8. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Como mecanismos de monitoreo, se utilizan las auditorías que registran los accesos a sistemas y datos de todos los usuarios con el objetivo de detector posibles riesgos de seguridad.

Los registros de auditoría deberán incluir:

1. Identificación del usuario.
2. Fecha de inicio y fin.
3. Registros de intentos exitosos y fallidos de acceso a los sistemas.
4. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere, la periodicidad de las revisiones se realizará de manera semestral.

La **USTPDN,** junto a los responsables de los sistemas de información, definirán un cronograma de depuración de registros.

Monitoreo del Uso de los Sistemas

Se realiza un monitoreo sobre el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente. La periodicidad de las revisiones se realizará de manera semestral.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, así como las actividades que pueden ser objeto de control y monitoreo.

Entre los eventos que deben tenerse en cuenta, se enumeran las siguientes:

Viaducto Presidente Miguel Alemán Valdés 105, Colonia Escandón sección 1, Alcaldía Miguel Hidalgo C.P. 11800, Ciudad de México
unidadtransparencia@sesna.gob.mx
55 5131 5645

1. Acceso no autorizado, incluyendo detalles como:

    a) Identificación del usuario.
    b) Fecha y hora de eventos clave.
    c) Tipos de eventos.
    d) Archivos a los que se accede.

2. Todas las operaciones con privilegio, como:

    a) Uso de cuenta de administrador.
    b) Inicio y cierre del sistema.
    c) Conexión y desconexión de dispositivos de ingreso y salida de información o que permitan copiar datos.
    d) Cambio de fecha/hora.
    e) Cambios en la configuración de la seguridad.
    f) Alta de servicios.

3. Intentos de acceso no autorizado, como:

    a) Intentos fallidos.
    b) Violaciones de accesos y notificaciones para "Gateways" y "Firewalls".
    c) Alertas de sistemas de detección de intrusiones.

4. Alertas o fallas de sistema como:

    a) Alertas o mensajes de consola.
    b) Excepciones del sistema de registro.
    c) Alarmas del sistema de administración de redes.

Registro y Revisión de Eventos

La **USTPDN** registra y revisa los eventos de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.

La periodicidad de dichas revisiones es de manera semestral utilizando herramientas específicas para auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

1. La desactivación de la herramienta de registro.
2. La alteración de mensajes registrados.
3. La edición o supresión de archivos de registro.
4. La saturación de un medio de soporte de archivos de registro.
5. La falla en los registros de los eventos.
6. La sobre escritura de los registros.

Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, los equipos que realicen estos registros deberán tener una correcta configuración y ajuste de sus relojes, donde se verificarán los mismos contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.