Gobernación de Norte de Santander

SECRETARÍA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

Secretaría de las TIC

Gobernación de Norte de Santander

2025

Avenida 5 calles 13 y 14 Palacio de Gobierno
Tel: **5956200 - 018000185783** - Email: **tic@nortedesantander.gov.co**
www.nortedesantander.gov.co

Tabla de contenido

1. INTRODUCCIÓN

De acuerdo al Plan Documentado de Gestión de Riesgos de Seguridad Digital de la Gobernación de Norte de Santander, donde se establecen procesos, procedimientos y actividades encaminadas a lograr un equilibrio entre la prestación de servicios y los riesgos asociados de los activos de información, que dan apoyo y soporte en el desarrollo de la misión de la Entidad, se debe considerar e implementar medidas que implican tiempo, esfuerzos y recursos necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad digital efectiva que controle los eventos o incidentes, y mitigar el impacto en su interior.

Casi siempre una situación no prevista provoca una crisis y consecuencias que, de acuerdo con su impacto y valor, pueden ser catastróficas para los intereses de la Entidad, y atentos a ello, se pretende definir un documento asertivo y ejecutable para la Gobernación del Departamento, en materia de recuperación de la normalidad para situaciones que se generen en los activos de información.

Por ello la Gobernación de Norte de Santander pretende estar preparada bajo un modelo de seguridad digital óptimo, que aporte medidas de control ante riesgos y desastres de tipo tecnológico.

2. OBJETIVOS

2.1 Objetivo General

Suministrar lineamientos encaminados a implementar un modelo de tratamiento de gestión de riesgos de seguridad digital para afrontar riesgos residuales que cesen actividades, alteren y afecten el funcionamiento de los procesos de la Gobernación de Norte de Santander.

2.2 Objetivos Específicos

- Identificar, evaluar y solucionar cualquier anomalía, de manera rápida y eficaz, que exista en los activos de información de la Gobernación.

- Implementar un plan de contingencia que oriente recuperación de información en las diferentes secretarías de la Gobernación.

- Reducir al máximo la materialización de los riesgos asociados infraestructura tecnológica y sistemas de información.

- Garantizar la disponibilidad, integridad y confidencialidad de los activos de información de la Entidad.

- Garantizar el normal desarrollo de los macroprocesos de gestión de la Gobernación.

3. ALCANCE

Mediante el registro y reporte de riesgos críticos generados en el Plan Ejecutado de Gestión de Riesgos de Seguridad Digital, se pretende implementar un Plan de Tratamiento de Riesgos de Seguridad Digital que genere confianza y un ambiente seguro en la utilización de los recursos tecnológicos y el procesamiento de la información bajo la normalización del desarrollo de actividades y servicios prestados por la Gobernación de Norte de Santander.

4. ROLES Y RESPONSABILIDADES

El Plan de Tratamiento de Riesgos de Seguridad Digital de la Entidad, es una responsabilidad conjunta y liderada por el Grupo de Trabajo de Arquitectura Empresarial para la Transformación Digital de la Gobernación Norte de Santander. Grupo que fue definido mediante Resolución No. 0010 del 27 de marzo de 2019 - Secretaría de las TIC, Gobernación de Norte de Santander.

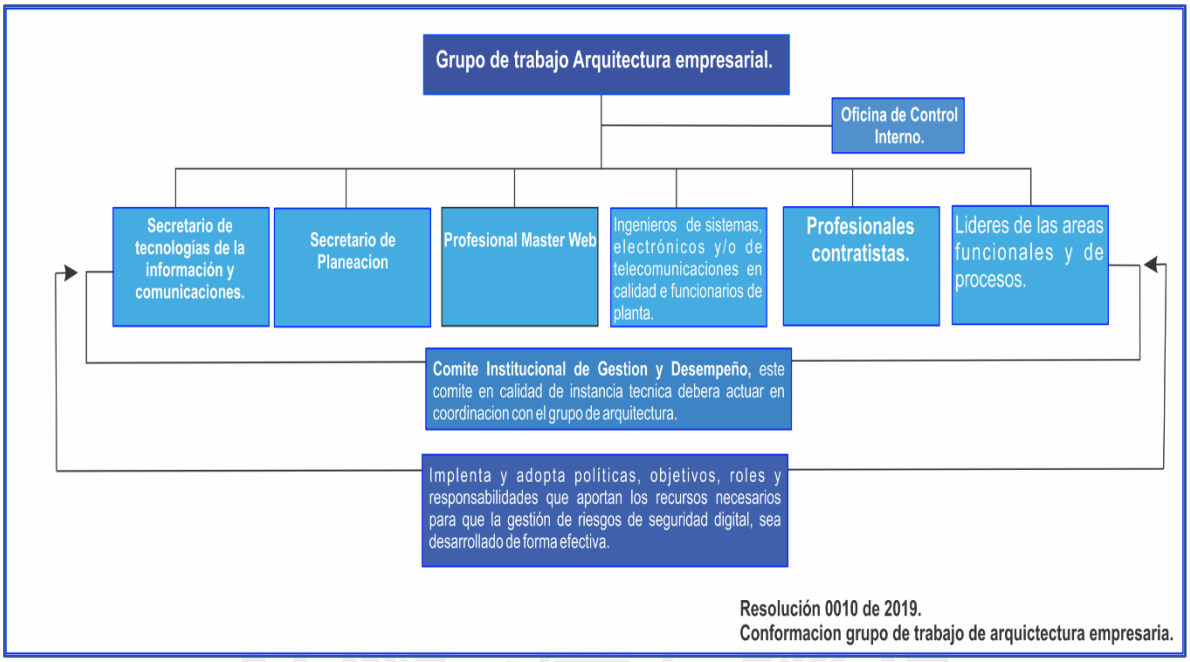

Imagen1: Grupo de trabajo de Arquitectura Empresarial para la Transformación Digital de la Gobernación N.D.S.
Fuente: Resolución No. 0010 de 27 de marzo de 2019 de Secretaría de las TIC de la Gobernación de N.D.S

El Grupo de Trabajo de Arquitectura Empresarial estará conformado por:

- El Secretario(a) de Tecnologías de la Información y Comunicaciones, en su calidad de rol de (CEO), o su delegado.
- El Secretario(a) de Planeación y Desarrollo Territorial, o su delegado.
- El profesional Máster Web de la Gobernación de Norte de Santander.
- Los Ingenieros de Sistemas, Electrónicos y/o de Telecomunicaciones en calidad de funcionarios de planta de la entidad que desempeñan funciones de la naturaleza de su cargo en todas las dependencias de la entidad.
- Los profesionales contratistas que cumplen actividades relacionadas con su profesión en las diferentes dependencias de la entidad.
- Los Líderes de las áreas funcionales y de procesos, cuando así se requiera su participación.
- La Oficina de Control Interno de Gestión conformará el Grupo de Trabajo de Arquitectura Empresarial en calidad de apoyo al desarrollo de un adecuado ambiente de control, monitoreo y supervisión continua a la gestión de la entidad.

El Grupo de Trabajo de Arquitectura Empresarial en calidad de instancia técnica deberá actuar en coordinación con el Comité Institucional de Gestión y Desempeño, para definir y tomar decisiones operativas y técnicas con relación a la Arquitectura Empresarial de la Entidad. Por lo tanto, cumplirá las siguientes funciones:

- El Secretario(a) TIC o su delegado en calidad de Líder del Grupo de Trabajo convocará al Grupo de Trabajo de Arquitectura para asistir al Comité Institucional de Gestión y Desempeño.
- Evaluar los impactos de las decisiones de inversión que sobre la materia de arquitectura de TI y Sistemas de Información e Infraestructura Tecnológica adelanten todas las dependencias de la Entidad, y en articulación con el Comité Institucional de Gestión y Desempeño presentar recomendaciones a las dependencias respectivas.
- Teniendo en cuenta el revestimiento técnico de este grupo de Trabajo, también cumple con funciones de gobierno sobre la arquitectura empresarial de la Entidad; por lo tanto, deberá remitirse al Comité Institucional de Gestión y Desempeño cuando se requiera tomar decisiones de alto nivel.
- Las demás funciones que, por la naturaleza técnica de arquitectura de TI en la entidad se deba cumplir.

5. IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La Gobernación de Norte de Santander percibiendo la importancia y necesidad de proteger los activos de información derivados de los sistemas de información, redes de comunicaciones y servicios web, destinará recursos para la adquisición e implementación de controles de tipo tecnológico, procedimental y operacional, minimizando de esta forma la exposición a peligros en el contorno digital que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Luego de revisión exhausta, mediante lluvia de ideas y juicio de expertos, funcionarios y contratistas de la Gobernación de Norte de Santander, se califican cada uno de los activos y se identifican amenazas y/o vulnerabilidades de cada uno de ellos para identificar los posibles riesgos de los activos de información.

Según el plan de gestión de riesgos de seguridad digital, resultaron los diferentes riesgos a los que puede encontrarse sometida el área tecnológica y activos de información, ellos se pueden agrupar y resultan controlarse mediante acciones de mitigación, como se describe a continuación:

IDENTIFICACIÓN, MITIGACIÓN Y CALIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL				
Riesgos	**Mitigación**	**Probabilidad**	**Impacto**	**Zona Riesgo**
Desastre natural	El edificio de la Gobernación cuenta con una estructura sismo resistente y planes de contingencia de riesgos de desastres para respuestas a emergencias, ya sea de origen natural, o derivada de la misma acción del hombre sobre el medio ambiente	1	3	Moderado
Interrupción del fluido eléctrico	Existe banco de UPS que respaldan el Data Center durante 3 horas de interrupción de fluido eléctrico.	3	1	Bajo
Cambio en Normatividad Externa (leyes, decretos, ordenanzas y acuerdos)	La Secretaría de las TIC del Departamento, cuenta con el grupo de trabajo de arquitectura empresarial conformado de acuerdo con las recomendaciones y políticas de Gobierno Digital de MINTIC, quien enfoca el diseño, planificación e implementación de políticas de seguridad digital en la Gobernación.	3	1	Bajo
Pérdida o Robo de Información Digital	La Gobernación cuenta con respaldo de la información de los servidores que se encuentran en el Data Center. Dicho respaldo se realiza todos los días en servidores remotos y discos duros externos. Se cuenta con cámaras de seguridad, detector de metales y planes de contingencia de seguridad interna.	2	2	Bajo
Falla de equipos electrónicos	La Gobernación cuenta con plan de mantenimiento preventivo, predictivo y correctivo (hardware, software, telefonía IP) para todas las Secretarías.	2	2	Bajo

IDENTIFICACIÓN, MITIGACIÓN Y CALIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL				
Riesgos	**Mitigación**	**Probabilidad**	**Impacto**	**Zona Riesgo**
Falla en servidores	La Gobernación contrata profesionales que prestan los servicios de administración de los servidores para actuar ante cualquier falla.	1	3	Moderado
Virus informáticos	La Gobernación contrata profesionales que interactúan en la configuración de los equipos, de acuerdo con políticas de seguridad y privacidad de información.	3	1	Bajo
Calentamiento del Data Center:	La Gobernación cuenta con una supervisión permanente para el control de temperatura en el salón provisto para el Data Center. Igualmente, los profesionales de administración de servidores realizan seguimiento diario a posibles fallas ocasionadas por hardware en servidores, rack y ups.	1	2	Bajo
No existan copias de seguridad sistemas de información	La Gobernación cuenta con respaldo de la información de los servidores que se encuentran en el Data Center. Dicho respaldo se realiza todos los días en servidores remotos y discos duros externos.	1	2	Bajo
Falta de planeación e inversión de recursos para infraestructura tecnológica.	La Gobernación cuenta con el grupo de trabajo de arquitectura empresarial, quien evalúa impactos de decisiones de inversion que sobre la materia de arquitectura TIC, sistemas de información e infraestructura tecnológica adelantan todas las dependencias de la Entidad.	1	3	Moderado

IDENTIFICACIÓN, MITIGACIÓN Y CALIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL				
Riesgos	**Mitigación**	**Probabilidad**	**Impacto**	**Zona Riesgo**
Atraso en adquisición, actualización y mantenimiento de la Infraestructura tecnológica y nuevas tecnologías.	Prioridad en el resguardo de la seguridad de la información, por tal motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado para la dirección TIC, decisiones que se verán reflejadas en los planes de compra anuales.	1	3	Moderado
Equivocaciones humanas	La Gobernación bajo la coordinación de la oficina de talento humano, implementa el plan anual de capacitaciones, que contrarresta debilidades y desarrolla conocimientos relativos al servicio que presta cada funcionario.	1	3	Moderado
Activos de información desactualizados	En trabajo conjunto, secretaría TIC y oficina de archivo, adelantan acciones bajo el macroproceso de Gestion Documental de la Gobernación, para planear la gestión y clasificación de activos de información.	1	2	Bajo
Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso.	La Gobernación se encuentra en etapa de transición e implementación para establecer lineamientos de adopción del protocolo IPV6, y así estar a la vanguardia del nuevo protocolo a implementar en el país, Igualmente se está modernizando la arquitectura de red en todas las secretarías de la Entidad.	2	2	Bajo

De acuerdo con la matriz de riesgos diseñada bajo estos parámetros y definidos en el plan de gestión de riesgos de seguridad digital de la Gobernación, y luego de una aceptación de los riesgos inherentes a los que puede estar expuesto críticamente la Entidad, se diseñan los controles de tratamiento de riesgos y recuperación de activos de información.

6. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

Ante una eventualidad que afecte el normal funcionamiento de las operaciones de la Gobernación, lo primero que se quiere es restablecer todos los servicios con el objetivo que el cliente no se vea afectado.

Parte muy importante de la Política de Seguridad y Privacidad de la Información, debe ser el plan de continuidad del negocio, el cual contempla las acciones que la Gobernación debe seguir para recuperar y restaurar las actividades críticas del negocio en un tiempo prudencial y de manera progresiva regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información.

La estrategia de Recuperación, basada en el hecho de que no hay acceso, y se encuentran inhabilitadas e inaccesibles por completo por un período inaceptable a los servicios del Data Center o a las instalaciones donde se ubica el Data Center.

Las estrategias a seguir serán acordes a la magnitud y duración esperada del incidente y se deberán tomar en cuenta los siguientes aspectos:

- Evaluación de los daños
- Evaluación del tiempo estimado de la recuperación.
- Análisis exhaustivo para determinar las acciones específicas que deberán seguirse de acuerdo al tipo de incidente.

6.1 ESTRATEGIA DE RECUPERACIÓN

Es necesario tomar en cuenta que para cada situación contingente corresponde una respuesta específica.

Según se considere las necesidades de recuperación y de acuerdo con los resultados del Tiempo objetivo de Recuperación, definidos por las diversas Unidades de Negocio, las estrategias de recuperación se considerarán dependiendo de la contingencia a prestar.

Responsabilidades de la estrategia de recuperación:

- Los ingenieros de la secretaría de las TIC efectuarán inmediatamente respaldos de emergencia y procedimientos de apagado, si el tiempo y la seguridad lo permiten.
- Los Ingeniero de soporte, ayudarán en la evaluación de daño del equipo, restauración de Comunicaciones y en la evaluación de las condiciones del Data Center.
- Las aplicaciones y servicios de criticidad menor serán restablecidas de acuerdo con las estrategias de recuperación y en los Tiempos Objetivos de Recuperación

(RTO) definidos. Todas las otras aplicaciones que no fueron definidas como críticas, serán restablecidas después de 6 horas.

Cabe anotar que la Secretaría de las TIC de la Gobernación, tiene a cargo estas responsabilidades y debe estar puesto a restablecer el servicio en el menor tiempo posible con la ayuda de los ingenieros de todas las secretarías de la Gobernación, esto dependiendo del tipo de riesgo que se llegase a producir.

Como herramientas de recuperación para algún tipo de desastre, en primer lugar, está el restablecer la información guardada mediante copias de seguridad en el menor tiempo posible.

El equipo de Ingenieros de la Secretaria de las TIC de la Gobernación de Norte de Santander, dispone una base de datos con todas las contraseñas de los equipos de cómputo, servidores para restablecimiento de la información de caso de pérdida o robo, desastre natural, etc.

6.2 RECUPERACIÓN DEL DESASTRE: PLAN DE ACCIÓN.

El Plan propone que debe utilizarse un Centro alterno de trabajo, si la emergencia afecta en forma general (en más de un 50%) las instalaciones físicas y técnicas con las que se cuentan.

Primera fase: Procedimientos de Respuesta/Notificación inmediata.
Los siguientes deben ser los procedimientos a ser implantados en el momento del desastre, dichos procedimientos deben continuar hasta que se restauren los servicios de procesamiento de datos en el sitio original u otro permanente. En el caso de incendio, explosión u otro desastre mayor en el Data Center, deben implantarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional o prevención de desastres de la Gobernación de Norte de Santander, previa notificación a uno de sus integrantes.
Procedimientos de Emergencia en el Data Center. Si la naturaleza del desastre no da tiempo para apagar y evacuar, la prioridad más alta es la seguridad de las personas. Ellos deben salir inmediatamente del área afectada. En un caso de estos, el siguiente paso es notificar inmediatamente al grupo de administración de emergencia (Grupo de Salud Ocupacional o gestión de riesgos de la Gobernación de Norte De Santander). Si hay tiempo para apagar, se deben realizar las siguientes actividades, en el orden especificado:

1. Iniciar procedimientos de emergencia organizacional estándar (los establecidos por el Grupo de Salud Ocupacional gestión de riesgos de la gobernación de Norte de Santander).
2. Ejecutar procedimientos de apagado para los servidores y demás dispositivos del Data Center.
3. Apagar extractores.
4. Apagar luces y bajar tacos en las cajas de distribución

Segunda fase: Procedimientos para el proceso de restauración.
Tan pronto como se haya declarado un desastre, los líderes del grupo serán llamados para implantar el plan a tomar en el desarrollo del Plan de Contingencias. El grupo de Ingenieros de las Tic junto con el grupo de atención a usuarios establecerá un centro de control y empezarán la coordinación para la restauración de los sistemas que hayan sido afectados.
Acciones a seguir:
Dentro de las seis (6) horas siguientes al desastre se debe: 1. Notificar a los usuarios la interrupción del servicio. 2. Efectuar una evaluación de daños e identificar que equipos se pueden reusar para transferirlo al Data Center alterno. 3. Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.
Dentro de las veinticuatro (24) horas siguientes al desastre debe:
1. Contactar con el proveedor y ordenar el soporte Internet, Vmware (sistema de virtualización de servidores). 2. Iniciar y coordinar los procedimientos de preparación del lugar para el Data Center alterno. 3. Montar data center alterno. 4. Notificar a los proveedores las con figuraciones de hardware nuevas y alistar los requerimientos que surjan de esas configuraciones. 5. Confirmar el soporte dado por el proveedor. 6. Inicializar las preparaciones ambientales en el Data Center o Centro de Respaldo (Eléctrica, protección contra incendio, extractores). 7. Ordenar los circuitos para comunicación de datos en el Data Center, si es necesario.
Dentro de las cuarenta y ocho (48) horas siguientes al desastre:

1. El Data center alterno de la gobernación debe estar totalmente preparado para operar llevar el inventario de los medios magnéticos, los listados y otra documentación en el centro Alterno.
2. Recibir en el Data center suficientes suministros, muebles y equipo relacionado.
3. Establecer un diálogo de procedimiento de las aplicaciones críticas.

Dentro de los cuatro (04) días siguientes al desastre debe:

1. Completar la preparación ambiental del Centro Alterno.
2. Recibir la documentación y el medio magnético de los lugares de almacenamiento en el Data center alterno.
3. Asegurar el ambiente físico en el Data Center alterno y establecer la seguridad de los datos.
4. Reestablecer los backups de datos.
5. Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
6. Notificar a los usuarios el estado de la recuperación.

Dentro de los Ocho (08) días siguientes al desastre:

1. Asegurar la operación total de los sistemas críticos.
2. Continuar la implantación por fases de la red de comunicación de datos.

Tercera fase: Recuperación en el sitio original o alterno

Mientras que las operaciones se estén ejecutando en el Data Center alterno, se harán planes para la recuperación total en el sitio original. Si hay un desastre mayor, o si está dentro de los planes de la organización, se puede realizar la recuperación en un sitio alterno improvisado.

Los siguientes son los componentes procedimentales importantes de las actividades en esta fase:

- Decisiones en el tiempo y equipo de recuperación.
- Preparar restauración del lugar.
- Desarrollo de los procedimientos de recuperación para la localización permanente.
- Repetir los procedimientos de recuperación.
- Asegurar el ambiente físico y establecer la seguridad de los datos.
- Montaje de los sistemas.
- Evaluación de los sistemas.
- Realizar auditoria post-desastre.
- Preparar reclamación de los seguros.
- Reportar a la gobernación.

Cuarta fase: Mantenimiento
Parte del mantenimiento del Plan será la Programación de sistemas requeridos para mantener los programas con los cambios sobre el tiempo, del hardware, software y aplicaciones. Esta es obviamente la clave para el futuro exitoso del plan. La actualización de nombres, responsabilidades y números telefónicos de los participantes claves de la dirección TIC y la secretaría Administrativa, es además, críticamente importante. El plan será auditado para ver que estos detalles sean actualizados rutinariamente en el plan y en todas sus copias.

Implementación del plan
Para la implementación del plan, debe estar formalmente documentados, y en operación, los siguientes procedimientos: • Retención y respaldo de archivos permanente y corrientes de los aplicativos que se manejen en el Data Center de la gobernación de Norte de Santander. • Recuperación de errores y fallas del sistema. • Seguridad física y lógica. • Seguimiento al plan de mantenimiento preventivo y correctivo de equipos por parte del supervisor del contrato de dicho mantenimiento. • Administración de personal en lo referente a las emergencias. • En primera instancia, el presente plan debe ser puesto a consideración, revisión y aprobación por parte de la Secretario(a) de las TIC. • En segunda instancia, desarrollar un programa de entrenamiento a los sujetos y áreas directamente involucradas, aquellas que asumen responsabilidades y funciones dentro del plan. • Finalmente debe adoptarse a nivel institucional mediante Acto Administrativo, es decir reglamentado por resolución.

Sonia Arango Medina

Secretaria de las Tecnologías de la Información y las Comunicaciones