AG-F-48-2020

Riesgo Digital

FISCALIZACIÓN

Proceso	*CGGR02 Dirección de Riesgos Corporativos.*
Subproceso u actividades	*CGTI01 Tecnologías de Información*
Dependecias que participan	*La Dirección de Seguridad de la Información y Riesgo Digital, Dirección de Servicios Tecnológicos y Dueños de los procesos y sistemas.*
Muestra visita a puntos de venta u otros	*Se consideran todas las evaluacionnes de Riesgo Digital del 2020*
Período de evaluación	*2020*
Generalidad	*El estudio comprende el análisis de la Metodología de Riesgo Digital: alineamiento con las mejores prácticas, aplicación en la identificación, clasificación, evaluación y tratamiento de los riesgos, determinar si tiene un enfoque preventivo, habilidades y competencias de las partes interesadas; concientización y cultura; seguimiento y mejora continua.*
Objetivo(s) del Estudio	➔ *Determinar el grado de implementación por parte de la Dirección de Riesgos de la Metodología de Riesgo Digital en la identificación, análisis y tratamiento de los riesgos según lo establecido por ISO 27000, ISO 31000 y COBIT.* ➔ *Verificar si la Dirección de Riesgos desarrolla la Metodología de Riesgo Digital con un enfoque preventivo y si los elementos que la conforman están alineados con lo solicitado por ISO 31000, ISO 27005 y COBIT.*
Objetivos Institucionales relacionados	*Superar la experiencia del cliente a través del liderazgo digital.*

Principales Hallazgos

El estudio evalúa la gestión que realiza la Dirección de Riesgos con respecto al riesgo digital, su metodología, aplicación, seguimiento y mejora continua sobre los sistemas del Conglomerado Financiero Banco Nacional.

El Banco tiene la Metodología de Riesgo Digital, la cual tiene como objetivo ser una guía que contribuya en administrar y mitigar el riesgo digital, sin embargo, la aplicación de la metodología contiene debilidades que no permiten que se cumpla ese objetivo.

Los resultados de la aplicación de la Metodología de Riesgo Digital no están relacionados o impactan los objetivos estratégicos del Conglomerado Financiero Banco Nacional, además estos resultados contienen oportunidades de mejora en la identificación, valoración y tratamiento del riesgo, como los siguientes:

- ⇨ *La herramienta de aplicación no identifica las fuentes riesgo, eventos, causas y consecuencias en la valoración que se realiza al sistema.*
- ⇨ *El resultado de riesgo digital para cada sistema esta conformado por los 55 riesgos definidos en la Metodología de Riesgo Digital, inclusive aquellos riesgos que no estén dentro del contexto del sistema que se analiza.*
- ⇨ *Los resultados de la aplicación contienen diferencias en la valoración final para el mismo tipo de riesgo para el mismo sistema y ausencia de observaciones que complementen el valor del riesgo asignado por parte del funcionario que realizo la valoración.*
- ⇨ *Las valoraciones se realiza por proceso y no por sistema tal como lo solicita la Metodología de Riesgo Digital.*

- *Los planes para el tratamiento de los riesgos no incluyen las recomendaciones que define ISO 31000 para una eficiente y oportuna acción mitigadora.*

La Dirección de Riesgos debe incorporar, como parte de la gestión de riesgo digital, actividades que permitan generar mejora en la supervisión, seguimiento, reporte de la gestión y rendición de cuentas de los participantes en la aplicación de la metodología.