INFORME MONITOREO DE RIESGOS DE SEGURIDAD DIGITAL

Edwing Lujan González Martínez

Secretaría TIC

Bucaramanga, 07 de enero de 2025

TABLA DE CONTENIDO

1. Introducción

En la Gobernación de Santander el seguimiento trimestral de los riesgos presentados permite tener un análisis de la efectividad de los controles realizados por cada una de las dependencias, y su nivel de criticidad, de acuerdo a los tipos identificados: de *corrupción, de gestión y digitales*.

El informe tiene como objetivo presentar el estado actual de la gestión de riesgos de seguridad digital en los diversos procesos de la Gobernación de Santander adjuntado el análisis de las evidencias proporcionadas y su relación con el estado del trimestre anterior.

El análisis abarca todos los procesos de la Gobernación que gestionan riesgos de seguridad digital y han reportado evidencias de su gestión a los Sistemas Integrados de Gestión (SIG), con fecha de corte 18 de diciembre de 2024, formulando recomendaciones para la gestión de los riesgos identificados.

2. Evaluación del estado de los riesgos

A continuación, se presenta la evaluación del estado actual de los riesgos de seguridad digital en la Gobernación de Santander. Esta evaluación se basa en la información recopilada sobre los riesgos identificados en los diferentes procesos, de acuerdo con la estructura de gestión de calidad disponible en la Intranet, específicamente en el archivo cargado por SIG en el cual se encuentran todos los riesgos consolidados.

De igual manera, se toma en cuenta la evidencia obtenida durante el último monitoreo de Sistemas Integrados de Gestión (SIG) realizado con corte a diciembre18 de 2024, en el que cada proceso busca evidenciar la gestión y aplicación de controles para mitigar los riesgos identificados.

1.1. Análisis de los riesgos de Seguridad Digital identificados según MAPA DE CALOR

A continuación, se presenta los mapas de calor del estado actual de los riesgos de seguridad digital en la Gobernación de Santander:

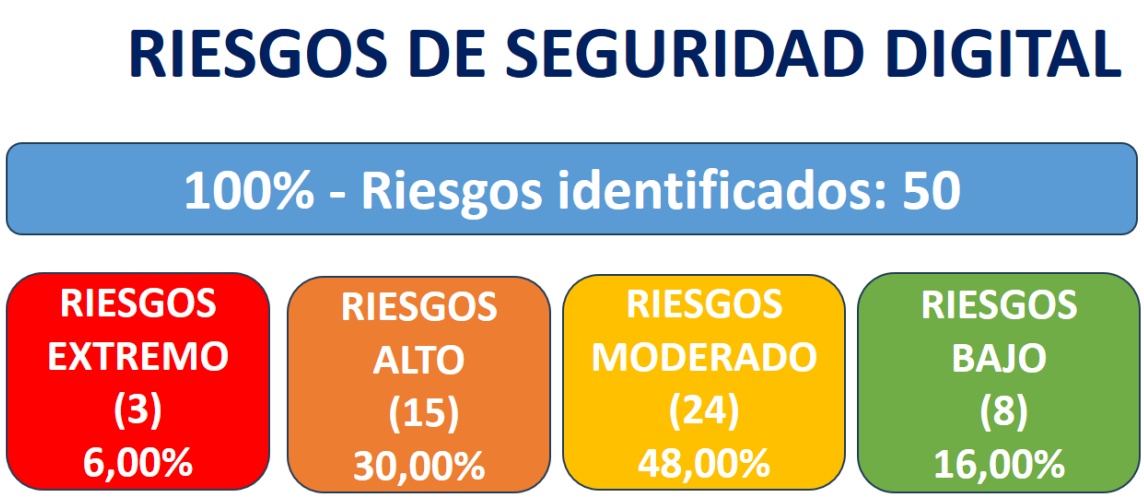

Imagen 1 Porcentaje de cada uno de los riesgos y sus niveles de valoración inherente

De los riesgos identificados, se clasificaron 3 como extremos, 15 como altos, 24 como moderados y 8 como bajos. Esta clasificación representa la valoración inicial inherente asignada a cada uno de los riesgos.

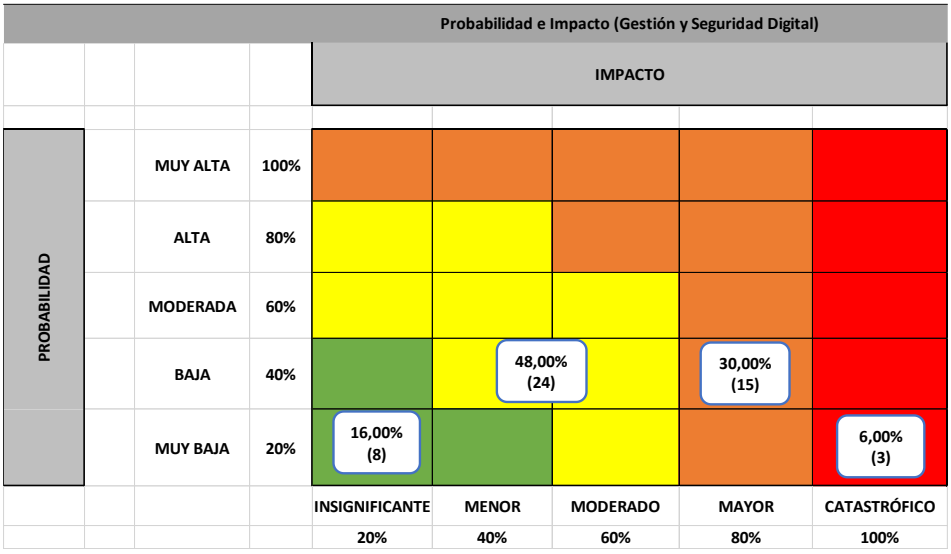

Imagen 2. Mapa de Calor y porcentaje de los riesgos según su valoración inherente

El cuadro anterior presenta y visualiza, a través de un mapa de calor, la distribución de los riesgos identificados según su valoración inherente.

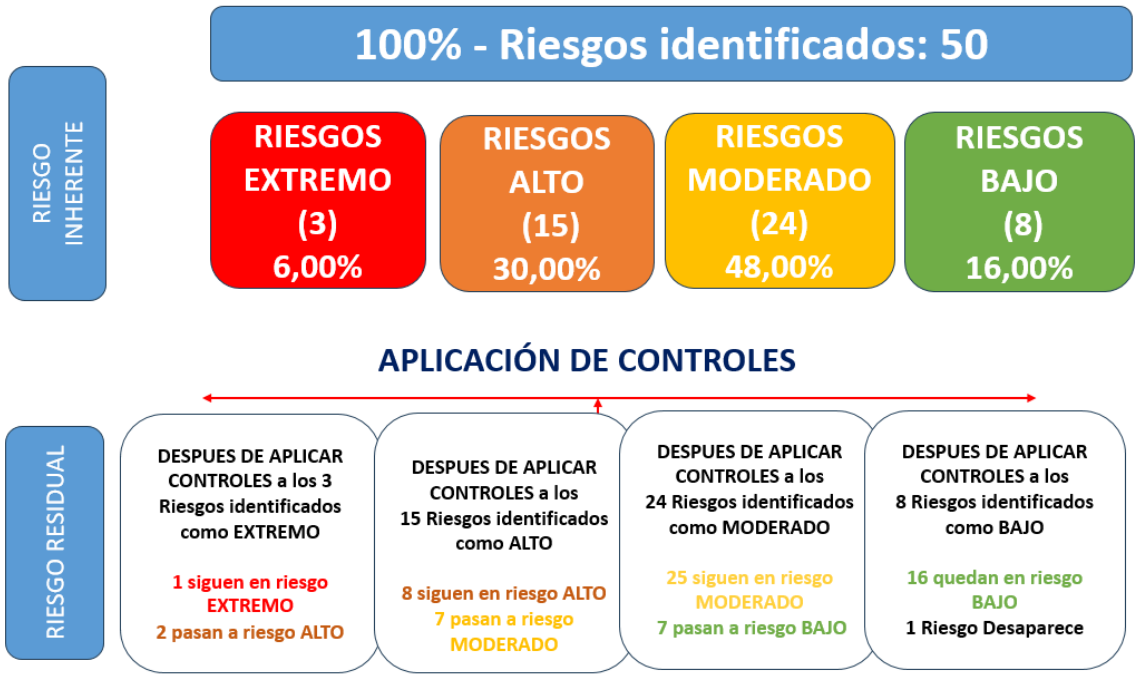

Imagen 3 Porcentaje de cada uno de los riesgos y sus niveles de valoración residual

La imagen anterior ilustra cómo los riesgos inherentes, inicialmente identificados, han sido mitigados tras la aplicación de controles. Se observa que un(1) riesgo permanece clasificado como extremo, mientras que dos(2) de los riesgos extremos han sido reevaluados y ahora se clasifican como altos.

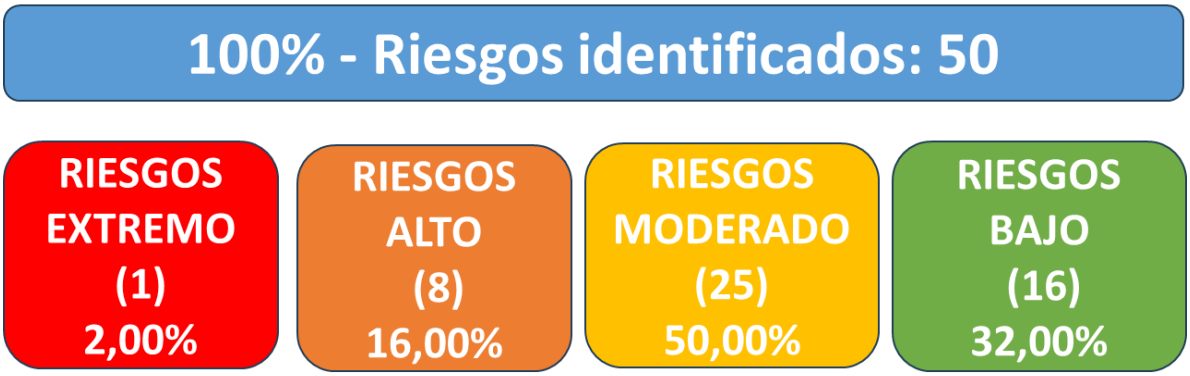

Imagen 4 Nivel de valoración residual de los riesgos

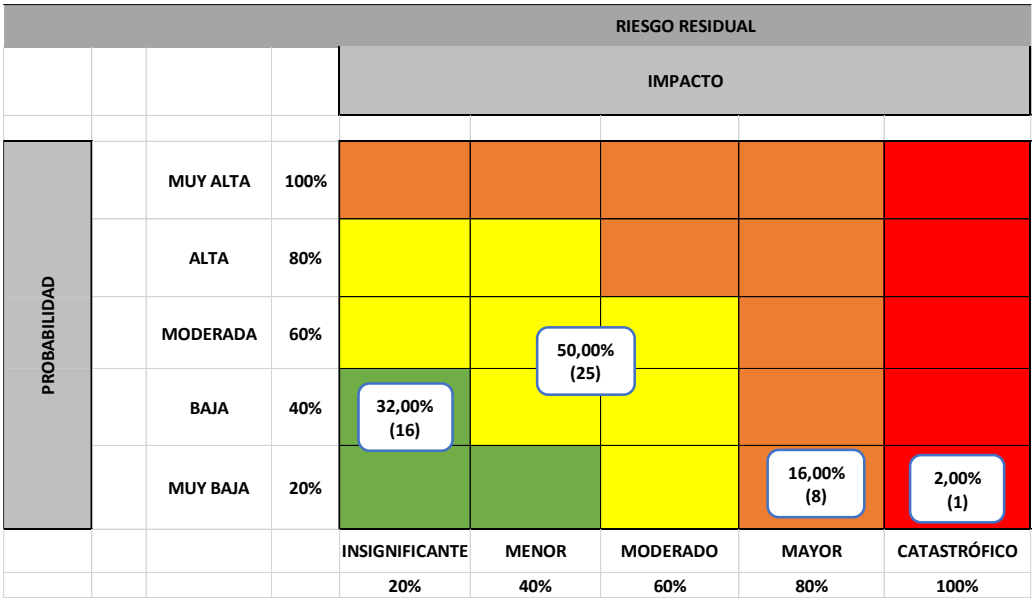

Imagen 5. Mapa de Calor y porcentaje de los riesgos según su valoración residual

El cuadro anterior muestra el mapa de calor correspondiente a la valoración residual de los riesgos tras la aplicación de controles. En él se detalla la distribución de los riesgos y su clasificación actual.

Con relación al informe del tercer trimestre se aprecia que se pasó de 51 riesgos a 50, situación que refleja como a partir de las acciones y controles realizados, se eliminó un riesgo del total detectado en el trimestre anterior, sin embargo es preocupante que muchas dependencias no enviaron las evidencias de los controles, probablemente por el corto lapso de tiempo para presentarlas y la época de finalización del año, donde ya no se tiene vinculación de contratistas.

2. Análisis de los riesgos de Seguridad Digital identificados por proceso

Adjunto a este documento se incluye una matriz en formato Excel que relaciona los 50 riesgos de seguridad digital, junto con sus controles y planes de acción propuestos por cada uno de los procesos. En la última columna de esta matriz en formato Excel se presenta el resultado del análisis realizado para cada riesgo. A continuación, se destacan las conclusiones de este análisis:

- ✓ **Efectividad de los Controles**: Muchos de los controles implementados no logran reducir el riesgo a niveles aceptables. A pesar de la existencia de estos controles, el riesgo inherente y residual se mantiene en niveles moderados, altos o incluso extremos.
- ✓ **Deficiencia de Controles Correctivos**: Se observa una notable falta de controles correctivos, recomendándose su implementación, especialmente en situaciones que requieren la realización de copias de respaldo.
- ✓ **Evidencias Insuficientes**: Las evidencias presentadas con frecuencia no respaldan la ejecución efectiva de los controles. En muchos casos, estas evidencias son incompletas, no corresponden a los controles o simplemente no se han presentado, presentando un notable incremento de falta de evidencias para el último trimestre.
- ✓ **Mejora de Planes de Acción**: Se recomienda la creación o mejora de planes de acción, ya que los existentes en ocasiones son poco claros, no cumplen su función de manera efectiva o no existen en absoluto.
- ✓ **Claridad en la Redacción**: Es necesario revisar y ajustar la redacción de ciertos riesgos, controles y planes de acción para lograr mayor claridad y coherencia. Se han identificado casos donde la descripción del riesgo no es precisa, los controles no están alineados con el riesgo o los planes de acción no abordan adecuadamente los problemas.
- ✓ **Mejora en la Gestión de Riesgos**: Se evidencia la necesidad de mejorar la gestión de los riesgos de seguridad digital, lo que implica la implementación de controles más efectivos, la presentación de evidencias sólidas que respalden su ejecución y la elaboración de planes de acción clara y concisa.

Para finalizar como recomendaciones generales en búsqueda de optimizar el proceso de recolección de evidencias y la formulación de riesgos, se reitera la propuesta para diseñar una mejor estructura para el almacenamiento de evidencias. La estructura actual resulta compleja, generando confusión sobre la pertenencia de las evidencias a los riesgos de seguridad digital. De igual manera, se ha observado que el consolidado de riesgos de seguridad digital que fueron evaluados presenta numerosos errores ortográficos y de redacción que requieren atención.