Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Estándar Escaneo de Vulnerabilidades

17
CAPÍTULO

Estándar de TI:
Estándar Escaneo de Vulnerabilidades

1.0 Propósito y Beneficios

Las Reparticiones utilizan herramientas automatizadas para escanear sistemas, dispositivos informáticos y de red, aplicaciones web y códigos de aplicaciones. Los resultados de estos análisis ayudan a informar al Ministerio de Planificación Estratégica y Modernización y a los administradores del sistema sobre vulnerabilidades conocidas y potenciales.

La gestión de vulnerabilidades es un proceso mediante el cual las vulnerabilidades identificadas mediante el escaneo se rastrean, evalúan, priorizan y gestionan hasta que se remedian o se resuelven adecuadamente. La gestión de las vulnerabilidades identificadas durante los análisis garantiza que se tomen las medidas adecuadas para reducir la posibilidad de que estas vulnerabilidades sean explotadas y, por lo tanto, reducir el riesgo de comprometer la confidencialidad, integridad y disponibilidad de los activos de información.

2.0 Declaración de información

Según la Política de seguridad de la información, todos los sistemas deben escanearse en busca de vulnerabilidades. Además, cada sistema debe estar inventariado y tener asignada una responsabilidad individual o grupal para el mantenimiento y la administración.

2.1 TIPOS DE EXPLORACIONES

El tipo de análisis de vulnerabilidad apropiados para un objetivo determinado depende del tipo de objetivo (es decir, hardware, software, código fuente) y de la ubicación del objetivo (es decir, interno o externo a la red). La siguiente tabla enumera los tipos de análisis de vulnerabilidades requeridos por este estándar.

Tipo	Descripción
Escaneo de infraestructura externa	Escaneos del perímetro de las redes o de cualquier infraestructura alojada disponible externamente para identificar posibles vulnerabilidades en la infraestructura de TI accesible a Internet.
Infraestructura interna Escanear	Escaneos de la infraestructura de TI en redes protegidas o cualquier infraestructura alojada para identificar posibles vulnerabilidades.
Escaneo de aplicaciones web “lite”	Escaneos superficiales no autenticados de aplicaciones web de producción externas para identificar vulnerabilidades de seguridad.
Escaneo en profundidad de aplicaciones web	Al momento de implementación, se debe escanear en profundidad con autenticación de las aplicaciones web para identificar vulnerabilidades de seguridad.
Análisis del código fuente de la aplicación	Durante el desarrollo de software se deben ejecutar escaneos del código fuente de la aplicación para identificar problemas en el código que podrían causar posibles vulnerabilidades.

2.2 ESCANEO

Las Reparticiones son responsables de confirmar que se realizan análisis de vulnerabilidades. Las Reparticiones deben utilizar una herramienta de escaneo aprobada por la ISO/encargados de seguridad designado. Cualquier herramienta de escaneo aprobada debe poder proporcionar sugerencias de solución y asociar un valor de gravedad a cada vulnerabilidad descubierta en función del impacto relativo de la vulnerabilidad en el sistema afectado.

Según el Estándar de clasificación de la información, los informes de escaneo se clasifican con confidencialidad e integridad moderadas y deben protegerse como tales.

Las Reparticiones deben proporcionar todas las direcciones IP externas y localizadores uniformes de recursos (URL) para todas las aplicaciones web externas a los encargados de seguridad designados/ISO.

Los administradores de redes y sistemas deben proporcionar acceso suficiente para permitir que el motor de escaneo de vulnerabilidades explore todos los

servicios proporcionados por el sistema. Ningún dispositivo conectado a la red deberá configurarse específicamente para bloquear los escaneos de vulnerabilidades de los motores de escaneo autorizados.

Los análisis se deben realizar dentro del ciclo de vida de desarrollo del sistema (consultar el estándar relacionado) en entornos previos a la implementación, cuando se implementan en el entorno de implementación de destino y periódicamente a partir de entonces, como se especifica a continuación:

a. Los análisis previos a la implementación se realizan antes de mover el sistema o la aplicación web al entorno de implementación de destino:

    1. Todos los sistemas deben someterse a un escaneo de infraestructura interna autenticado, cuando sea técnicamente factible o necesario, antes de implementarse en el entorno de implementación de destino. Cualquier vulnerabilidad de infraestructura descubierta debe ser remediada o determinada como un falso positivo o un riesgo insignificante por el Oficial de Seguridad de la Información (ISO)/encargado de seguridad designado, antes de implementar el sistema para el uso previsto.

    2. Cuando el código fuente está disponible, las aplicaciones deben someterse a un escaneo del código fuente antes de que el código actualizado pase al entorno de implementación de destino si ha habido un cambio en el código de la aplicación.

    3. Los análisis deben autenticarse cuando la aplicación requiere autenticación antes de implementarse en el entorno de implementación de destino o en un entorno al que se pueda acceder externamente. Cuando se requiere autenticación para acceder a la aplicación, los análisis deben ejecutarse con acceso autenticado en cada nivel de acceso (por ejemplo, usuario, administrador) admitido por la aplicación, excepto cuando las limitaciones de la herramienta impidan el análisis autenticado. Cualquier vulnerabilidad de la aplicación web descubierta debe ser remediada o determinada como un falso positivo o un riesgo insignificante por parte del encargado de seguridad designado o del ISO, antes de colocar el sistema en el entorno de implementación de destino.

    4. Cualquier sistema o aplicación implementada en su entorno de implementación objetivo con vulnerabilidades no remediadas debe tener un plan de remediación formal y la aprobación documentada del ejecutivo responsable de la gestión de riesgos o su designado.

b. Los escaneos de implementación ocurren la primera vez que un sistema o aplicación web se mueve a su entorno de implementación de destino:

    1. Los sistemas deben escanearse inmediatamente después de colocarse en el entorno de implementación de destino con un escaneo de infraestructura interna autenticado, cuando sea técnicamente factible o necesario. Si se puede acceder al sistema desde Internet o una red externa, entonces el sistema debe escanearse con un escaneo de infraestructura externa.

    2. Las aplicaciones web deben escanearse dentro del primer mes de su colocación en el entorno de implementación de destino. Si es posible, se requiere un análisis en profundidad de la aplicación web autenticado, pero como mínimo se requiere un análisis "lite" de la aplicación web. Se deben considerar la sensibilidad y criticidad de la aplicación al determinar el cronograma para el escaneo de implementación inicial.

c. Escaneos recurrentes: después del escaneo inicial en el entorno de implementación de destino, la frecuencia de los escaneos debe ocurrir de acuerdo con la clasificación de riesgo del sistema o la aplicación (consulte la Tabla 2).

    1. Al realizar análisis de infraestructura interna en sistemas creados con una imagen compartida, como estaciones de trabajo, los análisis se pueden ejecutar en una muestra de sistemas, pero el conjunto de muestras debe variar de un análisis a otro.

    2. Las aplicaciones web en producción deben someterse a análisis recurrentes. Como mínimo, las aplicaciones web en producción deben someterse a análisis "lite" recurrentes.

    3. Todas las vulnerabilidades encontradas durante los análisis deben abordarse según lo establecido en **sección de remediación** abajo.

2.3 DETERMINAR LA CLASIFICACIÓN DE RIESGO Y LA FRECUENCIA DE LOS ESCANEOS

El riesgo que las vulnerabilidades representan para los sistemas y aplicaciones se basa en la probabilidad de que una vulnerabilidad sea explotada y el impacto si la confidencialidad, integridad o disponibilidad de los activos de información se vieran comprometidas. La probabilidad de que se aproveche una vulnerabilidad aumenta en relación directa con la accesibilidad del sistema o la aplicación desde otros sistemas.

El impacto sobre los activos de información se basa en la clasificación de la información del activo (ver Norma de Clasificación de Información). Se debe considerar el impacto (es decir, alto, moderado o bajo) si la confidencialidad, integridad o disponibilidad se ve comprometida y se debe utilizar la calificación de impacto individual más alta para la confidencialidad, integridad o disponibilidad dentro de la siguiente tabla.

Tabla 2: CLASIFICACIÓN DE RIESGO			
Impacto (Confidencialidad, Integridad, Disponibilidad)	Exposición		
	Sistemas sin conectividad de red a los datos de producción.	Sistemas con conectividad de red a datos de producción (sin acceso a Internet)	Sistema que está disponible públicamente en Internet.
Alto	Medio	Alto	Alto
Medio	Bajo	Medio	Alto
Bajo	Bajo	Bajo	Medio

La frecuencia mínima de los escaneos depende de la clasificación de riesgo. Los sistemas sin una clasificación de riesgo deben escanearse como si tuvieran una clasificación de riesgo “Alto” hasta que sean calificados.

TABLA 3: FRECUENCIA DE ESCANEOS	
Calificación de riesgo	Frecuencia
Escaneos de infraestructura	
Alto	Mensual
Medio	Trimestral
Bajo	Semi anualmente
Escaneos de aplicaciones web	
Alto	Trimestralmente o después de un cambio significativo
Medio	Semi anualmente
Bajo	Anualmente

2.4 REMEDIACIÓN

Las vulnerabilidades descubiertas durante los análisis deben remediarse según la clasificación de riesgo (consulte Tabla 2) y la gravedad de la vulnerabilidad identificada por la herramienta de escaneo según la siguiente tabla.

TABLA 4: PLAZOS DE REMEDIACIÓN			
Calificación de riesgo (de Tabla 2)	Gravedad de la vulnerabilidad		
	Bajo o por debajo	**Por encima de bajo a por debajo de alto**	**Alto o superior**
Alto	A discreción del ISO/encargado de seguridad designado	Plan de acción en 2 semanas, resuelto en 6 meses	Plan de acción en 1 semana, resuelto en 1 mes
Medio	A discreción del ISO/ encargado de seguridad designado	Plan de Acción en 3 Semanas, Resuelto en 1 año	Plan de acción en 2 semanas, resuelto en 6 meses
Bajo	A discreción del ISO/ encargado de seguridad designado	A discreción del ISO/ encargado de seguridad designado	Plan de Acción en 3 semanas, resuelto en 1 año

El encargado de seguridad designado/ISO puede revisar las vulnerabilidades para ajustar la clasificación de gravedad si es necesario. Se deben realizar pruebas para verificar que se haya completado la remediación.

Las personas que administran los análisis de vulnerabilidades deben notificar al ISO/encargado de seguridad designado dentro de **1 día hábil** después de la finalización del análisis para detectar nuevas vulnerabilidades y al menos una vez al mes para las vulnerabilidades no reparadas en sistemas o aplicaciones que se ejecutan en producción.

Los ISO/encargados de seguridad designados deben notificar a la gerencia sobre cualquier vulnerabilidad no remediada que no se haya abordado en los plazos prescritos en este estándar, de modo que la parte correspondiente acepte el riesgo.

3.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 Definiciones de términos clave

Término	Definición
lite	Hace referencia a una implementación leve o superficial.

5.0 Historial de revisiones

Fecha	Descripción de Cambio
29/07/24	Revisión de documento, agregado de definición de términos clave.

6.0 Documentos relacionados

Estándar de Gestión de Parches.