Uruguay Presidencia | agesic

# Guía
# Gestión de vulnerabilidades

Seguridad de la información – Gestión y auditoría

Versión 2.0

Año 2022

## Contenido

Acerca de esta guía ..... 3
Acerca de las vulnerabilidades ..... 3
Proceso de gestión de vulnerabilidades ..... 4
1.Identificar activos ..... 4
Fases propuestas para la identificación de activos ..... 5
2. Planificar el análisis de vulnerabilidades ..... 9
3. Ejecutar el análisis de vulnerabilidades ..... 9
4. Clasificar las vulnerabilidades ..... 10
5. Priorizar las correcciones de vulnerabilidades ..... 11
Paso 1: Decidir lo que es necesario solucionar ..... 12
Paso 2: Decidir qué puede solucionarse ..... 13
6. Remediar las vulnerabilidades ..... 13
7. Validar ..... 14

## Acerca de esta guía

La gestión de vulnerabilidades ayuda a proteger la información de una organización con la finalidad de mantener la confidencialidad, integridad y disponibilidad de los sistemas.

Este documento se centra en la gestión de vulnerabilidades para software y hardware de utilización masiva, mediante la búsqueda de configuraciones débiles conocidas y la implementación de parches. Queda fuera del alcance de esta guía aquellas vulnerabilidades del software a medida o el descubrimiento de problemas desconocidas incluso por los fabricantes del software.

## Acerca de las vulnerabilidades

Una vulnerabilidad de seguridad es un fallo técnico, o deficiencia de un sistema, que puede permitir el acceso ilegítimo a información o llevar a cabo operaciones no autorizadas de manera remota.

La práctica más segura sería corregir todas las vulnerabilidades tan pronto como se publique el parche relevante para los sistemas afectados. Sin embargo, algunas variables como las limitaciones de recursos, las interrupciones que puedan darse a las tareas necesarias para el negocio o las compatibilidades con el hardware y software utilizados, pueden volver a esta práctica inviable.

Las actualizaciones de software pueden implicar algún riesgo ya que las herramientas pueden funcionar de manera diferente cuando se ejecutan.

La posibilidad de una actualización masiva altera a cualquier empresa, y es posible que no todas las empresas cuenten con las habilidades adecuadas para planificar e implementar dicha tarea. De esta manera, los retrasos en el trabajo de actualización solo aumentan el tamaño de la tarea, haciéndola más cara y menos atractiva.

## Proceso de gestión de vulnerabilidades

Pueden distinguirse siete fases en el proceso de gestión de vulnerabilidades:

1. Identificar activos.
2. Planificar el análisis de vulnerabilidades.
3. Ejecutar el análisis de vulnerabilidades.
4. Clasificar las vulnerabilidades encontradas.
5. Priorizar las vulnerabilidades.
6. Remediar.
7. Validar.


### 1.Identificar activos

Elaborar un inventario de forma de tener identificados todos los activos de la organización que es necesario mantener protegidos a través de controles adecuados.

Si la organización ya cuenta con inventarios, modelos de procesos de negocio o diagramas de red, por ejemplo, se puede comenzar por ellos verificando que estén debidamente actualizados.

Es recomendable la utilización de software que permita su clasificación y definir procesos que permitan la automatización del inventario. Dichos procesos, y/o los procedimientos asociados, deben además documentarse.

No es necesario contar con un inventario exhaustivo de cada activo, pero si tener identificados al menos grupos de ellos que puedan necesitar los mismos controles, por ejemplo, agrupar sistemas que tienen configuraciones similares y que se utilizan para las mismas tareas.

Como regla general se pueden agrupar los componentes cuando:

- Son del mismo tipo.
- Tienen configuraciones idénticas o casi idénticas.
- Están integradas en la red de la misma o casi de la misma manera.
- Están sujetos a las mismas condiciones administrativas y de infraestructura.
- Usan las mismas aplicaciones.
- Tienen los mismos requisitos de protección.

Se debe tener precaución al determinar los objetos que se desea agrupar, si se hace con activos que tienen diferentes requisitos de protección puede dar lugar a vulnerabilidades de seguridad.

## Fases propuestas para la identificación de activos

a. Procesos de negocios


Teniendo en cuenta que el objetivo siempre es proteger la información crítica de una organización, para identificar qué es crítico es necesario examinar los procesos de negocio y pensar qué información es necesaria para permitir que esos procesos se ejecuten.

Los resultados pueden presentarse en una tabla que detalle:

- Identificador único.
- Nombre.
- Descripción de su propósito, los flujos de trabajo involucrados y la información procesada.
- Responsables.
- Aplicaciones claves que requiere el proceso.

b. Aplicaciones


Implica identificar las soluciones de Tecnologías de la Información (TI) que respaldan los procesos comerciales y operativos de la organización. Este tipo de activos requiere, por parte de quienes están involucrados en estos procesos, de un nivel mínimo de protección de acuerdo a requisitos de confidencialidad, integridad y disponibilidad*.

* Se recomienda realizar talleres que involucren no solo al departamento de TI de la organización sino también a quienes utilizan estos activos como responsables de los procesos y aplicaciones.

Para cada aplicación identificada como esencial puede crearse una tabla con el siguiente nivel de detalle:

- Identificador único (un número o abreviatura)
- Nombre
- Breve descripción de su finalidad y la información tratada
- Responsable
- Quienes usan la aplicación

Además, se deberán documentar las dependencias que existen entre aplicaciones, procesos de negocios y tareas especializadas, es decir, identificar los procesos y tareas en los que se usa una aplicación determinada.

Al identificarlas, es mejor aplicar un nivel adecuado de granularidad y considerar su nivel de detalle.

Por ejemplo, no es aconsejable dividir un producto de Microsoft Office en sus partes constituyentes (procesamiento de texto, presentaciones, hojas de cálculo, entre otras.) y describirlos individualmente. Por otra parte, no ser lo suficientemente granular (software, base de datos, portales, entre otras), impedirá lograr la diferenciación necesaria y, en particular, definir los controles específicos.

c. Diagrama de redes


Un diagrama de red es una descripción gráfica de los componentes de una red y sus interconexiones. Es importante que estos esquemas contengan como mínimo los siguientes objetos:

- Sistemas de TI en la red, incluidas las computadoras (clientes y servidores), impresoras de red y activos componentes de red (switch, router, access point).
- Conexiones que unen estos sistemas de TI a través de LAN (por ejemplo, Ethernet), tecnología de red troncal.
- Conexiones externas de estos sistemas; (conexiones a internet, VPN, etc.)

La organización generalmente ya cuenta con un diagrama de red de este tipo, sin embargo, están sujetos a cambios frecuentes, por eso es conveniente revisarlo frecuentemente para determinar si toda la información sigue siendo precisa.

Existen herramientas que pueden generar automáticamente un diagrama de red, basado en las circunstancias encontradas en una red dada. Sin embargo, estas ilustraciones suelen contener mucha más información de la que realmente se requiere. En particular, tampoco logran agrupar los sistemas o equipos disponibles de manera adecuada.

La recomendación es agrupar los componentes individuales, con una agregación lo suficientemente pertinente para el negocio, permitiendo así obtener una vista clara de los componente o grupos de componentes a proteger según su criticidad.

d. Equipos de TI


Al identificar los equipos de TI, se debe compilar aquellos que están en funcionamiento actualmente y los que está previsto incorporar. Asimismo, se listarán los componentes de la red de información correspondiente y sus características, y se documentará las aplicaciones para las que cada equipo de TI es relevante.

Los equipos de TI incluyen:

- Todas las computadoras (clientes y servidores), grupos de computadoras, componentes de red activos, redes e impresoras en una red determinada.
- Sistemas de control industrial (ICS) que pueden incluir dispositivos utilizados con fines de control o supervisión en producción, como lógica programable

controladores (PLC), máquinas que se controlan a través de redes inalámbricas y vehículos autónomos.
- Computadoras de estación de trabajo utilizadas para controlar máquinas junto con los dispositivos conectados a estas computadoras (como escáneres o impresoras).
- Dispositivos de telecomunicaciones, teléfonos móviles y otros dispositivos móviles.
- Internet de las cosas (IoT), es decir, dispositivos en red capaces de recopilar, almacenar, procesar y transmitir datos. Incluyen cámaras web, componentes domésticos inteligentes y asistentes virtuales activados por voz.

Los detalles que se requieren para identificar los equipos de TI son:

- Un identificador único.
- En el caso de un grupo, el número de equipos que contiene.
- Una descripción. Es especialmente importante citar el tipo y propósito del equipo, por ejemplo: personal, servidor de administración o enrutador a Internet público.
- Plataforma (tipo de hardware, sistema operativo).
- Ubicación (edificio y número de habitación).
- Estado (planeado, en prueba, operativo).
- Usuarios con acceso habilitado.
- Administrador del equipo.

Cuando se trate de equipos de TI en red, es importante asegurar que la información de la lista coincida con el diagrama de red.

### e. Espacios físicos


El grado de protección de la información y los activos relacionados dependen también de la seguridad del entorno físico en el que se alojan. Es por esta razón que se deben identificar todos los edificios y locales que son de importancia en relación con la información y el negocio, junto con salas de servidores y otros espacios relacionados explícitamente con TI. Se pueden incluir los caminos trazados por: líneas de comunicación; oficinas, salas de formación y reuniones; e instalaciones de archivos.

Los detalles mínimos a incluir en la identificación de espacios físicos serán:

- Nombre.
- Descripción.
- Tipo.
- Locación.

## 2. Planificar el análisis de vulnerabilidades

Recomendamos que las organizaciones realicen evaluaciones de vulnerabilidades mensualmente. Se informan nuevas vulnerabilidades constantemente y muchos proveedores de software lanzan actualizaciones en un ciclo mensual (como el “Patch Tuesday” de Microsoft).

Un régimen de evaluación regular es esencial para garantizar que la organización sea consciente de los riesgos presentes.

## 3. Ejecutar el análisis de vulnerabilidades

Si bien el estado de los parches de software se puede recopilar utilizando paquetes de administración de activos, se debe usar un Sistema de Evaluación de Vulnerabilidades Automatizado (VAS por sus siglas en inglés) para identificar las vulnerabilidades de los sistemas y equipos de TI de la organización.

Las suites de administración de activos de software no siempre buscan bibliotecas vulnerables y no verifican configuraciones erróneas.

Los VAS realizan acciones contra un sistema de destino, luego evalúan los datos devueltos con firmas de vulnerabilidades conocidas (por ejemplo: el número de versión informado por el servicio de red, el cual se compara contra vulnerabilidades conocidas).

Cuando se utilice un VAS, es necesario:

- Evaluar los sistemas desde una perspectiva externa, por ejemplo, desde Internet, así como desde una perspectiva interna, asumiendo que el diseño del sistema diferencia entre estas dos ubicaciones.

- Supervisar las cuentas utilizadas para ejecutar análisis de evaluación de vulnerabilidades en busca de cualquier actividad inusual. Cuando no se esté realizando una evaluación, hay que considerar deshabilitar la cuenta o cambiar las credenciales asociadas a ella.

- Realizar escaneos de las redes, además de escaneos específicos de sistemas conocidos, con el objetivo de descubrir dispositivos potencialmente desconocidos o no autorizados.

- Tener en cuenta que un VAS puede provocar resultados inesperados, que pueden incluir la corrupción de datos. Estos resultados son muy poco probables en sistemas relativamente modernos (aquellos desarrollados posteriores al 2010), pero es recomendable probar el VAS con copias de sistemas críticos que no sean de producción antes de ponerlo en funcionamiento.

- Ejecutar el VAS con las credenciales (típicamente usuario y contraseña) necesarias para realizar una evaluación en el host (computadora, servidor o sistema) no simplemente un escaneo no autenticado (sin credenciales). Algunos VAS usan un agente en el host, mientras que otros usan credenciales privilegiadas para autenticar y consultar el estado de los dispositivos. La elección entre estas dos opciones es una cuestión de qué es más fácil de integrar para la empresa en sus sistemas.

Las credenciales privilegiadas que se utilizan para realizar la evaluación de vulnerabilidades se utilizan para conectarse a una gran cantidad de sistemas y existe el riesgo de que quien ataque acceda al sistema comprometido.

## 4. Clasificar las vulnerabilidades

Se recomienda que en esta tarea participen personas con conocimientos de los riesgos de ciberseguridad, de negocio y de la gestión de activos de TI.

El software de evaluación de vulnerabilidades normalmente asignará una clasificación de gravedad a los problemas, la cual es un punto de partida, pero, dado que no toma en cuenta ningún riesgo de negocio o circunstancias atenuantes, no debe tomarse como un resultado definitivo.

Hay que tener en cuenta que la primera vez que se ejecuta un análisis a un sistema, pueden surgir muchas vulnerabilidades. Se debe dedicar tiempo a evaluarlas, basándose en toda la información disponible.

Recomendamos no ignorar los problemas que están marcados como “Críticos” o “Altos”.

El Common Vulnerability Scoring System (CVSS) es un marco abierto para comunicar las características y la gravedad de las vulnerabilidades del software, les asigna puntuaciones numéricas e intenta ayudar en el proceso de clasificación de las mismas. Puede ser una herramienta útil si se usa correctamente, pero hay que asegurarse de:

- No seleccionar una puntuación arbitraria por encima de la cual las vulnerabilidades deban corregirse, ignorando todos los problemas por debajo de ese nivel.

- No tomar puntuaciones CVSS brutas sin tener en cuenta las prioridades o mitigaciones específicas de la empresa.

Se deben clasificar las vulnerabilidades encontradas en tres categorías:

- Corregir
- Reconocer
- Investigar

Las vulnerabilidades a **corregir** son aquellas para las cuales es necesario aplicar un parche, una reconfiguración o una mitigación. Se debe dar prioridad a estas correcciones y otorgarles una fecha en la cual se implementarán.

Las vulnerabilidades **reconocidas** son aquellas que se decide que no sean corregidas en lo inmediato. Existen razones válidas para no resolver de inmediato una vulnerabilidad, estas deben registrarse junto con el razonamiento para reconocerla y una fecha de revisión. Si el nivel de riesgo que presentan es suficientemente alto, se debe registrar el problema en una bitácora de riesgos.

El motivo para reconocer un problema y no solucionarlo, debería ser suficiente para justificar la decisión tomada en caso de que la vulnerabilidad explote en el futuro.

Las vulnerabilidades a **investigar** deben usarse solo como un estado temporal mientras no puedan ser categorizados como "corregir" o "reconocer". Esto puede deberse a que se desconoce el costo de resolver el problema o que hay varias soluciones posibles y se requiere más tiempo para identificar cuál funciona mejor. El software de evaluación de vulnerabilidades no es infalible y pueden producirse falsos positivos. Cuando se sospeche de un caso se recomienda realizar una investigación antes de eliminar el problema. Los plazos para los problemas de esta categoría dependerán de su potencial gravedad.

La decisión de solucionar o no un problema es, en el fondo, una decisión de negocio y cada organización deberá definirlo.

## 5. Priorizar las correcciones de vulnerabilidades

Se deben priorizar las vulnerabilidades concentrándose en las que:

- Son accesibles para la mayor cantidad de potenciales atacantes.
- Tendrían el mayor impacto si se las explotara para la operativa de la organización.

El número de atacantes potenciales depende de la accesibilidad de la vulnerabilidad y la complejidad de la explotación.

El impacto de la explotación consiste tanto en lo técnico como en el negocio. Por ejemplo:

- Impacto técnico: un problema que podría permitir una denegación de servicio generalmente se considera un impacto menor, en comparación con un ataque donde un actor malicioso obtenga la capacidad de ejecutar código propio dentro del sistema destino.
- Impacto en el negocio: una vulnerabilidad en un sistema de procesamiento de pagos es mayor que una en un sistema de reserva de salas de reuniones.

A continuación, se proporciona un conjunto de pautas de muestra para decidir qué problemas deben solucionarse.

### Paso 1: Decidir lo que es necesario solucionar

**Prioridad 1:** Reparar los servicios expuestos a Internet y las aplicaciones web estándar que pueden explotarse automáticamente sin interacción de quien la usa o quien quiere atacar.

- Asegurar cualquier servicio al que se pueda acceder directamente desde Internet y para el que existan vulnerabilidades conocidas, explotables y graves. Los escáneres de vulnerabilidades pueden filtrar aquellos que tienen *exploits* conocidos y son 'altos' o 'críticos' en términos de su impacto negativo potencial.
- Incluir cualquier aplicación web lista para usar; si contienen vulnerabilidades conocidas, son altamente vulnerables a la explotación, incluida la explotación automatizada no dirigida.

**Prioridad 2:** Reparar las aplicaciones web específicas que puedan explotarse en Internet sin interacción de quien la usa o quien quiere atacar.

- Aplicaciones web seguras a medida, es decir, cualquier elemento que ejecute código en un sitio web, que no se haya comprado a un proveedor o que no provenga de un proyecto de código abierto importante. Estas aplicaciones web están cada vez más sujetas a ataques.
- En primera instancia, priorizar los servidores accesibles desde fuera del entorno.

**Prioridad 3:** Solucionar problemas que pueden explotarse en Internet con una interacción mínima de personas usuarias, como vulnerabilidades de la estación de trabajo, descargas no autorizadas o ataques basados en correo electrónico.

- Proteger las estaciones de trabajo contra descargas no autorizadas y ataques basados en correo electrónico. La protección de los navegadores web y las aplicaciones comunes es fundamental.
- No es necesario actualizar el sistema operativo de inmediato, aunque las versiones anteriores de Windows no son compatibles con las aplicaciones más nuevas.

**Prioridad 4:** Solucionar problemas que pueden explotarse en Internet con ingeniería social como aplicaciones maliciosas descargadas de la web o enviadas por correo electrónico. Estos ataques requieren que quienes lo usan desempeñen un papel, por ejemplo, descargando un archivo infectado o haciendo clic en un enlace o un archivo adjunto en un correo electrónico de Phishing.

### Paso 2: Decidir qué puede solucionarse

Decidir qué puede solucionarse es una definición de alto nivel y no solo un problema de TI.

La toma de decisiones prioritarias deberá combinar los siguientes factores:

- Lista de prioridades altas
- Costo directo
- Costo en contratiempos al personal
- Disponibilidad y costo de la solución a corto plazo
- Costo y disponibilidad de recursos calificados
- Costo de respuesta y recuperación ante incidentes (incluidas las multas impuestas)
- Daño a la reputación

Es relevante registrar las razones de las decisiones tomadas y establecer un plazo para revisar aquellos problemas que se definió “reconocer” y no “corregir”. Esta decisión, debe ser tomada a nivel de dirección de manera tal que la persona responsable de la misma pueda defenderla si se explota una vulnerabilidad en el futuro.

Para impulsar la remediación, las personas propietarias del activo necesitan datos empíricos de las vulnerabilidades encontradas para determinar cuáles deben corregirse junto con las instrucciones de cómo llevar a cabo la remediación.

Los informes deben describir:

- los activos más vulnerables,
- las vulnerabilidades de mayor puntuación,
- que aplicaciones específicas son altamente vulnerables.

## 6. Remediar las vulnerabilidades

En esta etapa se buscarán e implementarán los parches correspondientes a las vulnerabilidades clasificadas en estado a “corregir” en el orden de prioridad establecido.

Esto permitirá a las personas propietarias del sistema priorizar sus esfuerzos con un enfoque en las vulnerabilidades que reducirán la mayor cantidad de riesgos para la organización.

Al remediar se debe respetar el proceso de gestión de cambios:

- Testeando, en la medida de lo posible, los cambios en un ambiente de prueba antes de impactarlo en producción.
- Generando respaldos para prever los *rollback*.

## 7. Validar

Es importante validar el resultado de los hallazgos entre los escaneos de vulnerabilidades para ver si en siguientes iteraciones aumenta o se reduce la cantidad de vulnerabilidades detectadas.

Algunas métricas que se pueden definir para controlar el proceso son:

- Puntaje promedio de vulnerabilidad de cada activo por propietario y en general.
- Tiempo, en promedio, para remediar las vulnerabilidades por propietario y en general.
- Porcentaje de los activos que no ha sido escaneado recientemente en búsqueda de vulnerabilidades.
- Cantidad de vulnerabilidades explotables de forma remota que otorgan acceso privilegiado expuestas en los sistemas.

La clave es mostrar el progreso mes a mes, trimestre a trimestre y año a año.

Los puntajes de riesgo por vulnerabilidades y el tiempo para la remediación deben disminuir a medida que los equipos se familiarizan con el proceso y conocen mejor los riegos.