Estudio No. 05-2023
Generación y revisión de bitácoras

I. Alcance

El presente estudio busca verificar si la Administración ha establecido actividades que permitan una apropiada gestión del registro de eventos dentro de la infraestructura tecnológica, siendo almacenados, protegidos y analizadas con el fin de identificar desviaciones y/o excepciones que ameriten atención.

II. Objetivos

1. Comprender el proceso de registro de eventos en la plataforma tecnológica, verificando su alcance, la información que es registrada y el uso que se le da a ésta.

2. Constatar cómo es resguardada y protegida la información contenida en las bitácoras, así como el periodo de retención de estas.

III. Resultados Obtenidos

De conformidad con los objetivos propuestos para esta revisión:

- ✓ Se determinó que el proceso de generación y resguardo de bitácoras se encuentra implementado con diversos alcances (a nivel de dominio, base de datos y sistemas institucionales), procurando cubrir las actividades que son realizadas por los usuarios.

  Se observó, además, que la información registrada por cada tipo de bitácora es variable, pero permite mantener una trazabilidad de los eventos y generar correlaciones, siendo el Área de Seguridad de la Información la encargada de verificar de manera periódica los registros de estas pistas de auditoría.

  Si bien, se constató la existencia de normativa interna asociada, las directrices sobre el tema no son abundantes y se encuentran dispersas entre diferentes documentos normativos, por lo que existen oportunidades de mejora al respecto.

- ✓ Se observó que el resguardo de las bitácoras, en aras de procurar la disponibilidad de estas, ocurre mediante el proceso de gestión de respaldos institucionales, donde se realizan back up periódicos de los registros a nivel de base de datos y sistemas institucionales.

  Cabe señalar que los respaldos también incluyen los registros de herramientas como el Change Auditor, la cual almacena la actividad de los usuarios a nivel del dominio y acceso a recursos como carpetas compartidas.

Esta revisión fue aprobada en la Sesión Ordinaria No. 038-2024 del 02/04/2024.