AG-F-19-2021

Gestión de la Clasificación de la Información

2021

Informe de Auditoría

Generalidades del alcance

Cumplimiento normas de auditoría

El estudio de Auditoría se realiza de conformidad con:

- El Marco Internacional para la Práctica Profesional de la Auditoria Interna.
- Las Normas Generales de Auditoría para el Sector Público.
- Las Normas para el Ejercicio de la Auditoría Interna en el Sector Público.
- El Manual de Operaciones de las AI-CFBNCR.

Criterios

- MG05-MCGGR02 Metodología de identificación y clasificación de la información
- COBIT 5: APO01 Gestionar el Marco de Gestión de TI
- COBIT 19 AP014 Gestionar los datos
- OEA: Organización de Estados Americanos, Recomendaciones para establecer un sistema de clasificación de la información

Procesos

El estudio abarca los siguientes procesos:

✓ Banco: CGGR02 Dirección General de Riesgos

Áreas

Dirección de Seguridad de la Información y Riesgos Digitales.
Dirección de Servicios Tecnológicos

Objetivos

1 Determinar el nivel de implementación en la aplicación de la metodología y lineamientos en la clasificación de la información alineados con los principios técnicos de disponibilidad, integridad y confidencialidad de los activos de información.

2 Verificar si la Dirección de Riesgos gestiona la clasificación de la información bajo un enfoque de mejora continua de acuerdo con lo definido por COBIT y la OEA para la gestión y clasificación de la información.

Principales resultados informe de Auditoría

El estudio se refiere a la evaluación y análisis de la gestión de la clasificación de la información en la Dirección de Riesgo, en particular en la Dirección de Seguridad de la Información y Riesgo Digital, en la actualización, implementación, monitoreo y generación de acciones de mejora continua. Adicionalmente, incluye la definición y aplicación de un nivel de madurez, basado en las mejores prácticas, para identificar el estado actual del proceso.

La clasificación de la información permite a la organización mejorar su eficiencia y garantiza que la información reciba la protección adecuada de acuerdo con su sensibilidad, valor, criticidad y el nivel de riesgos resultantes de una divulgación indebida, daño o destrucción no autorizada.

La implementación de la clasificación de la información en el Banco cuenta con una base documental aprobada y publicada, tiene un esquema de clasificación y etiquetado para la información.

Las oportunidades de mejora identificadas están relacionadas con:

- La definición del alcance está limitado a un plan de sensibilización; no contiene un alcance para ser medido por indicadores o métricas.
- La metodología no se integra con otros proyectos.
- La iniciativa no tiene asignadas las responsabilidades.

La Dirección de Riesgo debe redefinir la gestión de la clasificación de la información aplicando un enfoque sistémico, identificando los riesgos y el estado de aseguramiento meta, un plan operativo, los indicadores, un esquema de rendición de cuentas a órganos de supervisión y la integración de las partes interesadas; además, el esquema de monitoreo y mejora continua en la aplicación de la metodología de clasificación de la información.