intiza

Norma de Monitoreos de Eventos y Análisis de Logs

Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO **Consultoría Externa**	 **Carla Leiva - CISO**	 **Francisco Canale - Director**

NORMA DE MONITOREO DE EVENTOS Y ANÁLISIS DE LOGS	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 24/02/2025
Código: NO-SI-12 Monitoreo de Eventos y Análisis de Logs	Versión: 2.1

Contenido

1. Objetivo

Establecer los lineamientos generales para realizar, de forma eficiente y efectiva, el monitoreo de los accesos a recursos y eventos críticos de la organización con el fin de identificar y mitigar posibles incidentes de seguridad o anomalías en los sistemas tecnológicos de INTIZA.

A su vez, se establecen los lineamientos generales para registrar eventos y generar trazabilidad sobre las operaciones que se realizan en los sistemas de información y sistemas operativos de la organización, con el objetivo de monitorear todos aquellos servicios informáticos de INTIZA.

2. Alcance

La presente norma aborda actividades de Gestión de Logs del Sistema de Seguridad de la Información en tópicos de:

- Identificación de registros de eventos de actividad.
- Protección de la información de registros de eventos.
- Registros del administrador y el operador.
- Controles de auditoría de sistemas de información.
- Protección de los registros institucionales.

3. Responsabilidades

Seguridad de la Información es responsable de definir las pistas de auditoría que deben ser registradas por los aplicativos y sistemas de la compañía, considerando:

- La criticidad de la información involucrada;
- La posibilidad de detectar el responsable de la ocurrencia de un incidente que haya comprometido la seguridad de la información;

- La información necesaria para poder detectar un posible incidente en forma oportuna;
- El rendimiento de las prestaciones informáticas, de manera de no comprometerlas significativamente dado que se estaría afectando a la disponibilidad de la información;
- La activación de las pistas de auditorías definidas sobre los aplicativos y sistemas de la compañía;
- La revisión semestral de los mismos;
- La apertura de un incidente de seguridad en caso de detectar situaciones sospechosas;

4. Desarrollo

4.1. Autenticación

Seguridad de la Información deberá acceder a los registros de eventos de seguridad en la medida que lo permitan los sistemas.

4.2. Autorización

- El usuario autorizado para llevar a cabo los procesos de generación de copias de respaldo solo deberá tener los accesos que su función requiere. No podrá acceder al contenido de los registros de eventos de seguridad.
- Las acciones de mantenimiento sobre los registros de eventos de seguridad deberán estar restringidas a los administradores de la plataforma.
- Las solicitudes especiales de accesos a los registros de eventos de seguridad deberán ser solicitados previa aprobación.
- Los archivos de logs deberán ser protegidos de accesos no autorizados cualquiera sea su medio de almacenamiento. Los eventos deberán ser almacenados históricamente en línea o medios de resguardo que aseguren su recuperación en caso de ser necesario

consultar un dato anterior. Los medios de resguardo no deberán permitir la modificación de los archivos almacenados.

4.2.1. Se deberán registrar los siguientes eventos:

Usuarios	Registro de Eventos
Usuario Administrador de Plataforma Tecnológica	Todas sus actividades en el sistema.
Seguridad / Auditoría	Todas sus actividades en el sistema.
Cuentas especiales del software/servicios	Todas sus actividades en el sistema.
Cuentas de emergencia / Administrativa	Todas sus actividades de soporte en el sistema al ingresar al ambiente de producción con: ● Permisos de modificación de datos. ● Permisos de consulta sobre los datos.
Otros usuarios	Solamente los eventos generales que se hayan definido para todos los usuarios.

Se deberán registrar los siguientes sucesos generales para todas las cuentas de usuario:

- Registro de ingreso de usuarios.
    - Inicio de sesiones exitosas, dependiendo de lo definido en el estándar de la plataforma correspondiente, con la excepción de los accesos exitosos a la red debido al alto volumen de transacciones.
    - Intentos fallidos de inicio de sesión.

- Encendido y apagado de servidores y equipos de comunicación.
- Desconexión forzada de usuarios.
- Alta, Baja o Modificación de usuarios y grupos.
- Cambios en la configuración de los parámetros de seguridad.
- Instalación de software de aplicación.
- Eliminación manual de eventos.
- Cambios en las configuraciones de permisos y de privilegios de seguridad.

4.2.2. Eventos Especiales

Se deberán registrar los siguientes eventos “especiales”:

- Todos los accesos autorizados y todos los intentos de acceso no autorizados a la información crítica de INTIZA de acuerdo con lo definido por el propietario correspondiente.
- Todos los eventos de un usuario cuando sean específicamente solicitados.

4.3. Segregación de Funciones

El propietario correspondiente, Seguridad de la Información y los administradores de las plataformas deberán definir y podrán solicitar el registro / logs de un determinado evento, en la medida que se correspondan con la información o personal a su cargo.

4.4. Auditoría y Control

Contar con los registros/logs de auditoría, permite que se pueda realizar investigaciones especiales, cumplir con regulaciones, verificar eventos de seguridad entre otros.

Se deben definir actividades que permitan contar con estos rastros de auditoría y controlar su almacenamiento.

Seguridad de la información deberá realizar la revisión de los logs generados en los sistemas tecnológicos de la organización con el fin de poder monitorear las actividades definidas en sus

correspondientes procedimientos. Seguridad de la Información conservará un registro de las revisiones realizadas.

4.4.1. Sincronización de relojes

Los relojes de todos los sistemas de procesamiento deben estar sincronizados para asegurar que la registración de los eventos sea precisa y comparable.

Tecnología deberá asegurar la sincronización de los relojes tanto en todos los equipos que conforman la infraestructura como los dispositivos móviles que se conectan a los activos de la compañía.

4.4.2. Análisis de Logs

Todos los sistemas de información, aplicativos, sistemas operacionales, bases de datos, dispositivos de comunicación, dispositivos de seguridad y servidores, deben contar con los logs o registros de auditoría que registren las actividades de los usuarios, las excepciones, las fallas y eventos de seguridad.

Es responsabilidad de los propietarios y/o Tecnología, estar pendientes de la activación de los logs de auditoría. El encargado del aplicativo debe mantener un inventario de los registros de auditoría existentes por aplicación y su ubicación.

4.4.3. Verificación de Eventos

Se debe elaborar, conservar y revisar periódicamente los registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información.

Es responsabilidad de los propietarios de la información, solicitar y conocer qué eventos se han producido sobre los sistemas de tratamiento de su información.

Es responsabilidad de Tecnología proveer la información de eventos solicitada por los usuarios.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Seguridad de la Información	PO-SI-01

5.2. Definiciones

Término	Descripción
Seguridad de la Información	Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
Evento	Los eventos representan acciones que se pueden auditar en un sistema. Cada evento de auditoría está conectado a una llamada del sistema o comando de usuario, y está asignado a una o más clases de auditoría.
Log	Se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema

Monitoreo y Control	Proceso sistemático de recolectar, analizar y utilizar información para hacer seguimiento al progreso de un programa en pos de la consecución de sus objetivos, y para guiar las decisiones de gestión.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	01/11/2021	Creación de la norma de Monitoreos de Eventos y Análisis de Logs.
1.0	06/06/2022	Aprobado por Comité de Dirección: MI-DI-04- Minuta de Comité de Dirección N° 4
2.0	22/09/2022	Se incluyó la mención de la sincronización de los relojes.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06 Minuta de Comité de Dirección N° 6
2.1	08/01/2025	Se revisó contenido del documento confirmando su vigencia. Se ajustó el formato del encabezado y pie de página.
2.1	24/02/2025	Aprobado por Comité de Dirección.