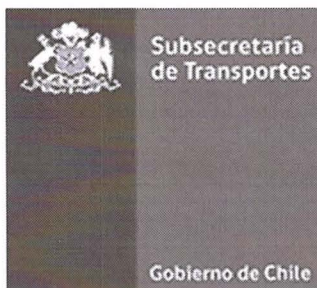


INSTRUCTIVO DE CAPTURA - PROTECCIÓN Y AUDITORÍAS DE LOGS

INS-SSI-12.3 v1.0



SUBSECRETARÍA DE TRANSPORTES

Diciembre 2017


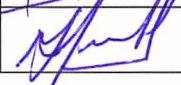
	Nombre	Cargo	Firma	Fecha
Aprobado por	Jaime Gonzalez	Encargado Unidad de TIC		19/12/2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		19/12/2017



TABLA DE CONTENIDO

1. OBJETIVOS DEL INSTRUCTIVO.....	3
2. CONTEXTO O ÁMBITO DE APLICACIÓN.....	3
3. ROLES Y RESPONSABILIDADES.....	4
4. MATERIAS QUE ABORDA.....	4
5. MODO DE OPERACIÓN.....	5
5.1 LOGS Y REGISTRO DE EVENTOS DE ACTIVIDAD.....	5
5.2 PROTECCIÓN DE LOS REGISTRO DE EVENTOS DE ACTIVIDAD.....	5
5.3 REGISTROS DEL OPERADOR Y ADMINISTRADOR.....	6
5.4 CONTROLES DE AUDITORÍA DE INTERNA.....	6
5.5 PROTECCIÓN DE LOS REGISTROS INSTITUCIONALES.....	6
6. REGISTROS DE OPERACIÓN Y/O LOGS.....	6
7. EXCEPCIONES AL CUMPLIMIENTO DE ESTE INSTRUCTIVO.....	7
8. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS.....	7
9. HISTORIAL Y CONTROL DE VERSIONES.....	7

Nota de equidad de género:

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.



INSTRUCTIVO DE CAPTURA - PROTECCIÓN Y AUDITORÍAS DE LOGS

Versión: 1.0
Página: 3 de 7
Fecha: Diciembre 2017

1. OBJETIVOS DEL INSTRUCTIVO

Los objetivos generales del instructivo de captura - protección y auditorías de LOGs, son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Cumplir con la Política de Seguridad en la Operación y Administración de Sistemas.
- Proteger los registros de eventos o LOGs de las plataformas tecnológicas de la Subsecretaría, con el fin de facilitar eventos de correlación y auditorías de seguridad.

2. CONTEXTO O ÁMBITO DE APLICACIÓN

El Instructivo de captura - protección y auditorías de LOGs se aplica a toda plataforma tecnológica de la Subsecretaría de Transportes y sus Programas dependientes; así como a su personal sean de planta, contrata o a honorarios, y externos que presten servicios a ella, e involucra a las visitas y a todos sus instalaciones, recursos y activos de información.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de este instructivo corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Dominios y Controles de Seguridad relacionados	
A.12	Dominio: Seguridad en las Operaciones
A.12.04.01	Registro de evento
A.12.04.02	Protección de la información de registros
A.12.04.03	Registros del administrador y el operador
A.12.07.01	Controles de auditoría de sistemas de información
A.18.01.03	Protección de los registros

En cuanto al ámbito institucional de aplicación de este instructivo, corresponde a los siguientes objetivos y productos estratégicos del formulario A1 relacionados con procesos críticos que corresponden al alcance declarado del Sistema de Seguridad de la Información de la SUBSECRETARÍA DE TRANSPORTE:

Objetivo, Producto estratégico y Proceso crítico en ámbito de aplicación		
Objetivo Estratégico SUBSECRETARÍA DE TRANSPORTE	Producto Estratégico A1	Proceso crítico protegido
(1) Disminuir fallecidos por accidentes de tránsito. (2) Desarrollar planes y estudios que permiten definir políticas y normativas en los temas relevantes a transporte de carga.	(1) Regulación que rige el transporte	Políticas y normas que rigen el transporte.
(3) Mejorar las condiciones para la operación e integración del Transporte Público a través de infraestructura prioritaria, con foco inicial en la mejora de los tiempos de viaje. (4) Diseñar sistemas de transportes que respondan a las principales necesidades multimodales de las personas, priorizando los modos más eficientes y sustentables y mejorando la convivencia de usuarios de los distintos modos.	(5) Subsidios e iniciativas de inversión para la operación y fortalecimiento de los Servicios de Transporte Público.	Transporte Público Regional.



INSTRUCTIVO DE CAPTURA - PROTECCIÓN Y AUDITORÍAS DE LOGS

Versión: 1.0
Página: 4 de 7
Fecha: Diciembre 2017

- | | | |
|--|--|--|
| (6) Velar por la accesibilidad, calidad, seguridad e impacto ambiental que entregan los servicios de transporte terrestre y otros modos. | | |
|--|--|--|

3. ROLES Y RESPONSABILIDADES

- **El Encargado de Seguridad de la Información (ESI)**

- Es responsable de la elaboración del presente instructivo, de su actualización y velar por el cumplimiento de sus disposiciones.

- **Encargado de la Unidad de TIC**

- Implementar las recomendaciones técnicas de este instructivo.

- **Administrador de plataforma y SYSLOGs**

- Esta función de seguridad de la información, se debe asociar a diversos roles del área de Infraestructura de TIC, como: Ingeniero de Sistemas, Operadores TIC, DBA y Administradores de Redes y Comunicaciones.
- Se asocia a un responsable de la revisión interna de Seguridad Informática (o ciberseguridad) para este caso, encargado de efectuar los análisis de los registros de log de los sistemas.
- Posee acceso a los logs y sistemas de auditoría y monitoreo.

- **Encargado de Infraestructura TIC**

- Responsable de implementar las herramientas de captura y gestión de LOGs.

4. MATERIAS QUE ABORDA

El presente instructivo 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.



5. MODO DE OPERACIÓN

5.1 LOGs y Registro de eventos de actividad

- Se deben identificar, producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información de las plataformas tecnológicas de la institución.
- La gestión de dichos LOGs o registro de eventos se orientará al análisis de funcionamiento, errores y corrección, tanto de sistemas/aplicativos como de las plataformas que lo soportan.
- Se recomienda el uso de un SYSLOG Server como plataforma LOGGER de repositorio y concentrador de LOGs, para resguardo y consulta de los tipos de LOGs que se consideren necesarios para la supervisión de Seguridad de las plataformas tecnológicas de la institución.
- Se integran a este LOGGER, previa definición del caso de uso como situación de riesgo y de un análisis de factibilidad, los eventos de las plataformas centrales TIC y de Seguridad de la Subsecretaría, tales como Equipos de comunicaciones; File Servers; IPS; Consola de gestión malware; motor de BDs; Gateway Mail AntiSpam; DNS; Firewalls, Servidores Exchange, etc.
- Previo la integración de una plataforma tecnológica oficial para la Red de Institución, se debe evaluar su impacto a nivel de consumo de ancho banda y factibilidad de captura de sus LOGs.
- El sensor o "recolector" principalmente SYSLOG; se activa en la misma plataforma que genera el evento.
- Se deben configurar los registros de eventos para incluir, cuando corresponda:
 - Sujetos participantes
 - IDs; cuentas de usuarios; direcciones IPs; nombres de equipos o sistemas involucrados en el evento;
 - Ubicación física (dependencia) o lógica (Segmento IP);
 - Actividades o acciones relevantes efectuadas;
 - Fechas, horas de los eventos clave, es decir el inicio y la finalización de la sesión o proceso;
 - Los registros de los accesos al sistema o recurso TI críticos, exitosos y rechazados;
 - Los cambios a la configuración del sistema;
 - El uso de cuentas con altos privilegios;
 - El uso de utilitarios que requieran altos privilegios y aplicaciones del sistema.
 - Las alarmas que se activaron con el sistema de control de acceso;
 - La activación y la desactivación de los sistemas de protección, como los sistemas de antivirus y los sistemas de detección de intrusos;
 - Los registros de las transacciones críticas ejecutadas por los usuarios en las aplicaciones.
 - Se mantendrá una matriz que relacione nivel de detalle del LOG según se encuentre en situación Normal o de excepción.

5.2 Protección de los Registro de eventos de actividad

- Las tecnologías de gestión de los registros y la información de dichos LOGs o registros de eventos de seguridad deben estar protegidos contra una posible adulteración y acceso no autorizado. Por tanto, los controles de protección de los registros deben apuntar a evitar cambios no autorizados y adulteración de su gestión.
- Los servidores y equipos deben contar con el espacio suficiente para almacenar los Logs o bien se debe incorporar LOGGER Server con el suficiente espacio de almacenamiento.



INSTRUCTIVO DE CAPTURA - PROTECCIÓN Y AUDITORÍAS DE LOGS

Versión: 1.0
Página: 6 de 7
Fecha: Diciembre 2017

- Se debe efectuar gestión de capacidad para dicho almacenamiento manteniendo capacidades de servicio para un año -al menos- y evaluar anualmente su política de retención.
- Para todas las plataformas de servidores, los LOGS se respaldan junto con la data de la plataforma.
- Los controles de protección de los registros deben considerar al menos:
 - Alteraciones a los tipos de mensajes que se registran;
 - Archivos de registro editados o eliminados;
 - Capacidad de almacenamiento.
- Los siguientes son modos de protección de los registros (LOGs):
 - Identificación del registro
 - Logs
 - Almacenamiento
 - Servidor o dispositivo específico
 - Control de acceso
 - Login/password, restringido a Auditor / Gestor de Seguridad TI / Operadores Autorizados
 - Recuperación
 - A través de cuentas con acceso de lectura a logs de auditoria
 - Tiempo retención y disposición
 - 1 año en servidor depósito de documentos.

5.3 Registros del Operador y Administrador

- Se deben activar los registrar las actividades o LOGs del operador y del administrador de los sistemas y plataformas tecnológicas de la institución.
- Estos registros se deben proteger adecuadamente de su integridad y disponibilidad, además de fijar un proceso periódico de revisión.

5.4 Controles de auditoría de Interna

- Se establecerán requisitos y alcances de auditoría de seguridad para los sistemas y datos más críticos de la institución.
- Dichas revisiones de auditoría deben limitarse al acceso de sólo lectura y no afectar la disponibilidad de las plataformas o sistemas revisados en horarios de servicio.
- Todo el acceso debe ser autorizado y registrado para producir un rastro de referencia.

5.5 Protección de los registros institucionales.

- Deben establecerse directrices institucionales para la retención, almacenamiento, manejo y eliminación de los registros y la información vital de la institución.
- Debe mantenerse un inventario de las fuentes de información clave.
- Los registros de seguridad de las plataformas claves son parte de los registros institucionales.

6. REGISTROS DE OPERACIÓN Y/O LOGS

Son registros de operación de este Instructivo:

- Ejemplo de SYSLOGs de un sistema monitoreado.
- Pantalla de configuración de la Consola Logger.



INSTRUCTIVO DE CAPTURA - PROTECCIÓN Y AUDITORÍAS DE LOGS

Versión: 1.0
Página: 7 de 7
Fecha: Diciembre 2017

7. EXCEPCIONES AL CUMPLIMIENTO DE ESTE INSTRUCTIVO

Frente a casos de especiales, el Jefe de la Unidad de Informática de la Subsecretaría evaluará la situación y podrá establecer condiciones puntuales de excepción en el cumplimiento del presente instructivo, siempre que no infrinja las políticas internas existentes. Toda excepción debe ser documentada y monitoreada, generando un proceso de revisión del instructivo, para determinar si se deben efectuar actualizaciones en las condiciones de operación particular.

8. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

El completo glosario de términos y siglas utilizados en los documentos del Sistema de Gestión de Seguridad de la Información de la Subsecretaría de Transporte, se encuentran integrados en el Estándar de Seguridad "Glosario Términos de SSI-MTT", ubicado en la sección Políticas de Seguridad de la Información de la intranet institucional.

Las siguientes son definiciones necesarias para la comprensión de la presente política.

- **Sistemas o aplicaciones:**
 - Corresponde al software que registra, procesa o intercambia datos y que sustenta los procesos de negocio.
- **Plataforma:**
 - Corresponde al hardware y software base (Sistemas operativos, servicios, etc.) requeridos para que las aplicaciones y redes de comunicaciones del negocio funcionen.
- **Log:**
 - Archivos que contienen el registro de las operaciones y de eventos de seguridad, que son almacenados para su posterior análisis. Los datos contenidos en el log permiten rehacer la traza del proceso u operación que está siendo registrada.
- **Sistema de monitoreo:**
 - Sistema que permite medir y visualizar en línea variables críticas de las plataformas de comunicaciones y de procesamiento de datos.
- **Ofuscación**
 - Se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en un documento o el código fuente de un programa informático, con el fin de que no sea fácil de entender o evitar divulgación de información sensible.

9. HISTORIAL Y CONTROL DE VERSIONES

Nº de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
1	12/2017	Elaboración inicial	Todas	RM