CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de gestión de logs

Versión 1.0

APROBACIONES

Elaborado por:	Revisado por:	Aprobado por:
<Nombre>	<Nombre>	<Nombre>
<Cargo>	<Cargo>	<Cargo>
<Firma>	<Firma>	<Firma>

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	Diciembre 2021	Versión Inicial

Contenido

1. Introducción

1.1 Autoridad

El Centro Nacional de Seguridad Digital fue creado el 9 de enero del 2020, mediante Decreto de Urgencia N° 007-2020, es el encargado de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. También es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital.

1.2 Propósito

El propósito de esta política es Determinar los eventos más significativos dentro de nuestros sistemas de información que han de ser registrados, y en qué modo ha de efectuarse dicho registro. Establecer mecanismos de monitorización que permitan la detección de intrusiones, errores y situaciones anómalas o potencialmente peligrosas

1.3 Alcance

Esta política se aplica a todos los empleados y afiliados de la organización.

2. Política

2.1 Todos los sistemas de producción dentro de la organización deben registrar y retener información de registro de auditoría que incluya la siguiente información:

2.1.1 Actividades realizadas en el sistema.

2.1.2 El usuario o entidad (es decir, la cuenta del sistema) que realizó la actividad, incluido el sistema desde el que se realizó la actividad.

2.1.3 El archivo, la aplicación u otro objeto en el que se realizó la actividad.

2.1.4 La hora en que ocurrió la actividad.

2.1.5 La herramienta con la que se realizó la actividad.

2.1.6 El resultado (por ejemplo, éxito o fracaso) de la actividad.

2.2 Las actividades específicas que se registrarán deben incluir, como mínimo:

2.2.1 La información (incluida la información de autenticación, como nombres de usuario o contraseñas) se crea, lee, actualiza o elimina.

2.2.2 Conexiones de red aceptadas o iniciadas.

2.2.3 Autenticación y autorización de usuarios a sistemas y redes.

2.2.4 Concesión, modificación o revocación de derechos de acceso, incluida la adición de un nuevo usuario o grupo; cambiar privilegios de usuario, permisos de archivos, permisos de objetos de base de datos, reglas de firewall y contraseñas.

2.2.5 Cambios en la configuración del sistema, la red o los servicios, incluida la instalación de software, parches, actualizaciones u otros cambios de software instalados.

2.2.6 Inicio, apagado o reinicio de una aplicación.

2.2.7 El proceso de la aplicación aborta, falla o finaliza anormalmente, especialmente debido al agotamiento de los recursos o al alcanzar un límite o umbral de recursos (como CPU, memoria, conexiones de red, ancho de banda de red, espacio en disco u otros recursos), la falla de servicios de red como DHCP o DNS, o falla de hardware.

2.2.8 Detección de actividad sospechosa y / o maliciosa de un sistema de seguridad, como un sistema de detección o prevención de intrusiones (IDS / IPS), un sistema antivirus o un sistema anti-spyware.

2.3 A menos que sea técnicamente impráctico o inviable, todos los registros deben agregarse en un sistema central para que las actividades en diferentes sistemas puedan correlacionarse, analizarse y rastrearse en busca de similitudes, tendencias y efectos en cascada. Los sistemas de agregación de registros deben tener ingesta de registros automática y oportuna, etiquetado y alerta de eventos y anomalías, y capacidad de revisión manual.

2.4 Los registros deben revisarse manualmente de forma regular:

2.4.1 Las actividades de los usuarios, administradores y operadores del sistema deben ser revisadas al menos una vez al mes.

2.4.2 Los registros relacionados con la PII deben revisarse al menos una vez al mes para identificar comportamientos inusuales.

2.5 Cuando se utiliza un entorno de nube subcontratado, los registros deben mantenerse en el acceso y uso del entorno de nube, asignación y utilización de recursos y cambios en la PII. Se deben mantener registros para todos los administradores y operadores que realizan actividades en entornos de nube.

2.6 Todos los sistemas de información dentro de la organización deben sincronizar sus relojes implementando Network Protocolo de tiempo (NTP) o una capacidad similar. Todos los sistemas de información deben sincronizarse con el mismo sistema primario fuente de tiempo.

3. Cumplimiento de políticas

3.1.1 Medición de cumplimiento

Se verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la póliza.

3.1.2 Excepciones

Cualquier excepción a la política debe ser aprobada con anticipación.

3.1.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias.