPress Active Directory Integration / LDAP Integration anterior a la versión 4.1.10 almacena los registros LDAP sensibles en un archivo de búfer cuando un administrador quiere exportar dichos registros. Desafortunadamente, este archivo de registro nunca se elimina y permanece accesible para cualquier usuario que conozca la URL para hacerlo. | 7,5 | Alto |
| CVE-2023-48654 | One Identity Password Manager anterior a 5.13.1 permite Kiosk Escape. Este producto permite a los usuarios restablecer sus contraseñas de Active Directory en la pantalla de inicio de sesión de un cliente de Windows. Lanza un navegador basado en Chromium en modo quiosco para proporcionar la funcionalidad de reinicio. La secuencia de escape es: vaya a la sección Google ReCAPTCHA, haga clic en el enlace Privacidad, observe que hay una nueva ventana del navegador, navegue a cualquier sitio web que ofrezca carga de archivos, navegue a cmd.exe desde la ventana del explorador de archivos e inicie cmd.exe como NT AUTHORITY\SYSTEM. | 9,8 | Crítico |
| CVE-2023-4757 | El complemento de WordPress Staff / Employee Business Directory para Active Directory antes de 1.2.3 no desinfecta y escapa los datos devueltos por el servidor LDAP antes de mostrarlos en la página, lo que permite a los usuarios que pueden controlar sus entradas en el directorio LDAP inyectar javascript malicioso que podría usarse contra usuarios con altos privilegios, como un administrador del sitio. | 5,4 | Medio |
| CVE-2023-4506 | El plugin Active Directory Integration / LDAP Integration para WordPress es vulnerable a LDAP Passback en versiones hasta la 4.1.10 inclusive. Esto se debe a una validación insuficiente al cambiar el servidor LDAP. Esto hace posible que los atacantes autenticados, con acceso administrativo y superior, cambien el servidor LDAP y recuperen las credenciales del servidor LDAP original. | 2,2 | Bajo |
| CVE-2023-4505 | El plugin Staff / Employee Business Directory for Active Directory para WordPress es vulnerable a LDAP Passback en versiones hasta, e inclusive, 1.2.3. Esto se debe a una validación insuficiente al cambiar el servidor LDAP. Esto hace posible que los atacantes autenticados, con acceso administrativo y superior, cambien el servidor LDAP y recuperen las credenciales del servidor LDAP original. | 2,2 | Bajo |
| CVE-2023-42796 | Se ha identificado una vulnerabilidad en CP-8031 MASTER MODULE (Todas las versiones < CPCI85 V05.11), CP-8050 MASTER MODULE (Todas las versiones < CPCI85 V05.11). El servidor web de los dispositivos afectados no puede desinfectar correctamente la entrada del usuario para el punto final /sicweb-ajax/tmproot/. Esto podría permitir que un atacante remoto autenticado atraviese los directorios del sistema y descargue archivos arbitrarios. Al explorar los ID de sesión activos, la vulnerabilidad podría aprovecharse para escalar los privilegios al rol de administrador. | 7,5 | Alto |
| CVE-2023-42670 | Se encontró una falla en Samba. Es susceptible a una vulnerabilidad en la que se pueden iniciar varios agentes de escucha RPC incompatibles, lo que provoca interrupciones en el servicio AD DC. Cuando el servidor RPC de Samba experimenta una carga alta o falta de respuesta, los servidores destinados a fines de DC que no son AD (por ejemplo, "DC clásicos" de emulación NT4) pueden iniciarse y competir erróneamente por los mismos sockets de dominio Unix. Este problema conduce a respuestas de consulta parciales del controlador de dominio de AD, lo que provoca problemas como "El número de procedimiento está fuera del intervalo" al usar herramientas como Usuarios de Active Directory. Esta falla permite a un atacante interrumpir los servicios de AD DC. | 6,5 | Medio |
| CVE-2023-4154 | Se encontró una falla de diseño en la implementación del control DirSync de Samba, que expone contraseñas y secretos en Active Directory a usuarios privilegiados y controladores de dominio de solo lectura (RODC). Esta falla permite a los RODC y a los usuarios que poseen el derecho GET_CHANGES acceder a todos los atributos, incluidos los secretos confidenciales y las contraseñas. Incluso en una configuración predeterminada, las cuentas de RODC DC, que solo deben replicar algunas contraseñas, pueden obtener acceso a todos los secretos de dominio, incluido el vital krbtgt, eliminando efectivamente la distinción RODC / DC. Además, la vulnerabilidad no tiene en cuenta las condiciones de error (fail open), como las situaciones de falta de memoria, lo que podría otorgar acceso a atributos secretos, incluso bajo la influencia de atacantes con pocos privilegios. | 7,5 | Alto |
| CVE-2023-39069 | Un problema en StrangeBee TheHive v.5.0.8, v.4.1.21 y Cortex v.3.1.6 permite a un atacante remoto obtener privilegios a través del mecanismo de autenticación de Active Directory. | 9,8 | Crítico |
| CVE-2023-37943 | Jenkins Active Directory Plugin 2.30 y versiones anteriores ignoran las opciones "Requerir TLS" y "StartTls" y siempre realizan la prueba de conexión al directorio activo sin cifrar, lo que permite a los atacantes capturar el tráfico de red entre el controlador Jenkins y los servidores de Active Directory obtener credenciales de Active Directory. | 5,9 | Medio |
| CVE-2023-36871 | Vulnerabilidad de omisión de características de seguridad de Azure Active Directory | 6,5 | Medio |
| CVE-2023-36722 | Vulnerabilidad de divulgación de información de Servicios de dominio de Active Directory | 4,4 | Medio |
| CVE-2023-36655 | La API REST de inicio de sesión en ProLion CryptoSpike 3.0.15P2 (cuando se utiliza LDAP o Active Directory como almacén de usuarios) permite a un usuario bloqueado remoto iniciar sesión y obtener un token de autenticación especificando un nombre de usuario con una combinación diferente de caracteres en mayúsculas y minúsculas. | 9,8 | Crítico |
| CVE-2023-35785 | Zoho ManageEngine Active Directory 360 versiones 4315 y anteriores, ADAudit Plus 7202 y versiones anteriores, ADManager Plus 7200 y versiones anteriores, Asset Explorer 6993 y versiones anteriores y 7xxx 7002 y versiones anteriores, Cloud Security Plus 4161 y versiones anteriores, Data Security Plus 6110 y versiones anteriores, Eventlog Analyzer 12301 y versiones anteriores, Exchange Reporter Plus 5709 y versiones anteriores, Log360 5315 y versiones anteriores, Log360 UEBA 4045 y versiones anteriores, M365 Manager Plus 4529 y versiones anteriores, M365 Security Plus 4529 y versiones anteriores, Recovery Manager Plus 6061 y versiones anteriores, ServiceDesk Plus 14204 y versiones anteriores y 143xx 14302 y versiones anteriores, ServiceDesk Plus MSP 14300 y versiones anteriores, SharePoint Manager Plus 4402 y versiones anteriores, y Support Center Plus 14300 y versiones anteriores son vulnerables a la omisión de 2FA a través de algunos autenticadores TOTP. Nota: Se requiere un par válido de nombre de usuario y contraseña para aprovechar esta vulnerabilidad. | 8,1 | Alto |
| CVE-2023-35351 | Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability | 6,6 | Medio |
| CVE-2023-35350 | Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability | 7,2 | Alto |
| CVE-2023-35348 | Active Directory Federation Service Security Feature Bypass Vulnerability | 6,5 | Medio |
| CVE-2023-3447 | The Active Directory Integration / LDAP Integration plugin for WordPress is vulnerable to LDAP Injection in versions up to, and including, 4.1.5. This is due to insufficient escaping on the supplied username value. This makes it possible for unauthenticated attackers to extract potentially sensitive information from the LDAP directory. | 8,6 | Alto |
| CVE-2023-33254 | There is an LDAP bind credentials exposure on KACE Systems Deployment and Remote Site appliances 9.0.146. The captured credentials may provide a higher privilege level on the Active Directory domain. To exploit this, an authenticated attacker edits the user-authentication settings to specify an attacker-controlled LDAP server, clicks the Test Settings button, and captures the cleartext credentials. | 6,5 | Medio |
| CVE-2023-32235 | Ghost before 5.42.1 allows remote attackers to read arbitrary files within the active theme's folder via /assets/built%2F..%2F..%2F/ directory traversal. This occurs in frontend/web/middleware/static-theme.js. | 7,5 | Alto |
| CVE-2023-29057 | A valid XCC user's local account permissions overrides their active directory permissions under specific configurations. This could lead to a privilege escalation. To be vulnerable, LDAP must be configured for authentication/authorization and logins configured as “Local First, then LDAP”. | 7,3 | Alto |
| CVE-2023-2599 | The Active Directory Integration plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 4.1.4 due to missing nonce verification on the get_users function and insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to cause resource exhaustion via a forged request granted they can trick an administrator into performing an action such as clicking on a link. | 3,1 | Bajo |

| | | | |
|---|---|---|---|
| CVE-2023-2484 | The Active Directory Integration plugin for WordPress is vulnerable to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 4.1.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | 7,2 | Alto |
| CVE-2023-23749 | The 'LDAP Integration with Active Directory and OpenLDAP - NTLM & Kerberos Login' extension is vulnerable to LDAP Injection since is not properly sanitizing the 'username' POST parameter. An attacker can manipulate this paramter to dump arbitrary contents form the LDAP Database. | 7,5 | Alto |
| CVE-2023-21816 | Windows Active Directory Domain Services API Denial of Service Vulnerability | 7,5 | Alto |
| CVE-2023-0812 | The Active Directory Integration / LDAP Integration WordPress plugin before 4.1.1 does not have proper authorization or nonce values for some POST requests, leading to unauthenticated data disclosure. | 7,5 | Alto |
| CVE-2023-0476 | A LDAP injection vulnerability exists in Tenable.sc due to improper validation of user-supplied input before returning it to users. An authenticated attacker could generate data in Active Directory using the application account through blind LDAP injection. | 6,5 | Medio |
| CVE-2022-47966 | Multiple Zoho ManageEngine on-premise products, such as ServiceDesk Plus through 14003, allow remote code execution due to use of Apache Santuario xmlsec (aka XML Security for Java) 1.4.1, because the xmlsec XSLT features, by design in that version, make the application responsible for certain security protections, and the ManageEngine applications did not provide those protections. This affects Access Manager Plus before 4308, Active Directory 360 before 4310, ADAudit Plus before 7081, ADManager Plus before 7162, ADSelfService Plus before 6211, Analytics Plus before 5150, Application Control Plus before 10.1.2220.18, Asset Explorer before 6983, Browser Security Plus before 11.1.2238.6, Device Control Plus before 10.1.2220.18, Endpoint Central before 10.1.2228.11, Endpoint Central MSP before 10.1.2228.11, Endpoint DLP before 10.1.2137.6, Key Manager Plus before 6401, OS Deployer before 1.1.2243.1, PAM 360 before 5713, Password Manager Pro before 12124, Patch Manager Plus before 10.1.2220.18, Remote Access Plus before 10.1.2228.11, Remote Monitoring and Management (RMM) before 10.1.41. ServiceDesk Plus before 14004, ServiceDesk Plus MSP before 13001, SupportCenter Plus before 11026, and Vulnerability Manager Plus before 10.1.2220.18. Exploitation is only possible if SAML SSO has ever been configured for a product (for some products, exploitation requires that SAML SSO is currently active). | 9,8 | Crítico |
| CVE-2022-45141 | Since the Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability was disclosed by Microsoft on Nov 8 2022 and per RFC8429 it is assumed that rc4-hmac is weak, Vulnerable Samba Active Directory DCs will issue rc4-hmac encrypted tickets despite the target server supporting better encryption (eg aes256-cts-hmac-sha1-96) | 9,8 | Crítico |
| CVE-2022-43400 | A vulnerability has been identified in Siveillance Video Mobile Server V2022 R2 (All versions < V22.2a (80)). The mobile server component of affected applications improperly handles the log in for Active Directory accounts that are part of Administrators group. This could allow an unauthenticated remote attacker to access the application without a valid account. | 9,8 | Crítico |
| CVE-2022-38042 | Active Directory Domain Services Elevation of Privilege Vulnerability | 7,1 | Alto |
| CVE-2022-37978 | Windows Active Directory Certificate Services Security Feature Bypass | 7,5 | Alto |
| CVE-2022-37976 | Active Directory Certificate Services Elevation of Privilege Vulnerability | 8,8 | Alto |
| CVE-2022-37397 | An issue was discovered in the YugabyteDB 2.6.1 when using LDAP-based authentication in YCQL with Microsoft’s Active Directory. When anonymous or unauthenticated LDAP binding is enabled, it allows bypass of authentication with an empty password. | 8,3 | Alto |
| CVE-2022-34691 | Active Directory Domain Services Elevation of Privilege Vulnerability | 8,8 | Alto |
| CVE-2022-34379 | Dell EMC CloudLink 7.1.2 and all prior versions contain an Authentication Bypass Vulnerability. A remote attacker, with the knowledge of the active directory usernames, could potentially exploit this vulnerability to gain unauthorized access to the system. | 9,4 | Crítico |
| CVE-2022-30215 | Active Directory Federation Services Elevation of Privilege Vulnerability | 7,5 | Alto |
| CVE-2022-2987 | The Ldap WP Login / Active Directory Integration WordPress plugin before 3.0.2 does not have any authorisation and CSRF checks when updating it's settings (which are hooked to the init action), allowing unauthenticated attackers to update them. Attackers could set their own LDAP server to be used to authenticated users, therefore bypassing the current authentication | 7,5 | Alto |
| CVE-2022-29172 | Auth0 es un agente de autenticación que admite proveedores de identidad social y empresarial, incluidos Active Directory, LDAP, Google Apps y Salesforce. En las versiones anteriores a '11.33.0', cuando el “ campos de registro adicionales” feature [is configured](https://github.com/auth0/lock#additional-sign-up-fields), un actor malintencionado puede inyectar código HTML invalidado en estos campos adicionales, que luego se almacena en la carga útil del servicio 'user_metdata' (utilizando la propiedad 'name'). Los correos electrónicos de verificación, cuando corresponda, se generan utilizando estos metadatos. Por lo tanto, es posible que un actor elabore un enlace malicioso inyectando HTML, que luego se representa como el nombre del destinatario dentro de la plantilla de correo electrónico entregada. Se verá afectado por esta vulnerabilidad si está utilizando 'auth0-lock' versión '11.32.2' o inferior y está utilizando el “ campos de registro adicionales” en su aplicación. Actualice a la versión '11.33.0'. | 6,1 | Medio |
| CVE-2022-26923 | Vulnerabilidad de elevación de privilegios de Active Directory Domain Services | 8,8 | Alto |
| CVE-2022-23551 | aad-pod-identity asigna identidades de Azure Active Directory a las aplicaciones de Kubernetes y ahora ha quedado en desuso a partir del 24 de octubre de 2022. El componente NMI de AAD Pod Identity intercepta y valida las solicitudes de token en función de las expresiones regulares. En este caso, una solicitud de token realizada con barra invertida en la solicitud (ejemplo: '/metadata/identity\oauth2\token/') omitiría la validación de NMI y se enviaría a IMDS, lo que permitiría a un pod del clúster acceder a identidades a las que no debería tener acceso. Este problema se ha corregido y se ha incluido en la versión 1.8.13 de AAD Pod Identity. Si se usa el complemento de identidades administradas por pods de AKS, no se requiere ninguna acción. Los clústeres ahora deberían ejecutar la versión 1.8.13. | 5,3 | Medio |
| CVE-2022-23342 | Las versiones de Hyland Onbase Application Server anteriores a la 20.3.58.1000 y las versiones 21.1.1.1000 a 21.1.15.1000 de OnBase son vulnerables a una vulnerabilidad de enumeración de nombres de usuario. Un atacante puede obtener usuarios válidos en función de la respuesta devuelta para los usuarios válidos y no válidos mediante el envío de una solicitud de inicio de sesión POST al punto de conexión /mobilebroker/ServiceToBroker.svc/Json/Connect. Esto puede dar lugar a la enumeración de usuarios en los sistemas integrados de Active Directory subyacentes. | 5,3 | Medio |
| CVE-2022-23232 | Las versiones de StorageGRID (anteriormente StorageGRID Webscale) anteriores a la 11.6.0 son susceptibles a una vulnerabilidad que, cuando se explota con éxito, podría permitir que las cuentas de usuario externo deshabilitadas, caducadas o bloqueadas accedan a los datos de S3 a los que tenían acceso anteriormente. StorageGRID 11.6.0 obtiene el estado de la cuenta de usuario de Active Directory o Azure y bloqueará el acceso a S3 para las cuentas de usuario deshabilitadas durante la sincronización en segundo plano posterior. Las cuentas de usuario que han caducado o están bloqueadas para Active Directory o Azure, o las cuentas de usuario que están deshabilitadas, caducadas o bloqueadas en orígenes de identidad distintos de Active Directory o Azure deben eliminarse manualmente de las pertenencias a grupos o sus claves S3 se deben eliminar manualmente del Administrador de inquilinos en todas las versiones de StorageGRID (anteriormente StorageGRID Webscale). | 4,9 | Medio |
| CVE-2022-23105 | Jenkins Active Directory Plugin 2.25 y versiones anteriores no cifran la transmisión de datos entre el controlador Jenkins y los servidores de Active Directory en la mayoría de las configuraciones. | 6,5 | Medio |
| CVE-2022-21936 | En la versión 12.0 de Metasys ADX Server que ejecuta MVE, un usuario de Active Directory podría ejecutar acciones validadas sin proporcionar una contraseña válida al utilizar la interfaz de usuario de MVE SMP. | 8,1 | Alto |
| CVE-2022-21857 | Vulnerabilidad de elevación de privilegios de Active Directory Domain Services | 8,8 | Alto |
| CVE-2022-1697 | Las versiones 3.8.0 a 3.11.0 del agente de Active Directory de Okta instalaron el servicio de actualización del agente de Okta AD mediante una ruta sin comillas. Nota: Para remediar esta vulnerabilidad, debe desinstalar Okta Active Directory Agent y volver a instalar Okta Active Directory Agent 3.12.0 o superior según la documentación. | 3,9 | Bajo |
| CVE-2021-43935 | Los productos afectados, cuando se configuran para usar SSO, se ven afectados por una vulnerabilidad de autenticación incorrecta. Esta vulnerabilidad permite que la aplicación acepte la entrada manual de cualquier cuenta de directorio activo (AD) aprovisionada en la aplicación sin proporcionar una contraseña, lo que resulta en el acceso a la aplicación como la cuenta de AD suministrada, con todos los privilegios asociados. | 8,1 | Alto |
| CVE-2021-42291 | Vulnerabilidad de elevación de privilegios de Active Directory Domain Services | 7,5 | Alto |
| CVE-2021-42287 | Vulnerabilidad de elevación de privilegios de Active Directory Domain Services | 7,5 | Alto |
| CVE-2021-42282 | Vulnerabilidad de elevación de privilegios de Active Directory Domain Services | 7,5 | Alto |
| CVE-2021-42278 | Vulnerabilidad de elevación de privilegios de Active Directory Domain Services | 7,5 | Alto |
| CVE-2021-41361 | Vulnerabilidad de suplantación de servidor de federación de Active Directory | 5,4 | Medio |
| CVE-2021-41337 | Vulnerabilidad de omisión de funciones de seguridad de Active Directory | 4,9 | Medio |
| CVE-2021-3956 | Se informó de una vulnerabilidad de omisión de autenticación de solo lectura en la versión del tercer trimestre de 2021 del firmware de Lenovo XClarity Controller (XCC) que afectaba a los dispositivos XCC configurados en modo de solo autenticación LDAP y que utilizaban un servidor LDAP compatible con “ enlace no autenticado”, como Microsoft Active Directory. Un usuario no autenticado puede obtener acceso de solo lectura a XCC en dicha configuración, lo que permite que la configuración del dispositivo XCC se vea pero no se cambie. Dispositivos XCC configurados para usar autenticación local, autenticación LDAP + modo de autorización o servidores LDAP que solo admiten “ enlace autenticado” y/o “ enlace anónimo” no se ven afectados. | 4,3 | Medio |
| CVE-2021-37705 | OneFuzz es una plataforma Fuzzing-As-A-Service autoalojada de código abierto. A partir de OneFuzz 2.12.0 o superior, una comprobación de autorización incompleta permite a un usuario autenticado de cualquier inquilino de Azure Active Directory realizar llamadas API autorizadas a una instancia de OneFuzz vulnerable. Para ser vulnerable, una implementación de OneFuzz debe ser de la versión 2.12.0 o superior y debe implementarse con la opción --multi_tenant_domain no predeterminada. Esto puede dar lugar a un acceso de lectura/escritura a datos privados, como información sobre vulnerabilidades y fallos de software, herramientas de pruebas de seguridad y código y símbolos propietarios. A través de llamadas API autorizadas, esto también permite la manipulación de los datos existentes y la ejecución de código no autorizado en los recursos de proceso de Azure. Este problema se resuelve a partir de la versión 2.31.0, mediante la adición de la verificación a nivel de aplicación del "emisor" del token al portador contra una lista de permitidos configurada por el administrador. Como solución alternativa, los usuarios pueden restringir el acceso al inquilino de una instancia de OneFuzz implementada < 2.31.0 volviendo a implementarla en la configuración predeterminada, que omite la opción '--multi_tenant_domain'. | 10 | Crítico |
| CVE-2021-37153 | ForgeRock Access Management (AM) anterior a la versión 7.0.2, cuando se configura con Active Directory como almacén de identidades, tiene un problema de omisión de autenticación. | 9,8 | Crítico |
| CVE-2021-36949 | Vulnerabilidad de omisión de autenticación de Microsoft Azure Active Directory Connect | 7,1 | Crítico |
| CVE-2021-30651 | Un usuario administrador de SMG autenticado malintencionado puede obtener contraseñas para servidores LDAP/Active Directory externos a los que, de otro modo, no estaría autorizado a acceder. | 4,9 | Medio |
| CVE-2021-29643 | PRTG Network Monitor anterior a 21.3.69.1333 permite almacenar XSS a través de una cadena no desinfectada importada de un objeto de usuario en una instancia de Active Directory conectada. | 5,4 | Medio |
| CVE-2021-28197 | La función de configuración de Active Directory en ASUS BMC’ La página de administración web del firmware no verifica la longitud de la cadena introducida por los usuarios, lo que da lugar a una vulnerabilidad de desbordamiento de búfer. Al obtener el permiso con privilegios, los atacantes remotos utilizan la fuga para terminar de forma anormal el servicio web. | 4,9 | Medio |
| CVE-2021-28184 | La función de configuración de Active Directory en ASUS BMC’ La página de administración web del firmware no verifica la longitud de la cadena introducida por los usuarios, lo que da lugar a una vulnerabilidad de desbordamiento de búfer. Al obtener el permiso con privilegios, los atacantes remotos utilizan la fuga para terminar de forma anormal el servicio web. | 4,9 | Medio |
| CVE-2021-27330 | Triconsole Datepicker Calendar <3.77 se ve afectado por el scripting entre sitios (XSS) en calendar_form.php. Los atacantes pueden leer las cookies de autenticación que aún están activas, que se pueden usar para realizar ataques adicionales, como leer el historial del navegador, los listados de directorios y el contenido de los archivos. | 6,1 | Medio |

| | | | |
|---|---|---|---|
| CVE-2021-26999 | Las versiones de Cloud Manager de NetApp anteriores a la 3.9.9 registran información confidencial cuando falla una conexión de Active Directory. La información registrada solo está disponible para los usuarios autenticados. Los clientes con la actualización automática habilitada ya deben estar en una versión fija, mientras que se recomienda a los clientes que usan conectores locales con la actualización automática deshabilitada que actualicen a una versión fija. | 4,3 | Medio |
| CVE-2021-25216 | En BIND 9.5.0 -> 9.11.29, 9.12.0 -> 9.16.13 y las versiones BIND 9.11.3-S1 -> 9.11.29-S1 y 9.16.8-S1 -> 9.16.13-S1 de BIND Supported Preview Edition, así como en las versiones de lanzamiento 9.17.0 -> 9.17.1 de la rama de desarrollo BIND 9.17, los servidores BIND son vulnerables si están ejecutando una versión afectada y están configurados para utilizar las características de GSS-TSIG. En una configuración que utiliza la configuración predeterminada de BIND, la ruta de código vulnerable no se expone, pero un servidor se puede hacer vulnerable estableciendo explícitamente valores para las opciones de configuración tkey-gssapi-keytab o tkey-gssapi-credential. Aunque la configuración predeterminada no es vulnerable, GSS-TSIG se utiliza con frecuencia en redes donde BIND está integrado con Samba, así como en entornos de servidores mixtos que combinan servidores BIND con controladores de dominio de Active Directory. Para los servidores que cumplen con estas condiciones, la implementación de ISC SPNEGO es vulnerable a varios ataques, dependiendo de la arquitectura de CPU para la que se construyó BIND: Para binarios con nombre compilados para plataformas de 64 bits, esta falla se puede usar para desencadenar una lectura excesiva del búfer, lo que lleva a un bloqueo del servidor. En el caso de los binarios con nombre compilados para plataformas de 32 bits, esta falla se puede utilizar para desencadenar un bloqueo del servidor debido a un desbordamiento de búfer y posiblemente también para lograr la ejecución remota de código. Hemos determinado que las implementaciones estándar de SPNEGO están disponibles en las bibliotecas MIT y Heimdal Kerberos, que admiten una amplia gama de sistemas operativos, lo que hace que la implementación de ISC sea innecesaria y obsoleta. Por lo tanto, para reducir la superficie de ataque para los usuarios de BIND, eliminaremos la implementación de ISC SPNEGO en las versiones de abril de BIND 9.11 y 9.16 (ya se había eliminado de BIND 9.17). Normalmente no eliminaríamos algo de una ESV (versión de soporte extendido) estable de BIND, pero dado que las bibliotecas del sistema pueden reemplazar la implementación de ISC SPNEGO, hemos hecho una excepción en este caso por razones de estabilidad y seguridad. | 8,1 | Alto |
| CVE-2021-23008 | En la versión 15.1.x anterior a la 15.1.3, 14.1.x anterior a la 14.1.4, 13.1.x anterior a la 13.1.4, 12.1.x anterior a la 12.1.6 y todas las versiones 16.0.x y 11.6.x., la autenticación BIG-IP APM AD (Active Directory) se puede omitir a través de una respuesta AS-REP (Kerberos Authentication Service Response) falsificada enviada a través de una conexión KDC (Kerberos Key Distribution Center) secuestrada o desde un servidor AD comprometido por un atacante. Nota: Las versiones de software que han alcanzado el fin del soporte técnico (EoTS) no se evalúan. | 9,8 | Crítico |
| CVE-2021-1677 | Vulnerabilidad de suplantación de identidad de pod de Azure Active Directory | 5,5 | Medio |
| CVE-2020-9470 | Se descubrió un problema en Wing FTP Server 6.2.5 antes de febrero de 2020. Debido a los permisos inseguros al manejar las cookies de sesión, un usuario local puede ver el contenido de la sesión y los directorios de session_admin, que exponen las cookies de sesión activas dentro de la interfaz HTTP y el panel de administración de Wing FTP. Estas cookies se pueden utilizar para secuestrar sesiones de usuario y administrativas, incluida la capacidad de ejecutar comandos Lua como root dentro del panel de administración. | 7,8 | Alto |
| CVE-2020-9330 | Algunas impresoras Xerox WorkCentre anteriores a 073.xxx.000.02300 no requieren que el usuario vuelva a introducir o validar las credenciales de enlace LDAP al cambiar la dirección IP del conector LDAP. Un actor malintencionado que obtiene acceso a los dispositivos afectados (por ejemplo, mediante el uso de credenciales predeterminadas) puede cambiar la dirección IP de la conexión LDAP a un sistema propiedad del actor sin conocer las credenciales de enlace LDAP. Después de cambiar la dirección IP de la conexión LDAP, los intentos de autenticación posteriores harán que la impresora envíe credenciales LDAP (Active Directory) de texto sin formato al actor. Aunque las credenciales pueden pertenecer a un usuario sin privilegios, las organizaciones suelen usar cuentas de servicio con privilegios para enlazar a Active Directory. El atacante obtiene un punto de apoyo en el dominio de Active Directory como mínimo, y puede usar las credenciales para tomar el control del dominio de Active Directory. Esto afecta a los dispositivos 3655*, 3655i*, 58XX*, 58XXi*, 59XX*, 59XXi*, 6655**, 6655i**, 72XX*, 72XXi*, 78XX**, 78XXi**, 7970**, 7970i**, EC7836** y EC7856**. | 8,8 | Alto |
| CVE-2020-8625 | Los servidores BIND son vulnerables si ejecutan una versión afectada y están configurados para utilizar las funciones de GSS-TSIG. En una configuración que utiliza la configuración predeterminada de BIND, la ruta de acceso del código vulnerable no se expone, pero un servidor se puede hacer vulnerable estableciendo explícitamente valores válidos para las opciones de configuración tkey-gssapi-keytab o tkey-gssapi-credential. Aunque la configuración predeterminada no es vulnerable, GSS-TSIG se utiliza con frecuencia en redes donde BIND está integrado con Samba, así como en entornos de servidores mixtos que combinan servidores BIND con controladores de dominio de Active Directory. El resultado más probable de una explotación exitosa de la vulnerabilidad es un bloqueo del proceso nombrado. Sin embargo, la ejecución remota de código, aunque no está probada, es teóricamente posible. Afecta a: BIND 9.5.0 -> 9.11.27, 9.12.0 -> 9.16.11 y versiones BIND 9.11.3-S1 -> 9.11.27-S1 y 9.16.8-S1 -> 9.16.11-S1 de BIND Supported Preview Edition. También se publican las versiones 9.17.0 -> 9.17.1 de la rama de desarrollo BIND 9.17 | 8,1 | Alto |
| CVE-2020-8200 | Improper authentication in Citrix StoreFront Server < 1912.0.1000 allows an attacker who is authenticated on the same Microsoft Active Directory domain as a Citrix StoreFront server to read arbitrary files from that server. | 6,5 | Medio |
| CVE-2020-36167 | Se detectó un problema en el servidor de Veritas Backup Exec a través de la versión 16.2, la 20.6 antes de la revisión 298543 y la 21.1 antes de la 657517 de revisión. Al inicio, carga la biblioteca OpenSSL desde la carpeta de instalación. Esta biblioteca, a su vez, intenta cargar el archivo de configuración /usr/local/ssl/openssl.cnf, que puede no existir. En sistemas Windows, esta ruta podría traducirse a <drive>:\usr\local\ssl\openssl.cnf. Un usuario con pocos privilegios puede crear un archivo de configuración :\usr\local\ssl\openssl.cnf para cargar un motor OpenSSL malintencionado, lo que resulta en la ejecución de código arbitrario como SYSTEM cuando se inicia el servicio. Esto le da al atacante acceso de administrador en el sistema, lo que le permite (de forma predeterminada) acceder a todos los datos, acceder a todas las aplicaciones instaladas, etc. Si el sistema también es un controlador de dominio de Active Directory, esto puede afectar a todo el dominio. | 9,3 | Crítico |
| CVE-2020-36160 | Se descubrió un problema en Veritas System Recovery antes de la versión 21.2. Al inicio, carga la biblioteca OpenSSL desde \usr\local\ssl. Esta biblioteca intenta cargar el archivo de configuración from \usr\local\ssl\openssl.cnf, que no existe. De forma predeterminada, en los sistemas Windows, los usuarios pueden crear directorios en C:\. Un usuario con pocos privilegios puede crear un archivo de configuración C:\usr\local\ssl\openssl.cnf para cargar un motor OpenSSL malintencionado, lo que da lugar a la ejecución de código arbitrario como SYSTEM cuando se inicia el servicio. Esto le da al atacante acceso de administrador en el sistema, lo que le permite (de forma predeterminada) acceder a todos los datos y aplicaciones instaladas, etc. Si el sistema también es un controlador de dominio de Active Directory, esto puede afectar a todo el dominio. | 9,3 | Crítico |
| CVE-2020-27122 | A vulnerability in the Microsoft Active Directory integration of Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to elevate privileges on an affected device. To exploit this vulnerability, an attacker would need to have a valid administrator account on an affected device. The vulnerability is due to incorrect privilege assignment. An attacker could exploit this vulnerability by logging in to the system with a crafted Active Directory account. A successful exploit could allow the attacker to obtain root privileges on an affected device. | 4,4 | Medio |
| CVE-2020-26542 | An issue was discovered in the MongoDB Simple LDAP plugin through 2020-10-02 for Percona Server when using the SimpleLDAP authentication in conjunction with Microsoft’s Active Directory, Percona has discovered a flaw that would allow authentication to complete when passing a blank value for the account password, leading to access against the service integrated with which Active Directory is deployed at the level granted to the authenticating account. | 9,8 | Crítico |
| CVE-2020-25719 | A flaw was found in the way Samba, as an Active Directory Domain Controller, implemented Kerberos name-based authentication. The Samba AD DC, could become confused about the user a ticket represents if it did not strictly require a Kerberos PAC and always use the SIDs found within. The result could include total domain compromise. | 7,2 | Alto |
| CVE-2020-25718 | A flaw was found in the way samba, as an Active Directory Domain Controller, is able to support an RODC (read-only domain controller). This would allow an RODC to print administrator tickets. | 8,8 | Alto |
| CVE-2020-2303 | A cross-site request forgery (CSRF) vulnerability in Jenkins Active Directory Plugin 2.19 and earlier allows attackers to perform connection tests, connecting to attacker-specified or previously configured Active Directory servers using attacker-specified credentials. | 5,4 | Medio |
| CVE-2020-2302 | A missing permission check in Jenkins Active Directory Plugin 2.19 and earlier allows attackers with Overall/Read permission to access the domain health check diagnostic page. | 4,3 | Medio |
| CVE-2020-2301 | Jenkins Active Directory Plugin 2.19 and earlier allows attackers to log in as any user with any password while a successful authentication of that user is still in the optional cache when using Windows/ADSI mode. | 9,8 | Crítico |
| CVE-2020-2300 | Jenkins Active Directory Plugin 2.19 and earlier does not prohibit the use of an empty password in Windows/ADSI mode, which allows attackers to log in to Jenkins as any user depending on the configuration of the Active Directory server. | 9,8 | Crítico |
| CVE-2020-2299 | Jenkins Active Directory Plugin 2.19 and earlier allows attackers to log in as any user if a magic constant is used as the password. | 9,8 | Crítico |
| CVE-2020-12271 | Se encontró un problema de inyección SQL en SFOS 17.0, 17.1, 17.5 y 18.0 antes del 25/04/2020 en dispositivos Sophos XG Firewall, tal y como se explotó en abril de 2020. Esto afectaba a los dispositivos configurados con el servicio de administración (HTTPS) o el portal de usuario expuesto en la zona WAN. Un ataque exitoso puede haber provocado la ejecución remota de código que exfiltró nombres de usuario y contraseñas con hash para los administradores del dispositivo local, los administradores del portal y las cuentas de usuario utilizadas para el acceso remoto (pero no las contraseñas externas de Active Directory o LDAP) | 10 | Crítico |
| CVE-2020-10704 | Se encontró una falla al usar samba como controlador de dominio de Active Directory. Debido a la forma en que samba maneja ciertas solicitudes como un servidor LDAP de controlador de dominio de directorio activo, un usuario no autorizado puede causar un desbordamiento de la pila que conduzca a una denegación de servicio. La mayor amenaza de esta vulnerabilidad es la disponibilidad del sistema. Este problema afecta a todas las versiones de samba anteriores a la 4.10.15, antes de la 4.11.8 y antes de la 4.12.2. | 7,5 | Alto |
| CVE-2020-10678 | En Octopus Deploy antes de 2020.1.5, para los clientes que ejecutan Active Directory local vinculado a su servidor Octopus, un usuario autenticado puede aprovechar un error para escalar privilegios. | 8,8 | Alto |
| CVE-2020-1055 | Existe una vulnerabilidad de secuencias de comandos entre sitios (XSS) cuando los Servicios de federación de Active Directory (ADFS) no desinfectan correctamente las entradas del usuario, también conocida como "Vulnerabilidad de secuencias de comandos entre sitios de servicios de federación de Microsoft Active Directory". | 6,1 | Medio |
| CVE-2020-0856 | Existe una vulnerabilidad de divulgación de información cuando el DNS integrado de Active Directory (ADIDNS) maneja incorrectamente los objetos en la memoria. Un atacante autenticado que aprovechara con éxito esta vulnerabilidad sería capaz de leer información confidencial sobre el sistema objetivo. Para aprovechar esta condición, un atacante autenticado tendría que enviar una solicitud especialmente diseñada al AD|Servicio DNS. Tenga en cuenta que la vulnerabilidad de divulgación de información por sí sola no sería suficiente para que un atacante comprometiera un sistema. Sin embargo, un atacante podría combinar esta vulnerabilidad con vulnerabilidades adicionales para explotar aún más el sistema. La actualización corrige la vulnerabilidad corrigiendo la forma en que el DNS integrado de Active Directory (ADIDNS) maneja los objetos en la memoria. | 6,5 | Medio |
| CVE-2020-0837 | Existe una vulnerabilidad de elevación de privilegios cuando los Servicios de federación de Active Directory (ADFS) controlan incorrectamente las solicitudes de autenticación multifactor. Un atacante que aprovechara con éxito esta vulnerabilidad podría eludir algunos, pero no todos, los factores de autenticación. Para aprovechar esta vulnerabilidad, un atacante podría enviar una solicitud de autenticación especialmente diseñada. Esta actualización de seguridad corrige la forma en que ADFS controla las solicitudes de autenticación multifactor. | 5 | Medio |
| CVE-2020-0761 | Existe una vulnerabilidad de ejecución remota de código cuando el DNS integrado de Active Directory (ADIDNS) maneja incorrectamente los objetos en la memoria. Un atacante autenticado que aprovechara con éxito la vulnerabilidad podría ejecutar código arbitrario en el contexto de la cuenta del sistema local Para aprovechar la vulnerabilidad, un atacante autenticado podría enviar solicitudes maliciosas a un servidor DNS integrado de Active Directory (ADIDNS). La actualización corrige la vulnerabilidad corrigiendo la forma en que el DNS integrado de Active Directory (ADIDS) maneja los objetos en la memoria. | 8,8 | Alto |
| CVE-2020-0718 | Existe una vulnerabilidad de ejecución remota de código cuando el DNS integrado de Active Directory (ADIDNS) maneja incorrectamente los objetos en la memoria. Un atacante autenticado que aprovechara con éxito la vulnerabilidad podría ejecutar código arbitrario en el contexto de la cuenta del sistema local Para aprovechar la vulnerabilidad, un atacante autenticado podría enviar solicitudes maliciosas a un servidor DNS integrado de Active Directory (ADIDNS). La actualización corrige la vulnerabilidad corrigiendo la forma en que el DNS integrado de Active Directory (ADIDS) maneja los objetos en la memoria. | 8,8 | Alto |

| | | | |
|---|---|---|---|
| CVE-2020-0665 | Existe una vulnerabilidad de elevación de privilegios en las confianzas del bosque de Active Directory debido a una configuración predeterminada que permite a un atacante en el bosque de confianza solicitar la delegación de un TGT para una identidad del bosque de confianza, también conocida como "Vulnerabilidad de elevación de privilegios de Active Directory". | 8,1 | Alto |
| CVE-2020-0664 | Existe una vulnerabilidad de divulgación de información cuando el DNS integrado de Active Directory (ADIDNS) maneja incorrectamente los objetos en la memoria. Un atacante autenticado que aprovechara con éxito esta vulnerabilidad sería capaz de leer información confidencial sobre el sistema objetivo. Para aprovechar esta condición, un atacante autenticado tendría que enviar una solicitud especialmente diseñada al AD|Servicio DNS. Tenga en cuenta que la vulnerabilidad de divulgación de información por sí sola no sería suficiente para que un atacante comprometiera un sistema. Sin embargo, un atacante podría combinar esta vulnerabilidad con vulnerabilidades adicionales para explotar aún más el sistema. La actualización corrige la vulnerabilidad corrigiendo la forma en que el DNS integrado de Active Directory (ADIDNS) maneja los objetos en la memoria. | 6,5 | Medio |

**ANEXO 2 NORMA ISO/IEC 27001:2022**

# INTERNACIONAL ESTÁNDAR

# ISO/CEI 27001

Tercera edicion
2022-10

## Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos

*Seguridad de la información, ciberseguridad y protección de la vida privada — Sistemas de gestión de la seguridad de la información — Exigencias*

Número de referencia
ISO/CEI 27001:2022(E)



oficina de derechos de autor ISO
CP 401 • Cap. de Blandonnet 8
CH-1214 Vernier, Ginebra
Teléfono: +41 22 749 01 11 Correo electrónico: copyright@iso.org
Sitio web:www.iso.org

Publicado en Suiza

yo

# Contenido

# Prefacio

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con ISO e IEC, también participan en el trabajo.

Los procedimientos utilizados para desarrollar este documento y los destinados a su posterior mantenimiento se describen en las Directivas ISO/IEC, Parte 1. En particular, se deben tener en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos. Este documento fue redactado de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (verwww.iso.org/directivas o www.iec.ch/members_experts/refdocs).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no serán responsables de identificar ninguno o todos los derechos de patente. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento estarán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (verwww.iso.org/patents ) o la lista IEC de declaraciones de patentes recibidas (verhttps://patents.iec.ch ).

Cualquier nombre comercial utilizado en este documento es información proporcionada para la comodidad de los usuarios y no constituye un respaldo.

Para obtener una explicación de la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los obstáculos técnicos al comercio (TBT), consulte www.iso.org/iso/prefacio.html . En la CEI, véasewww.iec.ch/understanding-standards .

Este documento fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnologías de la información*, Subcomité SC 27, *Seguridad de la información, ciberseguridad y protección de la privacidad*.

Esta tercera edición cancela y reemplaza la segunda edición (ISO/IEC 27001:2013), que ha sido revisada técnicamente. También incorpora los Corrigenda Técnicos ISO/IEC 27001:2013/Cor 1:2014 e ISO/IEC 27001:2013/Cor 2:2015.

Los principales cambios son los siguientes:

— el texto se ha alineado con la estructura armonizada de normas de sistemas de gestión e ISO/IEC 27002:2022.

Cualquier comentario o pregunta sobre este documento debe dirigirse al organismo nacional de normalización del usuario. Una lista completa de estos organismos se puede encontrar enwww.iso.org/members.html y www.iec.ch/comités-nacionales .

# Introducción

## 0.1 generales

Este documento ha sido preparado para proporcionar requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de seguridad de la información de una organización está influenciado por las necesidades y objetivos de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información forme parte de los procesos y la estructura de gestión general de la organización y se integre con ellos, y que la seguridad de la información se tenga en cuenta en el diseño de los procesos, los sistemas de información y los controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se escale de acuerdo con las necesidades de la organización.

Este documento puede ser utilizado por partes internas y externas para evaluar la capacidad de la organización para cumplir con los requisitos de seguridad de la información de la propia organización.

El orden en que se presentan los requisitos en este documento no refleja su importancia ni implica el orden en que deben implementarse. Los elementos de la lista se enumeran solo con fines de referencia.

ISO/IEC 27000 describe la descripción general y el vocabulario de los sistemas de gestión de seguridad de la información, haciendo referencia a la familia de estándares del sistema de gestión de seguridad de la información (incluido ISO/IEC 27003[2], ISO/CEI 27004[3]e ISO/IEC 27005[4]), con términos y definiciones relacionados.

## 0.2 Compatibilidad con otros estándares de sistemas de gestión

Este documento aplica la estructura de alto nivel, los títulos de subcláusulas idénticos, el texto idéntico, los términos comunes y las definiciones básicas definidas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO consolidado y, por lo tanto, mantiene la compatibilidad con otros estándares de sistemas de gestión. que han adoptado el Anexo SL.

Este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que elijan operar un gestión.

# Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos

## 1 Alcance

Este documento especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Este documento también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en este documento son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Excluyendo cualquiera de los requisitos especificados enCláusulas 4 a10 no es aceptable cuando una organización reclama conformidad con este documento.

## 2 Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que parte o la totalidad de su contenido constituye requisitos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las

ISO/CEI 27000, *Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario*

## 3 Términos y definiciones

A los efectos de este documento, se aplican los términos y definiciones proporcionados en ISO/IEC 27000.

ISO e IEC mantienen bases de datos de terminología para su uso en la normalización en las siguientes direcciones:

— Plataforma de navegación ISO Online: disponible enhttps://www.iso.org/obp

— Electropedia IEC: disponible enhttps://www.electropedia.org/

## 4 Contexto de la organización

### 4.1 Entender la organización y su contexto

La organización debe determinar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados esperados de su sistema de gestión de seguridad de la información.

NOTA Determinar estos temas se refiere a establecer el contexto externo e interno de la organización. considerado en la Cláusula 5.4.1 de la Norma ISO 31000:2018[5].

### 4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización determinará:

a) partes interesadas que son relevantes para el sistema de gestión de seguridad de la información;

b) los requisitos pertinentes de estas partes interesadas;

c) cuál de estos requisitos se abordará a través del sistema de gestión de seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir requisitos legales y reglamentarios y requisitos contractuales. obligaciones

### 4.3 Determinación del alcance del sistema de gestión de seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Al determinar este alcance, la organización debe considerar:

a) las cuestiones externas e internas a que se refiere el4.1 ;

b) los requisitos a que se refiere el4.2 ;

c) interfaces y dependencias entre las actividades realizadas por la organización y aquellas que son realizadas por otras organizaciones.

El alcance debe estar disponible como información documentada.

### 4.4 Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

## 5 Liderazgo

### 5.1 Liderazgo y compromiso

La alta dirección deberá demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información mediante:

a) garantizar que la política de seguridad de la información y los objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de la organización;

b) garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;

c) asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;

d) comunicar la importancia de una gestión eficaz de la seguridad de la información y de cumplir con los requisitos del sistema de gestión de la seguridad de la información;

e) garantizar que el sistema de gestión de la seguridad de la información logre los resultados previstos;

f) dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información;

g) promover la mejora continua; y

h) apoyar a otros roles gerenciales relevantes para demostrar su liderazgo en lo que se refiere a sus áreas de responsabilidad.

NOTA La referencia a “negocios” en este documento puede interpretarse en sentido amplio para referirse a aquellas actividades que son esencial para los propósitos de la existencia de la organización.

## 5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

a) es apropiado para el propósito de la organización;

b) incluye objetivos de seguridad de la información (ver6.2 ) o proporciona el marco para establecer objetivos de seguridad de la información;

c) incluye un compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información;

d) incluye un compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información deberá:

e) estar disponible como información documentada;

f) ser comunicado dentro de la organización;

g) estar a disposición de los interesados, según corresponda.

### 5.3 Funciones, responsabilidades y autoridades de la organización

La alta dirección debe asegurarse de que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información se asignen y comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) garantizar que el sistema de gestión de la seguridad de la información se ajuste a los requisitos de este documento;

b) informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño de la sistema de gestión de la seguridad de la información dentro de la organización.

## 6 Planificación

## 6.1 Acciones para abordar riesgos y oportunidades

#### 6.1.1 Generalidades

Al planificar el sistema de gestión de la seguridad de la información, la organización debe tener en cuenta las cuestiones a las que se hace referencia en4.1 y los requisitos a que se refiere el4.2 y determinar los riesgos y oportunidades que deben abordarse para:

a) garantizar que el sistema de gestión de la seguridad de la información pueda lograr los resultados previstos;

b) prevenir o reducir los efectos no deseados;

c) lograr la mejora continua.

La organización debe planificar:

d) acciones para abordar estos riesgos y oportunidades; y

e) cómo

1) integrar e implementar las acciones en sus procesos del sistema de gestión de seguridad de la información; y

2) evaluar la efectividad de estas acciones.

#### 6.1.2 Evaluación de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

a) establece y mantiene criterios de riesgo de seguridad de la información que incluyen:

1) los criterios de aceptación del riesgo; y

2) criterios para realizar evaluaciones de riesgos de seguridad de la información;

b) asegura que las evaluaciones de riesgos de seguridad de la información repetidas produzcan resultados consistentes, válidos y comparables;

c) identifica los riesgos de seguridad de la información:

1) aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información; y

2) identificar a los propietarios del riesgo;

d) analiza los riesgos de seguridad de la información:

1) evaluar las consecuencias potenciales que resultarían si los riesgos identificados en6.1.2 c) 1) fueran a materializarse;

2) evaluar la probabilidad realista de ocurrencia de los riesgos identificados en6.1.2 c) 1); y

3) determinar los niveles de riesgo;

e) evalúa los riesgos de seguridad de la información:

1) comparar los resultados del análisis de riesgo con los criterios de riesgo establecidos en6.1.2 a); y

2) priorizar los riesgos analizados para el tratamiento de riesgos.

La organización debe conservar información documentada sobre el proceso de evaluación de riesgos de seguridad de la información.

#### 6.1.3 Tratamiento de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información, teniendo en cuenta los resultados de la evaluación de riesgos;

b) determinar todos los controles que son necesarios para implementar la(s) opción(es) de tratamiento de riesgos de seguridad de la información elegida(s);

NOTA 1 Las organizaciones pueden diseñar controles según sea necesario o identificarlos de cualquier fuente.

c) comparar los controles determinados en6.1.3 b) arriba con los deAnexo A y verificar que no se hayan omitido los controles necesarios;

NOTA 2 Anexo A contiene una lista de posibles controles de seguridad de la información. Los usuarios de este documento son dirigido aAnexo A para garantizar que no se pasen por alto los controles necesarios de seguridad de la información.

NOTA 3 Los controles de seguridad de la información enumerados enAnexo A no son información exhaustiva y adicional se pueden incluir controles de seguridad si es necesario.

d) producir una Declaración de Aplicabilidad que contenga:

— los controles necesarios (ver6.1.3 b) y c));

— justificación de su inclusión;

— si se aplican o no los controles necesarios; y

— la justificación para excluir cualquiera de losAnexo A control S.

e) formular un plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación de los propietarios de riesgos del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información.

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

NOTA 4 El proceso de evaluación y tratamiento de riesgos de seguridad de la información en este documento se alinea con el principios y directrices genéricas proporcionados en ISO 31000[5].

### 6.2 Objetivos de seguridad de la información y planificación para alcanzarlos

La organización debe establecer objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deberán:

a) ser coherente con la política de seguridad de la información;

b) ser medible (si es factible);

c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y el tratamiento del riesgo;

d) ser monitoreado;

e) ser comunicado;

f) actualizarse según corresponda;

g) estar disponible como información documentada.

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

h) lo que se hará;

i) qué recursos se requerirán;

j) quién será responsable;

k) cuándo se completará; y

l) cómo se evaluarán los resultados.

### 6.3 Planificación de cambios

Cuando la organización determina la necesidad de cambios en el sistema de gestión de la seguridad de la información, los cambios deben llevarse a cabo de manera planificada.

# 7 Soporte

## 7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

## 7.2 Competencia

La organización deberá:

a) determinar la competencia necesaria de la(s) persona(s) que realiza(n) el trabajo bajo su control que afecta su desempeño en seguridad de la información;

b) garantizar que estas personas sean competentes sobre la base de una educación, formación o experiencia adecuadas;

c) en su caso, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas; y

d) conservar la información documentada apropiada como evidencia de competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la provisión de capacitación, tutoría o re-asignación de empleados actuales; o la contratación o contratación de personas competentes.

## 7.3 Conciencia

Las personas que realicen trabajos bajo el control de la organización deberán ser conscientes de:

a) la política de seguridad de la información;

b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de un mejor desempeño de la seguridad de la información; y

c) las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información.

## 7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas relevantes para el sistema de gestión de la seguridad de la información, incluyendo:

a) sobre qué comunicar;

b) cuándo comunicar;

c) con quién comunicarse;

d) cómo comunicarse.

## 7.5 Información documentada

### 7.5.1 Generalidades

El sistema de gestión de la seguridad de la información de la organización debe incluir:

a) información documentada requerida por este documento; y

b) información documentada determinada por la organización como necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA El alcance de la información documentada para un sistema de gestión de seguridad de la información puede diferir de una organización a otra debido a:

1) el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;

2) la complejidad de los procesos y sus interacciones; y

3) la competencia de las personas.

### 7.5.2 Creación y actualización

Al crear y actualizar la información documentada, la organización debe garantizar lo siguiente:

a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);

b) formato (p. ej., idioma, versión de software, gráficos) y soporte (p. ej., papel, electrónico); y

c) revisión y aprobación de la idoneidad y adecuación.

### 7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de seguridad de la información y por este documento se controlará para garantizar:

a) está disponible y es adecuado para su uso, donde y cuando se necesite; y

b) está adecuadamente protegido (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y conservación, incluida la conservación de la legibilidad;

e) control de cambios (por ejemplo, control de versiones); y

f) retención y disposición.

La información documentada de origen externo, determinada por la organización como necesaria para la corresponda y controlarse.

NOTA El acceso puede implicar una decisión con respecto al permiso para ver únicamente la información documentada, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

## 8 Operación

### 8.1 Planificación y control operativo

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en la Cláusula 6, mediante:

— establecer criterios para los procesos;

— implementar el control de los procesos de acuerdo con los criterios.

La información documentada deberá estar disponible en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planeado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados, tomando medidas para mitigar cualquier efecto adverso, según sea necesario.

La organización debe garantizar que los procesos, productos o servicios proporcionados externamente que sean relevantes para el sistema de gestión de la seguridad de la información estén controlados.

### 8.2 Evaluación de riesgos de seguridad de la información

La organización debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan o ocurran cambios significativos, teniendo en cuenta los criterios establecidos en6.1.2 a).

La organización debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

### 8.3 Tratamiento de riesgos de seguridad de la información

La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.

La organización debe conservar información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

## 9 Evaluación del desempeño

## 9.1 Seguimiento, medición, análisis y evaluación

La organización determinará:

a) lo que debe monitorearse y medirse, incluidos los procesos y controles de seguridad de la información;

b) los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para garantizar la validez de los resultados. Los métodos seleccionados deben producir resultados comparables y reproducibles para que se consideren válidos;

c) cuándo se realizará el seguimiento y la medición;

d) quién deberá monitorear y medir;

e) cuándo se analizarán y evaluarán los resultados del seguimiento y la medición;

f) quién analizará y evaluará estos resultados.

La información documentada deberá estar disponible como evidencia de los resultados.

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

### 9.2 Auditoría interna

#### 9.2.1 Generalidades

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información:

a) se ajusta a
   1) los requisitos propios de la organización para su sistema de gestión de seguridad de la información;

2) los requisitos de este documento;

b) se implementa y mantiene de manera efectiva.

### 9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluida la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Al establecer los programas de auditoría interna, la organización debe considerar la importancia de los procesos en cuestión y los resultados de auditorías anteriores.

La organización deberá:

a) definir los criterios de auditoría y el alcance de cada auditoría;

b) seleccionar auditores y realizar auditorías que garanticen la objetividad y la imparcialidad del proceso de auditoría;

c) asegurarse de que los resultados de las auditorías se informen a la dirección pertinente;

La información documentada deberá estar disponible como evidencia de la implementación del programa(s) de auditoría y los resultados de la auditoría.

## 9.3 Revisión por la dirección

### 9.3.1 Generalidades

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados para garantizar su idoneidad, adecuación y eficacia continuas.

### 9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección incluirá la consideración de:

a) el estado de las acciones de revisiones de gestión anteriores;

b) cambios en cuestiones externas e internas que son relevantes para el sistema de gestión de seguridad de la información;

c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de seguridad de la información;

d) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias en:

1) no conformidades y acciones correctivas;

2) resultados de monitoreo y medición;

3) resultados de la auditoría;

4) cumplimiento de los objetivos de seguridad de la información;

e) retroalimentación de las partes interesadas;

f) resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos;

g) oportunidades de mejora continua.

### 9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección incluirán decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de la seguridad de la información.

La información documentada deberá estar disponible como evidencia de los resultados de las revisiones por la dirección.

# 10 Mejora

## 10.1 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

## 10.2 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar a la no conformidad y, según corresponda:

1) tomar acciones para controlarlo y corregirlo;

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acción para eliminar las causas de la no conformidad, a fin de que no se repita u ocurra en otro lugar, mediante:

1) revisar la no conformidad;

2) determinar las causas de la no conformidad; y

3) determinar si existen no conformidades similares o si podrían ocurrir potencialmente;

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva tomada; y

e) realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La información documentada deberá estar disponible como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción posterior tomada,

g) los resultados de cualquier acción correctiva.

# Anexo A
(normativo)

## Referencia de controles de seguridad de la información

Los controles de seguridad de la información enumerados enTabla A.1 se derivan directamente y están alineados con los enumerados en ISO/IEC 27002:2022[1], Cláusulas 5 a 8, y se utilizará en contexto con6.1.3 .

**Tabla A.1 — Controles de seguridad de la información**

| | | |
|---|---|---|
| **5** | **Controles organizacionales** | |
| 5.1 | Políticas de seguridad de la información | **Control**<br>La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. |
| 5.2 | Roles y responsabilidades de seguridad de la información | **Control**<br>Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de |
| 5.3 | Segregación de deberes | **Control**<br>Deben separarse los deberes conflictivos y las áreas conflictivas de responsabilidad. |
| 5.4 | responsabilidades de gestión | **Control**<br>La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización. |
| 5.5 | Contacto con autoridades | **Control**<br>La organización deberá establecer y mantener contacto con las autoridades pertinentes. |
| 5.6 | Contacto con grupos de interés especial | **Control**<br>La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales. |
| 5.7 | Inteligencia de amenazas | **Control**<br>La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para generar información sobre amenazas. |
| 5.8 | Seguridad de la información en la gestión de proyectos. | **Control**<br>La seguridad de la información se integrará en la gestión de proyectos. |
| 5.9 | Inventario de información y otros activos asociados | **Control**<br>Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios. |
| 5.10 | Uso aceptable de la información y otros activos asociados | **Control**<br>Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados. |
| 5.11 | Devolución de activos | **Control**<br>El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo. |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| 5.12 | Clasificación de la información | **Control**<br>La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas. |
| 5.13 | Etiquetado de información | **Control**<br>Se debe desarrollar e implementar un conjunto apropiado de procedimientos de la información adoptado por la organización. |
| 5.14 | Transferencia de información | **Control**<br>Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes. |
| 5.15 | Control de acceso | **Control**<br>Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio. |
| 5.16 | Gestión de identidad | **Control**<br>Se gestionará el ciclo de vida completo de las identidades. |
| 5.17 | Información de autenticación | **Control**<br>La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación. |
| 5.18 | Derechos de acceso | **Control**<br>Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización. |
| 5.19 | Seguridad de la información en las relaciones con los proveedores | **Control**<br>Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor. |
| 5.20 | Abordar la seguridad de la información en los acuerdos con los proveedores | **Control**<br>Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor. |
| 5.21 | Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC) | **Control**<br>Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC. |
| 5.22 | Seguimiento, revisión y gestión de cambios de servicios de proveedores | **Control**<br>La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios. |
| 5.23 | Seguridad de la información para el uso de servicios en la nube | **Control**<br>Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización. |
| 5.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información | **Control**<br>La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| 5.25 | Evaluación y decisión sobre eventos de seguridad de la información | **Control**<br>La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información. |
| 5.26 | Respuesta a incidentes de seguridad de la información | **Control**<br>Se debe responder a los incidentes de seguridad de la información de acuerdo con los |
| 5.27 | Aprender de los incidentes de seguridad de la información | **Control**<br>El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información. |
| 5.28 | Recolección de evidencia | **Control**<br>La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información. |
| 5.29 | Seguridad de la información durante la interrupción | **Control**<br>La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción. |
| 5.30 | Preparación de las TIC para la continuidad del negocio | **Control**<br>La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. |
| 5.31 | Requisitos legales, estatutarios, reglamentarios y contractuales | **Control**<br>Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados. |
| 5.32 | Derechos de propiedad intelectual | **Control**<br>La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual. |
| 5.33 | Protección de registros | **Control**<br>Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada. |
| 5.34 | Privacidad y protección de la información de identificación personal (PII) | **Control**<br>La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y |
| 5.35 | Revisión independiente de la seguridad de la información. | **Control**<br>El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos. |
| 5.36 | Cumplimiento de políticas, normas y estándares de seguridad de la información | **Control**<br>El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente. |
| 5.37 | Procedimientos operativos documentados | **Control**<br>Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite. |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| **6** | **Controles de personas** | |
| 6.1 | Poner en pantalla | **Control**<br>Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y la riesgos percibidos. |
| 6.2 | Términos y condiciones de empleo | **Control**<br>Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información. |
| 6.3 | Concientización, educación y capacitación en seguridad de la información | **Control**<br>El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral. |
| 6.4 | Proceso Disciplinario | **Control**<br>Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información. |
| 6.5 | Responsabilidades después de la terminación o cambio de empleo | **Control**<br>Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas. |
| 6.6 | Acuerdos de confidencialidad o no divulgación | **Control**<br>Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes. |
| 6.7 | Trabajo remoto | **Control**<br>Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización. |
| 6.8 | Informes de eventos de seguridad de la información | **Control**<br>La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna. |
| **7** | **Controles físicos** | |
| 7.1 | Perímetros físicos de seguridad | **Control**<br>Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados. |
| 7.2 | Entrada física | **Control**<br>Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados. |
| 7.3 | Asegurar oficinas, salas e instalaciones | **Control**<br>Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones. |
| 7.4 | Monitoreo de seguridad física | **Control**<br>Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado. |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| 7.5 | Protección contra amenazas físicas y ambientales. | **Control**<br>Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura. |
| 7.6 | Trabajar en áreas seguras | **Control**<br>Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras. |
| 7.7 | Escritorio despejado y pantalla despejada | **Control**<br>Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información. |
| 7.8 | Emplazamiento y protección de equipos | **Control**<br>El equipo se colocará de forma segura y protegida. |
| 7.9 | Seguridad de los activos fuera de las instalaciones | **Control**<br>Se protegerán los activos fuera del sitio. |
| 7.10 | Medios de almacenamiento | **Control**<br>Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización. |
| 7.11 | Utilidades de apoyo | **Control**<br>Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo. |
| 7.12 | seguridad del cableado | **Control**<br>Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños. |
| 7.13 | Mantenimiento de equipo | **Control**<br>El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información. |
| 7.14 | Eliminación segura o reutilización de equipos | **Control**<br>Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización. |
| **8** | **Controles tecnológicos** | |
| 8.1 | Dispositivos de punto final de usuario | **Control**<br>Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario. |
| 8.2 | Derechos de acceso privilegiado | **Control**<br>La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará. |
| 8.3 | Restricción de acceso a la información | **Control**<br>El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso. |
| 8.4 | Acceso al código fuente | **Control**<br>El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente. |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| 8.5 | Autenticación segura | **Control**<br>Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso. |
| 8.6 | Gestión de capacidad | **Control**<br>El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos. |
| 8.7 | Protección contra malware | **Control**<br>La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario. |
| 8.8 | Gestión de vulnerabilidades técnicas | **Control**<br>Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas. |
| 8.9 | Gestión de la configuración | **Control**<br>Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse. |
| 8.10 | Eliminación de información | **Control**<br>La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria. |
| 8.11 | Enmascaramiento de datos | **Control**<br>El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable. |
| 8.12 | Prevención de fuga de datos | **Control**<br>Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible. |
| 8.13 | Copia de seguridad de la información | **Control**<br>Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada. |
| 8.14 | Redundancia de las instalaciones de procesamiento de información | **Control**<br>Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad. |
| 8.15 | Inicio sesión | **Control**<br>Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes. |
| 8.16 | Actividades de seguimiento | **Control**<br>Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información. |
| 8.17 | Sincronización de reloj | **Control**<br>Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas. |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| 8.18 | Uso de programas de utilidad privilegiados | **Control**<br>El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado. |
| 8.19 | Instalación de software en sistemas operativos | **Control**<br>Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos. |
| 8.20 | Seguridad en redes | **Control**<br>Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones. |
| 8.21 | Seguridad de los servicios de red. | **Control**<br>Se identificarán, implementarán y controlarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red. |
| 8.22 | Segregación de redes | **Control**<br>Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización. |
| 8.23 | Filtrado web | **Control**<br>El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso. |
| 8.24 | Uso de criptografía | **Control**<br>Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas. |
| 8.25 | Ciclo de vida de desarrollo seguro | **Control**<br>Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas. |
| 8.26 | Requisitos de seguridad de la aplicación | **Control**<br>Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones. |
| 8.27 | Principios de arquitectura e ingeniería de sistemas seguros | **Control**<br>Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información. |
| 8.28 | Codificación segura | **Control**<br>Los principios de codificación segura se aplicarán al desarrollo de software. |
| 8.29 | Pruebas de seguridad en desarrollo y aceptación. | **Control**<br>Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo. |
| 8.30 | Desarrollo subcontratado | **Control**<br>La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados. |
| 8.31 | Separación de los entornos de desarrollo, prueba y producción | **Control**<br>Los entornos de desarrollo, prueba y producción deben estar separados y protegidos. |
| 8.32 | Gestión del cambio | **Control**<br>Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios. |
| 8.33 | Información de prueba | **Control**<br>La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente. |

**Tabla A.1***(continuado)*

| | | |
|---|---|---|
| 8.34 | Protección de los sistemas de información durante las pruebas de auditoría | **Control**<br>Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente. |

# Bibliografía

[1] ISO/CEI 27002:2022, *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información*

[2] ISO/CEI 27003, *Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información sistemas — Orientación*

[3] ISO/CEI 27004, *Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información — Seguimiento, medición, análisis y evaluación*

[4] ISO/CEI 27005, *Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de los riesgos de seguridad de la información*

[5]ISO 31000:2018, *Gestión de riesgos — Directrices*

**ICS 03.100.70; 35.030**

Precio basado en 19 páginas