Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Estándar de Registro de Seguridad

13
CAPÍTULO

Estándar de TI:
Estándar de Registro de Seguridad

1.0 Propósito y Beneficios

Los registros compilan datos para que los sistemas y las redes puedan monitorearse adecuadamente, mantener el uso para fines autorizados y el conocimiento del entorno operativo, incluida la detección de indicios de problemas de seguridad.

Este estándar define los requisitos para la generación, gestión, almacenamiento, eliminación, acceso y uso de registros de seguridad. Los registros de seguridad son generados por muchas fuentes, incluido el software de seguridad, como software antivirus, firewalls y sistemas de prevención y detección de intrusiones; sistemas operativos en servidores, estaciones de trabajo y equipos de red; bases de datos y aplicaciones.

2.0 Declaración de información

Los registros deben generarse en sistemas y redes de tecnología de la información (TI). Debido a la naturaleza de los datos contenidos en los registros de seguridad (por ejemplo, contraseñas, contenido de correo electrónico), se consideran información de identificación personal (PII) y deben protegerse con controles para una confidencialidad e integridad altas.

2.1 GENERACIÓN DE REGISTROS INICIAL

a. Todos los hosts y equipos de red deben generar registros de seguridad para todos los componentes (p. ej., sistema operativo, servicio, aplicación).
b. Todos los eventos de seguridad (**Apéndice A**) debe registrarse y debe configurarse para capturar niveles significativos de detalle para indicar actividad.

2.2 ADMINISTRACIÓN DE REGISTROS

a. Todos los hosts y equipos de red deben emitir alertas sobre fallas en el procesamiento de registros de seguridad, como errores de software/

hardware, fallas en los mecanismos de captura de registros y capacidad de almacenamiento de registros que se alcanza o excede. Todas las alertas deben ser lo más cercanas posible al tiempo real.

b. Cuando el almacenamiento de registros no rotativo alcanza el 90 % de su capacidad, se debe emitir una advertencia.

2.3 CONSOLIDACIÓN DE REGISTROS

a. La información relacionada con la seguridad de todos los sistemas, con excepción de las estaciones de trabajo individuales, debe transferirse a una infraestructura de registro consolidada. Los sistemas que ejecutan sistemas operativos de estaciones de trabajo que se utilizan para servicios compartidos, como almacenamiento de archivos compartidos o servicios web, también deben cumplir estos requisitos.
b. Todas las estaciones de trabajo deben tener la capacidad de transferir registros a una infraestructura de registros consolidada, si es necesario.
c. Los datos de registro deben transferirse en tiempo real desde hosts individuales a una infraestructura de registro consolidada. Cuando no sea posible la transferencia en tiempo real, los datos deben transferirse desde los hosts individuales a una infraestructura de registro consolidada tan rápido como lo permita la tecnología.
d. Las entidades deberán establecer procesos para el establecimiento, operación y, según corresponda, integración de sistemas de gestión de registros.

2.4 ALMACENAMIENTO Y ELIMINACIÓN DE REGISTROS

a. Dentro de la infraestructura de registros consolidada, los registros deben mantenerse y estar disponibles durante un mínimo de 90 días. Según los requisitos de la entidad, incluidas las necesidades legales o de auditoría, es posible que sea necesario conservar los registros durante un período de tiempo más largo.
b. Los datos de registro deben eliminarse de forma segura (tanto a nivel del sistema como de infraestructura) de conformidad con el Estándar de desinfección/eliminación segura.
c. Los sistemas que recopilan registros, ya sean locales o consolidados, deben mantener suficiente espacio de almacenamiento para cumplir con los requisitos mínimos tanto para los registros fácilmente disponibles como para los retenidos. La planificación del almacenamiento debe tener en cuenta las ráfagas de registros o los aumentos en los requisitos de almacenamiento que podrían razonablemente esperarse

como resultado de problemas del sistema, incluida la seguridad.

d. Se debe implementar un proceso para atender las solicitudes de preservación de registros, como un requisito legal para evitar la alteración y destrucción de registros particulares (por ejemplo, cómo se deben marcar, almacenar y proteger los registros afectados).
e. Es necesario preservar la integridad de los registros para la infraestructura de registros consolidados, como almacenar registros en medios de escritura única o generar resúmenes de mensajes para cada archivo de registro.

2.5 ACCESO Y USO DE REGISTROS

a. Los datos de registro deben analizarse inicialmente lo más cerca posible del tiempo real.
b. El acceso a los sistemas de gestión de registros debe registrarse y debe limitarse a personas con una necesidad específica de acceso a los registros. El acceso a los datos de registro debe limitarse a los conjuntos de datos específicos apropiados para las necesidades gubernamentales.
c. Deben existir procedimientos para gestionar eventos inusuales. La respuesta debe ser proporcional a la criticidad del sistema, la sensibilidad de los datos y los requisitos reglamentarios.

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 Historial de revisiones

Fecha	Descripción de Cambio	Crítico

5.0 Documentos relacionados

Publicación especial del NIST 800-92, Guía para la gestión de registros de seguridad informática

Los eventos de seguridad que deben registrarse para todos los sistemas incluyen, entre otros:

Eventos de autenticación exitosos y fallidos que incluyen, entre otros:

- inicio/cierre de sesión del sistema;
- cuenta o ID de usuario;
- cambio de contraseña;
- el tipo de evento;
- una indicación del éxito o fracaso del evento;
- la fecha y hora del evento; y
- Identificación de la fuente del evento, como ubicación, direcciones IP, ID del terminal u otros medios de identificación.

Los eventos de acceso fallido a recursos se registrarán para incluir como mínimo:

- cuenta o ID de usuario;
- el tipo de evento;
- una indicación del evento;
- la fecha y hora del evento;
- el recurso; y
- identificación de la fuente del evento, como ubicación, direcciones IP, identificación del terminal u otros medios de identificación.

Operaciones privilegiadas exitosas y no exitosas que incluyen, entre otras:

- uso de cuentas privilegiadas del sistema;
- el sistema arranca y se detiene;
- accesorios y desmontajes de hardware;
- alertas y mensajes de error de gestión de sistemas y redes; y
- eventos de seguridad: administración de cuentas/grupos y cambios de políticas.

Acceso exitoso y no exitoso a archivos de registro que incluyen, entre otros:

- cuenta o ID de usuario;
- el tipo de evento;
- una indicación del éxito o fracaso del evento;
- la fecha y hora del evento; y
- identificación de la fuente del evento, como ubicación, dirección IP, ID de terminal u otros medios de identificación.

La mayoría de los servidores web ofrecen la opción de almacenar archivos de registro en el formato de registro común o en un formato de registro extendido. El formato de registro extendido registra más información que el formato de archivo de registro común. Cuando sea técnicamente posible, los servidores web deben utilizar el formato de registro extendido. El formato de registro extendido agrega información de registro valiosa a su archivo de registro para que pueda determinar de dónde provienen los mensajes, quién envía el mensaje y agrega información al archivo de registro que sería necesaria para rastrear un ataque.

Para los sistemas identificados como críticos según una evaluación de riesgos o sistemas que aún no han sido clasificados, además de lo anterior, se registrarán eventos exitosos de acceso a recursos para incluir como mínimo:

- cuenta o ID de usuario;
- el tipo de evento;
- una indicación del evento;
- la fecha y hora del evento;
- el recurso; y
- identificación de la fuente del evento, como ubicación, direcciones IP, identificación del terminal u otros medios de identificación.