DECRETO ALCALDICIO N°977

APRUEBA POLÍTICA DE AUDITORÍA DE LOGS

DALCAHUE, 29 de Marzo de 2023.

VISTOS:

1.- Las facultades y atribuciones que me entrega la Ley Orgánica Constitucional de Municipalidades N°18.695, en especial, la señaladas en sus artículos 12° inciso 4°, 56°, y 63º letra d);

2.- El artículo 37 f) del Decreto 83/2005 del Ministerio Secretaría General de la Presidencia; las normas del capítulo 10.10.5 Registro de fallas de la norma técnica NCh 27002 de 2009

3.- El Decreto Alcaldicio N°548 de fecha 07 de Marzo de 2022 que declara Alcalde de Dalcahue en relación a la sentencia firme y ejecutoriada del Tribunal Calificador de Elecciones, Rol N°1459-2021 y

CONSIDERANDO:

1.- La necesidad de corregir lo observado en el Informe Final de Auditoría N°1038 del 14 de Abril de 2022 respecto a las tecnologías de la información en la Municipalidad de Dalcahue, en este caso, respecto de implementar un registro de fallas, donde se analicen y tomen las acciones apropiadas,

DECRETO:

Apruébese la siguiente **Política de Auditoría de Logs**:

	POLITICA DE AUDITORIA DE LOGS		
VERSIÓN	FECHA APROBACIÓN	MOTIVO DE LA REVISIÓN	AUTOR (ES)
1.0	Marzo 2023	- Creación de la Política	Alexis Bórquez Bahamonde / Encargado de la Seguridad de la Información de la I. Municipalidad de Dalcahue

1. PROPOSITO. Definir el procedimiento de auditoría de LOGs de la Municipalidad de Dalcahue.

2. -ALCANCE. El Instructivo de captura - protección y auditorías de LOGs se aplica a toda plataforma tecnológica de la Municipalidad de Dalcahue y sus Programas dependientes; así como a su personal sean de planta, contrata o a honorarios, practicantes 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 a Controles de Seguridad para los sistemas detallados a continuación

- Microsoft SQL Server
- Servidor de Respaldo de Archivos (NAS)

3.- ROLES Y RESPONSABLES

- **- Encargado de Oficina de Tecnologías, Información y**

Comunicación (OTIC). Es responsable de Implementar las recomendaciones técnicas de este instructivo.

4.- POLITICA

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 como de las plataformas que lo soportan.
- Se deben configurar los registros de eventos para incluir, cuando sea posible y corresponda:
- 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 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.

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. 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.
- 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.

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.

REVISION, VALIDACIÓN Y DIFUSIÓN

La Política se revisará al menos una vez al año, para efectos de mantenerla actualizada. Asimismo, efectuará toda modificación que sea necesaria en función de posibles cambios que puedan afectar su

definición, como, por ejemplo, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios legislativos, entre otros.

ANÓTESE, REGÍSTRESE, PUBLÍQUESE EN TRANSPARENCIA ACTIVA Y ARCHÍVESE.

MANUEL ANÍBAL ÁLVAREZ BARRÍA
Secretario Municipal (s)
Comuna de Dalcahue

ALEX WALDEMAR GÓMEZ AGUILAR
ALCALDE
Comuna de Dalcahue

Distribución:
- A todas las Direcciones y Unidades Municipales.
- Transparencia

AWGA/MAAB

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.