Política Específica de Monitoreo y Auditoría de Sistemas

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

Detectar las actividades de procesamiento de información no autorizada, monitorear los sistemas y grabar los eventos de la seguridad de información. DACTA debe cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades.

Este documento se aplica a todo el alcance del Sistema Integrado de Gestión (SIG); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SIG.

Los usuarios de este documento son todos los colaboradores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- Se actualiza el requisito normativo según nueva versión ISO 27001:2022. Clausulas 8.33, 8.34, 8.9, 8.16, 8.30.

3. POLÍTICA ESPECÍFICA

El monitoreo del sistema debe ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad de un acceso a un modelo de política. Todo trabajador de DACTA o tercero para el desempeño de sus funciones, se compromete a lo siguiente:

- El registro de los operadores y el registro de la avería debe ser usado para asegurar que los problemas del sistema de información sean identificados.

3.1. MONITOREO DEL USO DEL SISTEMA

En el monitoreo de control de los sistemas se deben incluir:

- Acceso autorizado, incluyendo detalles como:
  - La identificación del usuario.
  - La fecha y hora de los eventos claves.
  - El tipo de evento.
  - Los archivos ingresados.
  - El programa y recurso utilizado.

- Todas las operaciones privilegiadas como:
  - Uso de cuentas privilegiadas como supervisores o administradores.
  - Puesta en marcha y parada del sistema.
  - Conexión o desconexión de un recurso de entrada o salida.

- Intentos de acceso no autorizados como:
  - Intentos fallidos.
  - Acciones con fallas o rechazadas que involucran datos y otros recursos.
  - Violaciones a las políticas de acceso y las notificaciones de los firewalls y entrada de red.
  - Las alertas de los sistemas de dirección de intrusos del propietario.

- Alertas o fallas del sistema como:
  - Alertas o mensajes de consolas.
  - Excepciones de registro en el sistema.
  - Alarmas de la gerencia de red.
  - Alarmas levantadas por los sistemas de control de accesos.

- Cambios o intentos de cambio a la configuración y controles de los sistemas de seguridad. El número de veces que deberán ser revisadas las actividades de monitoreo debe depender de los riesgos implicados. Los factores de riesgo que deben ser considerados incluyen:
  - Criticidad de los procesos de aplicación.
  - Valor, sensibilidad y criticidad de la información implicada.
  - Experiencia pasada de infiltraciones del sistema, mal uso y frecuencia de las vulnerabilidades explotadas.
  - Extensión de la interconexión del sistema (particularmente redes públicas).
  - Registro de la instalación que está siendo desactivada.

3.2. PROTECCIÓN DE LA INFORMACION DE REGISTRO

Los controles deben proteger contra cambios no autorizados y problemas operacionales con la instalación de registro incluyendo:

- Alteraciones a los tipos de mensaje que son grabados.
- Archivos de registro editados o eliminados.
- La capacidad de almacenamiento del medio del archivo de registro que ha sido excedido, resultando en la falla de los eventos almacenados o la sobre escritura de eventos pasados.

3.3. REGISTRO DE AUDITORÍA

Los registros de auditoría deben incluir lo siguiente:

- Identificación de usuarios.
- Fecha y hora de conexión y desconexión.
- Identidad del terminal o locación si es posible.
- Registro de éxito o fracaso de los intentos de acceso al sistema.
- Registro de éxito o fracaso de datos y de otros intentos de accesos a recursos.
- Cambios de la configuración del sistema.
- Uso de privilegios.
- Uso de las instalaciones y aplicaciones del sistema.
- Archivos accesados y el tipo de acceso.
- Direcciones de red y protocolos.
- Las alarmas realizadas por el sistema de control de accesos.
- Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusos.

3.4. REGISTRO DE ADMINISTRADORES Y OPERADORES

Los registros de los administradores y usuarios del sistema deben ser revisados en una base regular (recomendable mensualmente). Los registros deben incluir lo siguiente:

- El tiempo en que ocurrió el evento
- Información acerca del evento o fallas
- Contabiliza que administrador u operador fue implicado
- Que procesos fueron implicados

3.5. REGISTRO DE AVERÍA

Las averías reportadas por usuarios o por programas del sistema relacionados con problemas en el procesamiento o comunicación de información, deben ser registradas. Deben existir reglas para maniobrar las averías reportadas incluyendo:

- Revisión de los registros de averías para asegurar que las fallas han sido resuelta satisfactoriamente.
- Revisión de las medias correctivas para asegurar que los controles no han sido comprometido y que la acción realizada es totalmente autorizada.
- Se debe asegurar que el registro de error es activado, si es que se encuentra disponible en el sistema.

3.6. CONSIDERACIONES DE AUDITORÍA

Los requerimientos y actividades de auditoría que involucran la verificación de los sistemas de producción deben ser cuidadosamente planeados y acordados para evitar disrupciones en los procesos de DACTA.

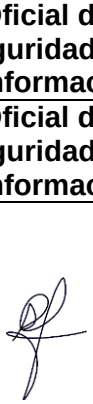
- Los alcances de las pruebas de auditoría técnica deben ser acordadas y controladas.
- Las pruebas de auditoría deben ser limitadas con accesos de solo lectura para el software y los datos.
- Otros accesos que no sean de solo lectura, deben ser sólo permitidos a través de copias aisladas en archivos de sistemas, los cuales deben ser borrados cuando la auditoría ha terminado o darle protección apropiada si existe alguna obligación a mantener tales archivos bajo los requerimientos de la documentación de auditoría.
- Los requerimientos para el procesamiento especial o adicional deben ser identificados y acordados.
- Las pruebas de auditoría que podrían afectar la disponibilidad de los sistemas deben hacerse fuera de las horas de labores de DACTA.
- Todos los accesos deben ser monitoreados y registrados para generar un rastro de referencia.

En caso de no cumplir con la presente Política Específica de Monitoreo, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Oficial de Seguridad de la Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, la autoridad competente de DACTA, tomará las medidas disciplinarias necesarias, las cuales están sujetas al RIT de DACTA.

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
N/A	N/A	N/A	N/A

5. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	22/02/2023	Actualización	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	22/02/2024	Revisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
Firmas de la versión vigente			 S. Rafaile	 S. Rafaile  A. Morales	 G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022.