Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Auditoría y Rendición de Cuentas

21
CAPÍTULO

Política de Auditoría y Rendición de Cuentas

1.0 OBJETIVO

Garantizar que los recursos y sistemas de información de tecnología de la información (TI) se establezcan con controles de seguridad efectivos y mejoras de control que reflejen las leyes, órdenes ejecutivas, directivas, regulaciones, políticas, estándares y directrices Nacionales y Provinciales aplicables.

2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. EVENTOS DE AUDITORÍA

Los propietarios de los sistemas de información, en cooperación con las auditorías y las TI, deberán:

a. Determinar que el sistema de información es capaz de auditar los siguientes eventos: inicio de sesión (exitoso, fallido, o cambio de contraseña) con respecto a archivos, creación, eliminación y tipo de red utilizada, configuración de GPOs, instalación de softwares, intentos de accesos por softwares o hardwares. Tiempo de actividad.

    a. El sistema de información deberá registrar los siguientes, entre otros eventos definidos por la Repartición:

        i. Acceso al sistema: Inicio de sesión (exitoso, fallido, cambio de contraseña) Intentos de acceso no autorizados (por software o hardware)
        ii. Gestión de archivos: Creación, modificación y eliminación de archivos
        iii. Configuración del sistema: Cambios en la configuración de GPOs, Instalación y desinstalación de software

    b. Uso de la red:

        i. Tipo de red utilizada en cada conexión.

b. Coordinar la función de auditoría de seguridad con otras Reparticiones que requieran auditoría, y fijar objetivos comunes. Con ese objetivo, deberán definirse procesos de recopilación, análisis y respuestas, así como frecuencias de coordinación y resguardo de los resultados.
c. Proporcionar una justificación de por qué los eventos auditables se consideran adecuados para respaldar las investigaciones posteriores a los incidentes de seguridad.
d. Determinar que dentro del sistema de información se deben auditar los siguientes eventos: inicio de sesión (exitoso, fallido, o cambio de contraseña) con respecto a archivos, creación, eliminación y tipo de red utilizada, configuración de GPOs, instalación de softwares, intentos de accesos por softwares o hardwares.

2. RESEÑAS Y ACTUALIZACIONES

a. Se deberá revisar y actualizar los eventos auditados en una frecuencia definida por la Repartición

3. CONTENIDO DE LOS REGISTROS DE AUDITORÍA

a. El sistema de información generará registros de auditoría, éstos contendrán información sobre: qué tipo de evento ocurrió, cuándo ocurrió, dónde ocurrió, la fuente del evento, el resultado del evento y la identidad de cualquier individuo o sujeto asociado con el evento.

4. INFORMACIÓN ADICIONAL DE AUDITORÍA

a. El sistema de información generará registros de auditoría que contengan información adicional, quedando en la Repartición la definición de los datos de información adicional y más detallada, siendo optativo de acuerdo a los recursos humanos y tecnológicos disponibles.

5. CAPACIDAD DE ALMACENAMIENTO DE AUDITORÍA

a. El propietario de la información deberá garantizar que la capacidad de almacenamiento de registros de auditoría se asigne de acuerdo con adonde se almacena y como se buscan los registros.

6. TRANSFERENCIA A ALMACENAMIENTO ALTERNO

a. El sistema de información descargará los registros de auditoría en una frecuencia definida por la Repartición, en un sistema o medio diferente al sistema que se está auditando.

7. RESPUESTA A FALLAS EN EL PROCESAMIENTO DE AUDITORÍA

El sistema de información deberá:

a. Alertar al superior inmediato que ha solicitado la auditoria, personal o roles definidos por la Repartición en caso de una falla en el proceso de auditoría.
b. Realizar acciones adicionales. La Repartición definirá las acciones que se deben tomar al procesar la falla; y (por ejemplo, cerrar el sistema de información, sobrescribir los registros de auditoría más antiguos, dejar de generar registros de auditoría).

8. CAPACIDAD DE ALMACENAMIENTO DE AUDITORÍA

a. El sistema de información proporcionará un aviso al encargado de seguridad de la información o IT asignado, personal, roles y/o ubicaciones definidos por la Repartición dentro de una frecuencia a definir por la Repartición (se sugiere en un rango de tiempo máximo de 24 horas) cuando se alcanza el volumen de almacenamiento de registros de auditoría asignado, en un porcentaje definido por la Repartición (se sugiere no superior al 90%) de la capacidad máxima de almacenamiento de registros de auditoría del repositorio.

9. ALERTAS EN TIEMPO REAL

a. El sistema de información proporcionará una alerta al superior jerárquico, personal, roles y/o agentes definidos por la Repartición cuando ocurran los siguientes eventos de falla de auditoría:

    i. Eventos de falla de auditoría definidos por la Repartición que requieren alertas en tiempo real.

Ante la detección de eventos de falla en el proceso de auditoría, configurados previamente por la Repartición, el sistema generará alertas inmediatas. Estas alertas serán enviadas a los usuarios, roles o agentes especificados, a través de los canales de comunicación definidos (correo electrónico, SMS, notificaciones push, etc.). Los eventos de

falla a monitorear podrán incluir, entre otros, la pérdida de datos de auditoría, la incapacidad de generar nuevos registros o la detección de anomalías en los datos.

10. UMBRALES DE VOLUMEN DE TRÁFICO CONFIGURABLES

El sistema de información aplicará umbrales de volumen de tráfico de comunicaciones de red configurables que reflejen los límites de la capacidad de auditoría y rechazará o retrasará el tráfico de red por encima de esos umbrales.

Para garantizar la eficiencia de la auditoría, el sistema establecerá límites máximos de tráfico de red. Cualquier comunicación que exceda estos umbrales será bloqueada o su procesamiento será pospuesto hasta que la situación de la red lo permita.

11. APAGADO EN CASO DE FALLA

El sistema de información invocará un apagado completo del sistema; apagado parcial del sistema; modo operativo degradado con funcionalidad limitada de misión disponible en el caso de fallos de auditoría definidos por la Repartición, a menos que exista una capacidad de auditoría alternativa.

Para proteger la integridad de los datos y garantizar la seguridad del sistema, ante la detección de un fallo de auditoría, se implementará una de las siguientes acciones: apagado total, apagado parcial o transición a un modo operativo restringido. Estas medidas se activarán a menos que exista una solución de auditoría alternativa que permita continuar las operaciones.

12. REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA

El propietario del sistema de información deberá:

a. Revisar y analizar registros de auditoría del sistema de información. En una frecuencia definida por la Repartición para indicaciones de actividad inapropiada o inusual que se haya definido por la Repartición.
b. Informar los hallazgos a personal o roles definidos por la Repartición, en caso de contar con órgano auditor, debe ser a esta entidad.

13. INTEGRACIÓN DE PROCESOS

Los propietarios del sistema de información deberán garantizar que se empleen mecanismos automatizados para integrar los procesos de revisión, análisis y presentación de informes de auditoría para respaldar los procesos organizacionales de investigación y respuesta a actividades sospechosas.

14. REPOSITORIOS DE AUDITORÍA

El propietario del sistema de información deberá garantizar el análisis y la correlación de los registros de auditoría en diferentes repositorios para obtener conocimiento de la situación. (documentación, evidencia de auditorías, papeles de trabajo, informe final y presentación).

15. REDUCCIÓN DE AUDITORÍAS Y GENERACIÓN DE INFORMES

a. El sistema de información deberá proporcionar una capacidad de reducción de auditorías y generación de informes que:
    i. Admita requisitos de revisión, análisis e informes de auditoría bajo demanda y a posteriori.
    ii. No altere el contenido original ni el orden temporal de los registros de auditoría.

16. PROCESAMIENTO AUTOMÁTICO

El sistema de información deberá contar con la capacidad de procesar registros de auditoría para eventos de interés, basados en campos o datos de auditoría definidos por la Repartición dentro de los registros de auditoría. Permitiendo a la Repartición definir los criterios de filtrado según sus necesidades

17. MARCAS DE TIEMPO

El sistema de información deberá:

a. Utilizar relojes internos del sistema para generar marcas de tiempo para los registros de auditoría.
b. Registrar marcas de tiempo para registros de auditoría que se pueden asignar a la hora universal coordinada (UTC) o a la hora media de

Greenwich (GMT) y cumple granularidad definida por la Repartición de la medición del tiempo, en situaciones de cambios de horario.

18. SINCRONIZACIÓN CON FUENTE DE TIEMPO AUTORIZADA

El sistema de información deberá:

a. Comparar los relojes del sistema de información interno en una frecuencia definida por la Repartición, con el servicio oficial de horario NTP, sugiriéndose que sea una entidad nacional de servicio NTP. actualmente el Servicio Público Nacional de la Hora Oficial (Decreto del Poder Ejecutivo Nacional Nº 1792/83).
b. Sincronizar los relojes internos del sistema con servicio horario autorizado cuando la diferencia horaria sea mayor que un período de tiempo definido por la Repartición.

19. PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA

a. El sistema de información deberá proteger la información de auditoría y las herramientas de auditoría contra el acceso, modificación y eliminación no autorizados.
   El sistema implementará medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información y las herramientas de auditoría, protegiéndolas contra cualquier acceso, modificación o eliminación no autorizada.

20. ACCESO POR SUBCONJUNTO DE USUARIOS CON PRIVILEGIO DE AUTORIZACIÓN

a. La Repartición debe autorizar el acceso a la gestión de la funcionalidad de auditoría solo a un subconjunto de usuarios con privilegios de acceso definido por Repartición.

21. RETENCIÓN DE REGISTROS DE AUDITORÍA

a. Los propietarios del sistema de información conservarán registros de auditoría durante el período de tiempo definido por la Repartición consistente con la política de retención de registros para brindar soporte a investigaciones de incidentes de seguridad y cumplir con los requisitos regulatorios de Plazos Mínimos de Conservación y Guarda de

Actuaciones Administrativas actualmente RESOL-2019-94-APN-SECMA#JGM.
Los propietarios del sistema garantizarán la conservación de los registros de auditoría durante el tiempo definido por la Repartición. Esta medida tiene como objetivo respaldar futuras investigaciones de incidentes de seguridad y asegurar el cumplimiento de las normativas legales y gubernamentales en materia de retención de datos.

22. CAPACIDAD DE RECUPERACIÓN A LARGO PLAZO

a. Los propietarios del sistema de información deberán emplear medidas definidas por la Repartición para garantizar que se puedan recuperar los registros de auditoría a largo plazo generados por el sistema de información.

23. GENERACIÓN DE AUDITORÍA

El sistema de información deberá:

a. Proporcionar capacidad de generación de registros de auditoría para los eventos auditables según lo definido en los componentes del sistema de información definidos por la Repartición.
b. Permitir al personal o los roles definidos por la Repartición (usuarios definidos en el punto 20) seleccionar qué eventos deben ser auditados por componentes específicos del sistema de información.
c. Generar registros de auditoría de los eventos con el contenido definido en componentes del sistema de información definidos por la Repartición.

24. REGISTRO DE AUDITORÍA CORRELACIONADO CON EL TIEMPO

a. El sistema de información deberá cumplir con los registros de auditoría de los componentes, definidos por la Repartición, en un registro de auditoría de todo el sistema (lógica o física) que está correlacionado en el tiempo dentro de un nivel de tolerancia, definido por la Repartición, para la relación entre marcas de tiempo de registros individuales en el registro de auditoría.

   El sistema integrará los registros de auditoría de sus diversos componentes en un único repositorio, garantizando que los eventos estén ordenados cronológicamente de manera precisa y coherente, conforme a los requisitos de tolerancia temporal definidos por la Repartición.

25. FORMATOS ESTANDARIZADOS

a. Correlacionado con el formato, el sistema de información deberá producir un registro centralizado de auditoría (lógica o física) para todo el sistema compuesto de registros de auditoría en un formato estandarizado. Deberá integrar los registros de auditoría de todos sus componentes para facilitar su análisis y consulta.

26. CAMBIOS POR PERSONAS AUTORIZADAS

a. El sistema de información deberá proporcionar la capacidad a individuos o roles previamente definidos, para cambiar la auditoría que se realizará en componentes del sistema de información ya definidos, basados en criterios de eventos seleccionables dentro de umbrales de tiempo definidos por la Repartición.

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 terceros ajenos a la repartición, 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 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

5.0 DEPARTAMENTO RESPONSABLE

Oficina principal de información y propietarios de sistemas de información.

6.0 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Participantes
01/08/2024	Revisión inicial	Alejandro Castro, Pablo Zalazar
26/08/2024	Visado, y corrección de errores	Alejandro Castro, Paula D'Agostino

7.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a - Auditoría y Responsabilidad (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100