PLAN DE GESTION DE RIESGOS DE SEGURIDAD DIGITAL.

GOBERNACION DE NORTE DE SANTANDER.

SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES.

Contenido

1. INTRODUCION

La gestión de riesgos de seguridad digital establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misión de la Gobernación de Norte de Santander. 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, mitigando el impacto en el interior de la entidad.

2. Objetivos

2.1 Objetivo General

Implementar un modelo de Gestión de Riesgos de Seguridad Digital a través del cual se mitiguen las debilidades y amenazas asociados al entorno digital de los activos de información de la Gobernación de Norte de Santander; bajo los principios de disponibilidad, integridad y confidencialidad de la información de la Entidad.

2.2 Objetivos Específicos

- ✓ Identificar las amenazas e impactos de seguridad digital asociadas a los macro procesos de la entidad.
- ✓ Analizar las amenazas y riesgos en el contexto de seguridad digital con relación a los activos de información.
- ✓ Valorar controles que atiendan la vulnerabilidad del entorno digital.
- ✓ Definir e implementar planes de acción que mitiguen el riesgo digital.

3. Alcance

El alcance del Plan de Gestión de Riesgos de Seguridad Digital, es el resultado de identificar factores internos y externos de la Entidad, asociados a procesos donde se apliquen criterios de evaluación del Riesgo de Seguridad Digital, ejecutando valoraciones de los riesgos en los activos de información y ejerciendo controles que permitan el tratamiento, registro y reporte de eventos de Riesgos; alcanzando estándares que permitan el mejoramiento continuo, mediante auditorías internas.

4. Glosario

Para la gestión de riesgos de seguridad digital es importante manejar claramente y con propiedad los siguientes términos:

- **Acceso a la información pública**

  Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Actitud hacia el riesgo**

  Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo. (NTC ISO 31000:2011)

- **Activo**

  Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

- **Activo cibernético**

  En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Amenaza**

  Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

- **Amenaza cibernética**

  Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

- **Análisis del riesgo**
  Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

- **Apetito de riesgo**
  Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar. (Componente COSO ERM II).

- **Ataque cibernético**
  Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

- **CCOC**
  Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

- **CERT**
  Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).

- **Cibercrímen (Delito cibernético)**
  Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

- **Ciberdefensa**
  Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES

3854, pág. 88).

- **Ciberseguridad**
  Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

- **Ciberterrorismo**
  Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas. (CONPES 3854, pág. 88).

- **Ciberdelincuencia**
  Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).

- **Ciberdelito/Delito cibernético**
  Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

- **Ciberespacio**
  Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Cibernética**
  Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).

- **Cibernético**
  Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Diccionario de la lengua española).

- **Convergencia**
  Evolución coordinada de redes que antes eran independientes hacia una

uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1).

- **CSIRT**
  Por su sigla en inglés: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

- **Comunicación y consulta**
  Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes involucradas con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

- **Consulta**
  La consulta es un proceso de doble vía de la comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema. La consulta es: un proceso que tiene impacto en la decisión a través de la influencia más que del poder; y: una entrada para la toma de decisiones, no para la toma conjunta de decisiones. (NTC ISO 31000 definición 2.12.).

- **Compartir el riesgo**
  Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

- **Conocimiento, capacidades y empoderamiento**
  Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto. (CONPES 3854, pág. 25).

- **Consecuencia**
  Resultado o impacto de un evento que afecta a los objetivos. (NTC ISO 31000:2011).

- **Contexto externo**
  Ambiente externo en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

- **Contexto interno**
  Ambiente interno en el cual la organización busca alcanzar sus objetivos.

(NTC ISO 31000:2011).

- **Control**
  Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- **Cooperación**
  Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

- **Criterios del riesgo**
  Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

- **Derechos humanos y valores fundamentales**
  Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

- **Entorno digital**
  Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

- **Entorno digital abierto**
  En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

- **Establecimiento del contexto**
  Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. (NTC ISO 31000:2011).

- **Evaluación del control**
  Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

- **Evaluación del riesgo**
  Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).

- **Evento de seguridad de la información**
  Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

- **Evitar el riesgo**
  Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).

- **Evento**
  Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).

- **Fuente de riesgo**
  Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

- **Frecuencia**
  Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).

- **Gestión del riesgo**
  Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

- **Gestión de riesgos de seguridad digital**
  Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854,

pág. 24).

- **ICC**
  Es la denominación de lo que el CCOC ha definido como infraestructuras críticas cibernéticas en el ámbito colombiano.

- **Identificación del riesgo**
  Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).

- **Incidente digital**
  Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Incidente de seguridad de la información**
  Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

- **Infraestructura crítica cibernética nacional**
  Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

- **Inventario de activos**
  Sigla en inglés: *Assets inventory*. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

- **ISO**
  Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).

- **Marco de referencia para la gestión del riesgo**
  Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través de toda la organización. (NTC

ISO 31000:2011).

- **Monitoreo**
  Verificación, supervisión, observación crítica o determinación continúa del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado. (NTC ISO 31000:2011).

- **Múltiples partes interesadas**
  El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades. (CONPES 3854, pág. 29).

- **Nivel de riesgo**
  Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).

- **Organización**
  Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones. (NTC ISO 31000:2011).

- **Parte involucrada**
  Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).

- **Peligro:**
  Una fuente de daño potencial. (NTC ISO 31000:2011).

- **Pérdida**
  Cualquier consecuencia negativa o efecto adverso, financiero u otro. (NTC ISO 31000:2011).

- **Perfil del riesgo**
  Descripción de cualquier conjunto de riesgos. (NTC ISO 31000:2011).

- **Política**
  Intenciones y dirección de una organización como las expresa formalmente su alta dirección. (ISO/IEC 27000:2016).

- **Política para la gestión del riesgo**
  Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

- **Posibilidad**
  Se utiliza como descripción general de la probabilidad o la frecuencia. (NTC ISO 31000:2011).

- **Plan para la gestión del riesgo**
  Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

- **Probabilidad**
  Oportunidad de que algo suceda. (NTC ISO 31000:2011).

- **Proceso para la gestión del riesgo**
  Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).

- **Propietario del riesgo**
  Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).

- **Responsabilidad**
  Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales. (CONPES 3854, pág. 25).

- **Revisión**
  Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos. (NTC ISO 31000:2011).

- **Reducción del riesgo**
  Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

- **Resiliencia**
  Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).

- **Retención del riesgo**
  Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

- **Riesgo**
  Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).

- **Riesgo inherente**
  Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

- **Riesgo residual**
  Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).

- **Seguridad de la información**
  Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).

- **Seguridad digital**
  Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).

- **Servicios esenciales**
  Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas (Tomado del documento ICC del CCOC).

- **SGC:**
  Sistema de gestión de calidad.

- **SGSI**
  Sistema de gestión de seguridad de la información.

- **Sistema para la gestión del riesgo**
  Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).

- **Telecomunicaciones**
  Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución MinTIC 202 de 2010).

- **TI**
  Tecnologías de la información.

- **TO**
  Tecnología de operación

- **TIC (Tecnologías de la información y las comunicaciones)**
  Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC).

- **Tratamiento del riesgo**
  Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009).

- **Valoración del riesgo**
  Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

- **Vulnerabilidad**
  Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

5. Metodología de Gestión de Riesgos de Seguridad Digital

La Gobernación de Norte de Santander adoptará la metodología del Modelo Nacional de Gestión de Riesgos de Seguridad Digital del MINTIC y La Guía para la Administración de los Riesgos de Gestión, Corrupción Seguridad Digital y el Diseño de Controles en Entidades - DAFP.

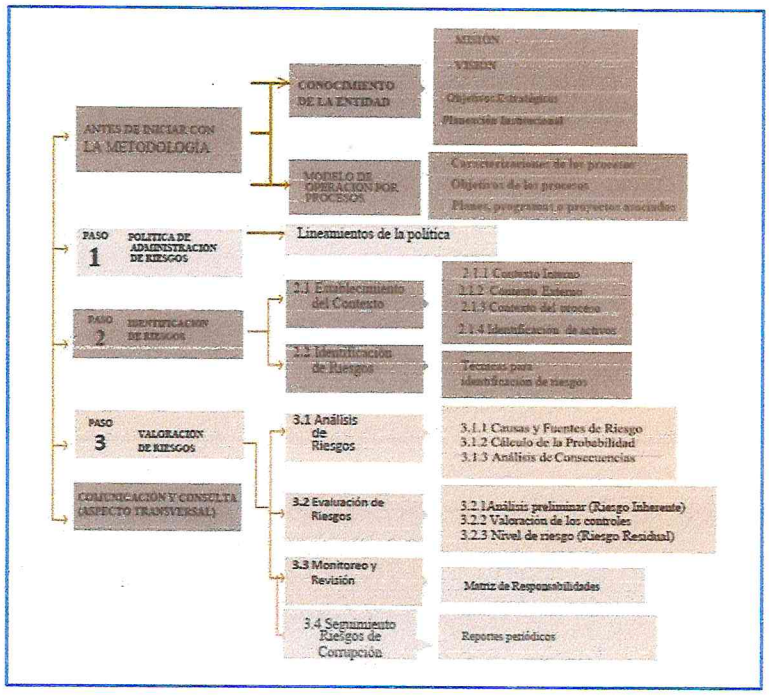


Imagen1: Metodología para la Administración de Riesgos
Fuente: Guía Para la Gestión de Riesgos de Seguridad Digital

En la Guía para la Administración de los Riesgos de Gestión, Corrupción Seguridad Digital y el Diseño de Controles en Entidades se propone una metodología que, a través de fases y actividades, permite gestionar los riesgos de seguridad digital a los que están expuestos los activos de información de la Gobernación de Norte de Santander.

En el marco conceptual del Modelo de Gestión de Riesgos de Seguridad Digital (MGSD) provee una guía para la implementación de gestión de riesgos de seguridad digital basado en principios generales y fundamentales donde se establece una interacción con los Sistemas de Gestión de la Seguridad de la Información (SGSI) o para el caso de las entidades del sector público colombiano con el Modelo de Privacidad y Seguridad de la Información (MPSI); así como la

relación con los activos de información que soportan la operación de cualquier Entidad u Organización a nivel general y en particular con las denominadas infraestructuras Criticas Cibernéticas por el CCOC (Modelo Nacional de Gestión de Riesgos de Seguridad Digital), tal como se observa en la imagen 2.

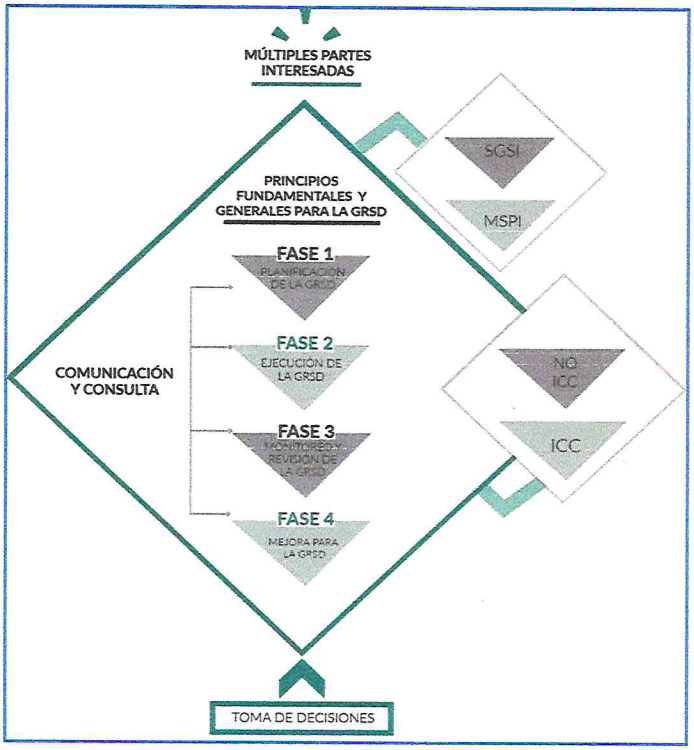


Imagen2: Marco Conceptual del MGRSD
Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital del MINTIC

El Modelo de Seguridad y Privacidad de la Información (MSPI) está complementado por el Plan de Gestión de Riesgos de Seguridad de la Digital (MGRSD) donde se integra con cada una de las fases propuestas, como se observa en la imagen 3.

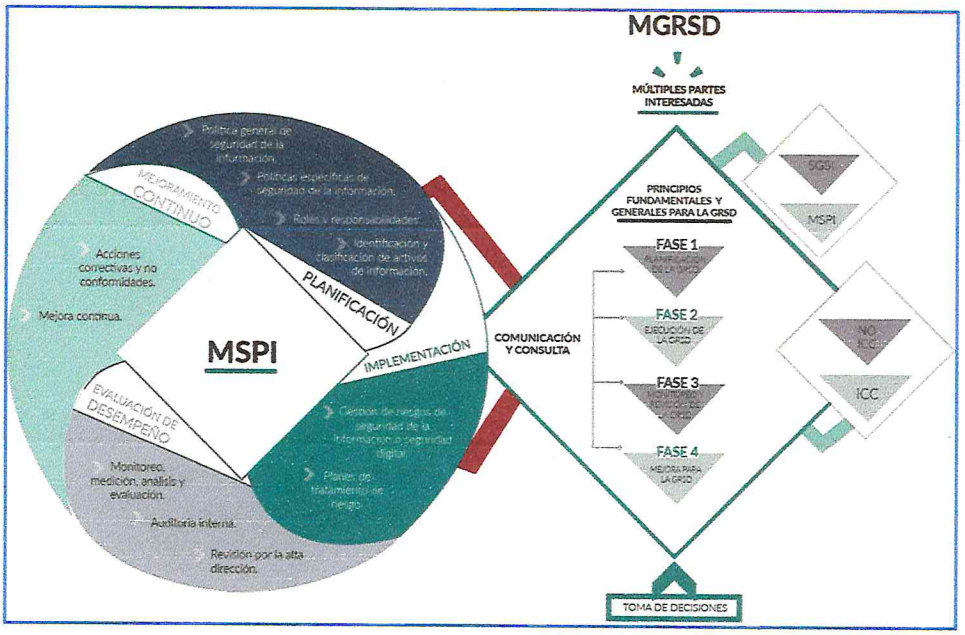


Imagen3: Interacción entre el MSPI y el MGRSD
Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital del MINTIC

6. Metodología de Plan de Gestión de Riesgos de Seguridad Digital

La Gobernación de Norte de Santander en seguimiento a los lineamientos establecidos por el Gobierno Nacional, expuestos en la Ley de transparencia y acceso a la información (Ley 1712 de 2014) y la Política de Gobierno Digital (Decreto 1008 del 2018). Establece un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y el nivel de impacto asociados a los activos de información sin importar el grado de criticidad que tengan.

En la gestión de riesgos de seguridad digital resulta importante lograr una comprensión de los riesgos con base en las posibles consecuencias de afectación; establecer una estrategia de mitigación adecuada que logre un entendimiento y aceptación del riesgo digital, así como de los recursos necesarios, en relación costo-beneficio con el fin de emplear medidas para proteger y asegurar la información de los sistemas de información, aplicaciones, servicios tecnológicos, bases de datos, redes de comunicaciones, equipos de cómputo garantizando la disponibilidad, confidencialidad e integridad de la información.

Por esto resulta preciso definir actividades que de manera articulada entre las secretarias, oficinas y altas consejerías que permitan la implementación de medidas de control que ayuden a la prevención, limitación y mitigación de coacciones a los que se encuentran expuestos los activos de información de la entidad por medio de una metodología descrita a continuación:

6.1 Fase de Planeación

6.1.1 Establecimiento del Contexto de la Entidad

6.1.1.1 Contexto Externo

El Congreso de la República estableció la Ley 1712 marzo 6 del 2014, por medio de la cual se creó la ley de transparencia y del derecho de acceso a la información pública nacional. En el cual se empodera al ciudadano el poder acceder a la información de carácter público que les permita realizar estudios de tipo estadísticos, científico o que simplemente les permita estar informados.

El Congreso de la República decretó la Ley 1581 octubre 17 de 2012, Por el cual se dictan disposiciones generales para la protección de datos personales, el cual tiene como objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la constitución política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Por lo anterior, toda información que se encuentre en los distintos sistemas de información, bases de datos, archivos digitales, dispositivos de almacenamiento y demás que sean de la Gobernación de Norte de Santander, deben contemplar las medidas mínimas de protección de esta información, de tal manera que no esta sea integra y no afecte de ninguna manera el buen nombre de las personas, de igual forma el Departamento está comprometido con toda la información que es creada y administrada, la cual es publicada por la entidad, cumpliendo de esta manera con lo estipulado en le Ley 1712.

Por otra parte, el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, estableció el decreto 1008 junio 14 del 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" que por medio del uso de tecnologías de la información y las comunicaciones permita lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que el Gobernación de Norte de

Santander desempeña una gran labor disponiendo recursos tanto económicos como humano con el objeto de implementar estrategias internas que de la mano con las nuevas tecnologías alcanzar los fines que dispone la ley, minimizando las amenazas digitales y de esta manera tener un gobernanza accesible, transparente y productivo.

6.1.1.2 Contexto Estratégico

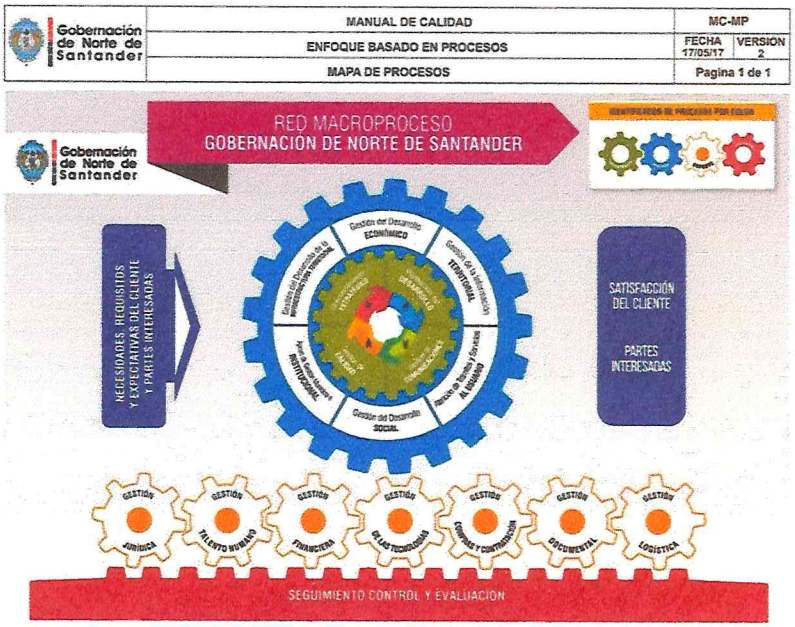
El Departamento de Norte de Santander creado mediante Ley 25 de julio 14 de 1910, que segrego del antiguo Departamento de Santander las provincias de Cúcuta, Ocaña y pamplona, época en que gobernaba la Nación el General Rafael González Valencia, tiene como principales funciones y objetivos, lo estipulado en el Decreto 1222 de 1986; en el cual las funciones del Departamento son las siguientes:

- Participar en la elaboración de los planes y programas nacionales de desarrollo económico y social y de obras públicas y coordinar la ejecución de los mismos. El Departamento de Nacional de Planeación citara a los gobernadores, al Alcalde mayor de Bogotá y a los intendentes y comisarios para discutir con ellos los informes y análisis regionales que prepares los respectivos consejos seccionales de planeación. Estos informes y análisis deberán tenerse en cuenta para la elaboración de los planes y programas de desarrollo a que se refieren los artículos 76 y 118 de la constitución política.
- Cumplir funciones y prestar servicios nacionales, o coordinar su cumplimiento y prestación, en las condiciones que prevean las delegaciones que reciban y los contratos o convenios que para el efecto celebren.
- Promover y ejecutar, en cumplimiento de los respectivos planes y programas nacionales y departamentales actividades económicas que interesen a su desarrollo y al bienestar de sus habitantes.
- Prestar asistencia administrativa, técnica y financiera a los municipios, promover su desarrollo y ejercer sobre ellos la tutela que las leyes señalen.
- Colaborar con las autoridades competentes en la ejecución de las tareas necesarias por la conservación del medio ambiente y disponer lo que requiera la adecuada preservación de los recursos naturales.
- Cumplir las demás funciones administrativas y prestar los servicios que les señalen la constitución y las leyes.

ARTICULO 6: Los departamentos tendrán independencia para la administración de los asuntos seccionales, con las limitaciones que establece la constitución, y ejercerán sobre los municipios la tutela administrativa necesaria para planificar y coordinar el desarrollo regional y local y la prestación de servicios, en los términos que las leyes señalen (CP Articulo 182, Inc 1).

6.1.1.3 Contexto Interno

LA GOBERNACION DE NORTE DE SANTANDER actualmente cuenta con una estructura organizacional con macro procesos estratégicos, misionales, soporte, y evaluación; se cuenta con distintos sistemas de información y servicios tecnológicos que soportan estos macro procesos y por lo cual es necesario velar por la protección y seguridad de estos activos de información, esto con el fin de mitigar los riesgos de seguridad digital más críticos, que puedan impactar de manera considerable la ejecución de las funciones y consecución de los objetivos.



En el contexto interno, el Gobernación de Norte de Santander definió el Plan de Desarrollo 2016 – 2019, el cual contempla mejorar la atención hacia el ciudadano, y el acercamiento de las personas para una gobernanza transparente. Por esta razón, El Departamento en función de velar por la disponibilidad, confidencialidad e integridad de los datos e información que se encuentran en el sistema de información **SIEPDOC**, el sistema de registro de eventos **RV** y sistema de gestión calidad **SGC**. Logrando de esta manera la consolidación de sistemas de

información de la entidad y así poder atender de forma ágil y oportuna los requerimientos de la ciudadanía.

De igual forma con la definición del Plan Estratégico de Tecnologías de la Información **PETI** formulado y ajustado a la Política de Gobierno Digital por la Gobernación de Norte de Santander, propone la inversión de recursos con el fin de llegar a un modelo integral y acceder equipos de nuevas tecnologías, apropiándonos así de las Tecnologías de la Información y de esta manera mejorar el servicio y la atención para el ciudadano.

En el año 2018 la entidad definió y adopto la Política de Seguridad y privacidad de la información. Este documento describe lineamientos para la gestión de la seguridad de la información y sirven como mecanismos para minimizar amenazas asociadas a los activos de información de la entidad.

6.1.1.4 Contexto del Proceso

El Plan de Gestión de Riesgos de Seguridad Digital hace parte de la Política de Seguridad y Privacidad de la Información definido por la Secretaria TIC de la Gobernación de Norte de Santander y los cuales hacen parte del macro proceso de soporte nombrado "GESTIÓN DE LAS TECNOLOGIAS" el cual tiene como objetivo: " Planear, organizar, dirigir, mantener, controlar y garantizar la integridad física de los recursos informáticos, y brindar una herramienta que sirva para dotar de información necesaria al Gobernador, Secretarias, Oficinas, Altas Consejerías, Funcionarios de Planta, Contratistas y Usuarios Externos, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software, así como la información y/o datos que son procesados y almacenados en cada una de las dependencias. De esta manera resguardar los activos de la Gobernación de Norte de Santander".

6.1.2 Política de Gestión del Riesgo

La Política de gestión de riesgos de seguridad digital GRSD definida por la entidad, será parte integral del documento titulado "Política de Seguridad y Privacidad de la Información".

6.1.3 Roles y Responsabilidades

La gestión de riesgos de seguridad digital es una responsabilidad que debe ser asumida por el Grupo de trabajo de Arquitectura Empresarial para la Transformación Digital de la Gobernación N.D.S. definido mediante Resolución No. 0010 de 27 de marzo de 2019 de Secretaría de las TIC de la Gobernación de N.D.S.

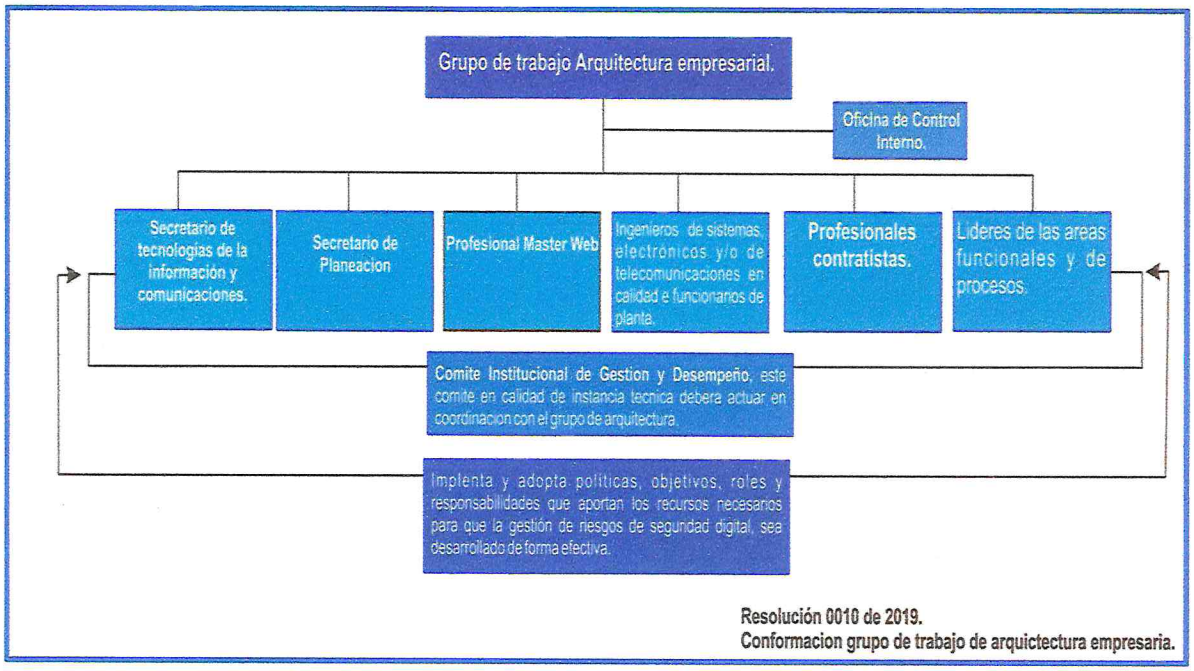


Imagen4: Grupo de trabajo de Arquitectura Empresarial para la Transformación Digital de la Gobernación N.D.S.
Fuente: Resolución No. 0010 de 27 de marzo de 2019 de Secretaría de las TIC de la Gobernación de N.D.S

6.1.4 Definición de Recursos para la Gestión de Riesgos de Seguridad Digital

Los recursos avalados, luego de estudio de impacto de decisiones de inversión de arquitectura TIC por parte del Grupo Empresarial para la Transformación Digital, provendrán de recursos propios de la Gobernación de Norte de Santander. El rubro será destinado a la adquisición de software e infraestructura tecnológica que ayude a minimizar los riesgos de seguridad digital y la posible contratación de personal con formación y conocimiento en seguridad y privacidad de la información.
Igualmente la Gobernación de Norte de Santander cuenta con pólizas de garantía y cumplimiento en los eventos en que los servicios tecnológicos sean administrados por un tercero.

6.1.5 Criterios para Evaluación de los Riesgos de Seguridad Digital

La Gobernación de Norte de Santander, define escalas o niveles de medición de los riesgos de seguridad digital, de acuerdo a la guía para la administración del riesgo de la función pública.

6.5.1.1 Criterios de Valoración de Impacto

Basado en el contexto en el cual se establece el MGRSD, las variables a considerar, para definir los criterios de impacto, son: integridad (I), disponibilidad (D) confidencialidad (C), social (S), económica (E), ambiental (A), las cuales se exponen a continuación:

Tabla 1. Criterios de valoración de impacto de acuerdo con la información

Nivel asignado	Valor del impacto	Criterios de impacto para características de seguridad de la información					
		Integridad (I)	Disponibilidad (D)	Confidencialidad ©	Social (S)	Económica (E)	Ambiental (A)
Insignificante	1	Sin afectación de la integridad	Sin afectación de la disponibilidad	Sin afectación de la confidencialidad	Afectación del X% de la población o menos	Afectación del X% del presupuesto anual de la entidad o menos	Sin Afectación medioambiental
Menor	2	Afectación muy leve de la integridad	Afectación muy leve de la disponibilidad	Afectación muy leve de la confidencialidad	Afectación del X% de la población	Afectación del X% del presupuesto anual de la entidad	Afectación leve del MA requiere de X meses de recuperación
Moderado	3	Afectación leve de la integridad de la información debido al interés particular de los empleados y terceros	Afectación leve de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación leve de la confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X% de la población	Afectación del X% del presupuesto anual de la entidad	Afectación leve del MA requiere de X años de recuperación
Mayor	4	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X% de la población	Afectación del X% del presupuesto anual de la entidad	Afectación importante del MA que requiere de X años de recuperación
Catastrófico	5	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X% de la población	Afectación del X% del presupuesto anual de la entidad	Afectación muy grave del MA que requiere de X años de recuperación

Fuente: estrategia de Gobierno en línea (GEL) dentro del marco del MSPI

6.5.1.2 Criterios de Valoración de Probabilidad

Para la definición de escalas o criterios de probabilidad se debe tomar como referencia la metodología de riesgos del DAFP y en general las buenas prácticas de riesgos que se sugieren una escala de cinco niveles como se muestra a continuación:

Tabla 2. Criterios de valoración de probabilidad de acuerdo con la información

CRITERIOS DE VALORACION DE PROBABILIDAD DE OCURRENCIA			
Nivel asignado	**Valor de la probabilidad**	**Frecuencia del evento**	**Posibilidad de ocurrencia del evento**
Raro	1	La situación se ha presentado al menos cada diez años	La situación puede suceder al menos cada diez años
Improbable	2	La situación se ha presentado al menos una vez cada año	La situación puede suceder al menos una vez cada año
Posible	3	La situación se ha presentado al menos una vez cada semestre	La situación puede suceder al menos una vez cada semestre
Probable	4	La situación se ha presentado al menos una vez al mes	La situación puede suceder al menos una vez al mes
Casi seguro	5	La situación se ha presentado al menos una vez a la semana	La situación puede suceder al menos una vez a la semana

Fuente: estrategia de Gobierno en línea (GEL) dentro del marco del MSPI

6.5.1.3 Zonas de Riesgos

Las zonas de riesgo que se consideran para esta guía, y según lo dispuesto por el DAFP, en los cinco niveles de impacto y en los cinco niveles de probabilidad (donde veinticinco es el mayor valor) son los siguientes:

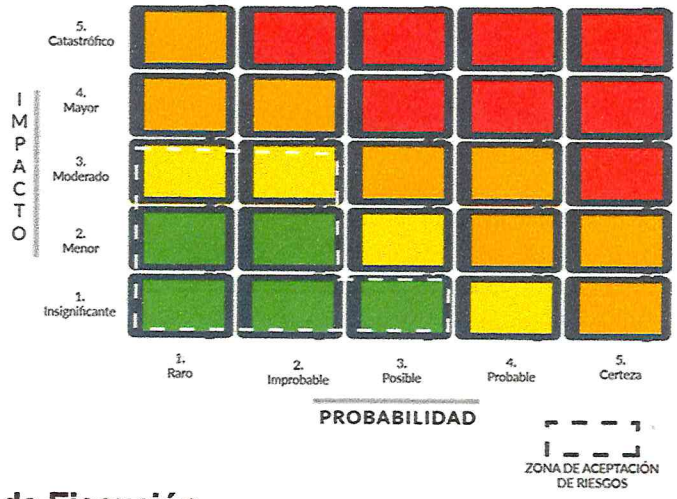
Tabla 3. Zonas de Riesgos de acuerdo a combinación de impacto y probabilidad

ZONA DE RIESGOS DE ACUERDO A LA COMBINACION DE IMPACTO Y PROBABILIDAD		
Zona de riesgo	Valor asignado	Acción requerida
Extremo	Mayor o igual a 15 y hasta 25	Requiere acciones inmediatas para evitar la materialización de los riesgos asociados a la seguridad digital
Alto	Mayor o igual a 9 y menor de 15	Requiere acciones rápidas, a corto plazo, por parte de la alta dirección para disminuir los riesgos asociados a la seguridad digital
Moderado	Mayor o igual a 4 y menor de 9	Requiere medidas a mediano plazo y adecuadas, que permitan disminuir los riesgos asociados a la seguridad digital
Bajo	Menor de 3	Requiere monitoreo y seguimiento a través de actividades propias de la entidad y preferiblemente de acciones de detección y prevención

Fuente: estrategia de Gobierno en línea (GEL) dentro del marco del MSPI

6.5.1.4 Apetito del Riesgo

La combinación de impacto y probabilidad estará representada por unos intervalos de valor y una descripción que establece a su vez una representación gráfica lo que se ha denominado en el contexto de la gestión de riesgos, "mapa de calor".



6.6 Fase de Ejecución

La Gobernación de Norte de Santander cada vez más consiente de los riesgos del mundo digital actual, ha venido implementado controles y procesos que ayudan en la mitigación de los mismo logrando de esta manera que exista una reducción de los riesgos a los cuales puedan estar expuestos los activos de información en el entorno cibernético o digital.

Actualmente se desea crear e implementar una ruta definida para la aplicación de controles, los cuales deberán estar a cargo de su aplicación en los tiempos definidos, los responsables o líderes de macro proceso o procesos con el apoyo de la Secretaria de las Tecnologías de la Información y Comunicaciones en lo relacionado a controles tecnológicos.

6.6.1 Identificación de los Activos de Seguridad Digital

Se identifican los activos de información, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores.
En la gestión de valoración del activo, se consideran los siguientes aspectos:

TIPOS DE ACTIVOS	DESCRIPCION
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios.
Datos/ Información	**Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012).
Hardware / Infraestructura	**Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Software / Aplicaciones Informáticas	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.
Servicios	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores
Soportes de Información	**Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).
Claves Criptográficas	**Esenciales para garantizar el funcionamiento de los mecanismos criptográficos.** Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación. Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.

TIPOS DE ACTIVOS	DESCRIPCION
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones}	Lugares donde albergan los sistemas de información y comunicaciones

Teniendo en cuenta lo anterior, para la fase de identificación de activos de información, se tomará como base de referencia el catálogo de servicios tecnológicos publicado en plataforma web institucional llamado CATÁLOGO_SERVICIOS_TI_V2.pdf.

6.6.2 Identificación de los 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, destinara recursos para la adquisición e implementación de controles de tipo tecnológicos, procedimentales y operaciones, minimizando de esta forma la exposición a peligros en el contorno digital que pueden afectar la integridad, confidencialidad y disponibilidad de la información.
De igual manera una actividad previa que es necesaria para la identificación de riesgos de seguridad digital consiste en tener consolidado y clasificado los activos de información de la entidad de acuerdo a los atributos de confidencialidad, integridad y disponibilidad que defina el grado o nivel de criticidad que poseen los activos para la entidad, por esta razón la Gobernación deberá diseñar la estrategia necesaria para catalogar el grado de criticidad de los activos de información de la entidad.

En esta etapa se identifica las fuentes que puedan estar originando estos riesgos, así como factores internos o externos por los cuales se presentan las vulnerabilidades y amenazas, de esta forma haciendo uso de conceptos profesionales, juicios de expertos y analizando los posibles escenarios. Es necesario lograr identificar los posibles iniciadores de estas causas, así como la descripción de los riesgos y las situaciones o consecuencias que se presentan producto macro procesos y procesos de la Gobernación de Norte de Santander. Por esto, estas actividades deben ser enfocadas a los riesgos potenciales que ocasionen un impacto negativo sobre la ejecución de los objetivos de los macro procesos estratégicos, misionales, de soporte y evaluación.

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.

A continuación, se muestran los riesgos agrupándose de la siguiente forma:

IDENTIFICACION DEL RIESGO				
TIPO	**Nº**	**RIESGO**	**CAUSAS**	**CONSECUENCIAS**
RIESGO POR INCIDENCIA EXTERNA	1	Desastre natural	A este riesgo estamos expuestos, en caso de incendio, terremoto, tormenta eléctrica, etc.	Destrucción parcial o total de la infraestructura, Interrupción de los servicios (luz eléctrica, internet, telefonía celular y fija).
	2	Interrupción del fluido eléctrico	Fallas en el fluido eléctrico de la red regulada o No regula.	Afectación de equipos eléctricos normales y fallas en los servicios de tecnología de información.
	3	Cambio en Normatividad Externa (leyes, decretos, ordenanzas y acuerdos)	desconocimiento o desacato de la normatividad legal y obligaciones contractuales.	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad e investigaciones disciplinarias.
RIESGO POR INCIDENCIA INTERNA	4	Pérdida o Robo de Información Digital	Falla en la seguridad de la información digital de cada uno de los procesos de la Gobernación (Intrusos ilegales, piratería informática, empleados mal intencionados, espionaje para intereses particulares).	Suspensión en la prestación de servicios que brindan cada una de las secretarias de la entidad.
	5	Falla de equipos electrónicos	Todo equipo electrónico es susceptible a fallos (falta de mantenimiento, vida útil del equipo) en cualquier momento.	Se paralizan los procesos y servicios que prestan cada una de las secretarias de la Entidad.
	6	Falla en servidores	Fallas de hardware, configuración y/o software, Fallo del suministro eléctrico, Falla en Cableado, Falla en Router/Switch, Fallo en la conexión a Internet, Error humano.	Interrupción de los aplicativos misionales y suspensión en la prestación de servicios de cada secretaria de la Gobernación
	7	Virus informáticos	Falta de software, antivirus y protocolos de seguridad digital.	Desactualización de paquetes de seguridad de sistemas operativos y perdida de información.
	8	Calentamiento del Data Center:	Falta de mantenimiento preventivo y correctivo de los equipos que conforman el data center y los aires acondicionados.	Demora en ejecución de aplicativos misionales y servicios tecnológicos.
	9	Copias de seguridad sistemas de información	Falta de aplicación de la política de seguridad y privacidad de la información de la Gobernación.	Perdida de información de las bases de datos de la Entidad y perdidas económicas.
	10	Falta de planeación e inversión de recursos para infraestructura tecnológica.	La no adquisición o destinación de un recurso económico, para la adquisición de nuevas tecnologías	Paralización de los servicios que presta la Gobernación a su cliente externo. Herramientas no aptas para el desarrollo de actividades misionales de la Entidad.

IDENTIFICACION DEL RIESGO				
	11	Atraso en adquisición, actualización y mantenimiento de la Infraestructura tecnológica y nuevas tecnologías.	fallas en la planeación y ejecución del proceso contractual de proyectos para adquisición de nuevas tecnologías (Licencias antivirus, proveedor de internet, mantenimiento preventivo y correctivo de equipos, licencia administración de máquinas virtuales, sistemas de información).	Perdida de soporte de software adquirido, lentitud en el desarrollo de las actividades, funciones y servicios que prestan o apoyan cada uno de los funcionarios de la entidad.
	12	Equivocaciones humanas	Falta de capacitaciones de personal de la Entidad, Problemas ajenos y personales de funcionarios	Perdida de información digital, perdidas económicas, suspensión en ejecución de procesos misionales, fallas en atención a usuario.
	13	Activos de información desactualizados	No documentación de activos y catálogo de servicios tecnológicos dentro de la arquitectura TIC	Perdida de información y no horizonte institucional en cumplimento de objetivos
	14	Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso	Equipos de red no configurados de acuerdo a políticas de seguridad y privacidad de información digital y vulnerabilidad de acceso por diseño de topología de red.	Conexión de internet fraudulenta, ataque cibernético, perdida de información digital.

6.6.3 Valoración de Riesgos de Seguridad Digital

En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, impacto y probabilidades de los riesgos.

IDENTIFICACION DEL RIESGO		CALIFICACION DEL RIESGO			
Nº	RIESGO	PROBABILIDAD	IMPACTO	EVALUACION DEL RIESGO	CRITERIOS DE IMPACTO
1	Desastre natural.	1	5	5	I,D,C,S,E,A
2	Interrupción del fluido eléctrico.	3	4	12	I,D
3	Cambio en Normatividad Externa (leyes, decretos, ordenanzas y acuerdos).	3	3	9	S,E
4	Pérdida o Robo de Información Digital.	2	4	8	I,D,C,S,E

5	Falla de equipos electrónicos.	4	2	8	I,D,S,E
6	Falla en servidores.	1	5	5	I,D,C,S,E
7	Virus informáticos.	4	2	8	I,D,C,S,E
8	Calentamiento del Data Center.	1	4	4	I,D,C,S,E
9	Copias de seguridad sistemas de información	2	4	8	I,D,C,S,E
10	Falta de planeación e inversión de recursos para infraestructura tecnológica.	2	4	8	I,D,C,S,E
11	Atraso en adquisición, actualización y mantenimiento de la Infraestructura tecnológica y nuevas tecnologías.	2	4	8	I,D,E
12	Equivocaciones humanas.	5	1	5	I,D,C,S,E
13	Activos de información desactualizados	2	2	4	I,D,C,S,E
14	Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso	4	1	4	I,C,E

Matriz de riesgos Inherentes

La matriz de riesgos es una confrontación analítica de los posibles riesgos a los que se encuentra sometida el área tecnológica, este análisis nos permitirá evaluar la probabilidad de ocurrencia de los distintos riesgos para diseñar los controles preventivos y correctivos, los que se considera más críticos y causan más impacto para la gobernación de Norte de Santander.

A continuación, se relaciona matriz de probabilidad e impacto de los riesgos relacionados con el tipo de activos para identificar los riesgos inherentes de seguridad digital.

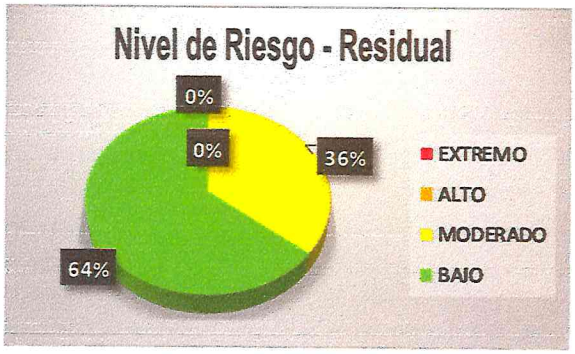
PROBABILIDAD DE IMPACTO

PROBABILIDAD DE OCURRENCIA

Probabilidad \ Impacto	1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrofico
1 Raro	0 BAJO	3 BAJO	5 MODERADO	0 ALTO	0 ALTO
2 Improbable	0 BAJO	3 BAJO	0 MODERADO	0 ALTO	0 EXTREMO
3 Posible	3 BAJO	0 MODERADO	0 ALTO	0 EXTREMO	0 EXTREMO
4 probable	0 MODERADO	0 ALTO	0 ALTO	0 EXTREMO	0 EXTREMO
5 Casi Cierto	0 ALTO	0 ALTO	0 EXTREMO	0 EXTREMO	0 EXTREMO

TOTAL	BAJO	MODERADO	ALTO	EXTREMO
	8	6	0	0

DISTRIBUCION DE RIESGOS - RESIDUAL	
ZONA DE RIESGO	TOTAL
EXTREMO	0
ALTO	0
MODERADO	5
BAJO	9
TOTAL	14



6.6.4 Identificación y Evaluación de los Controles Existentes

La Secretaria de las Tecnologías de la Información y Comunicaciones ha realizado su mayor esfuerzo para evaluar sobre la efectividad de los controles, lo cual le ha permitido concluir que es necesario la inversión o destinación de recursos para la adquisición de soluciones tecnológicas de seguridad que mejoran la protección del Data Center y los activos que se encuentran expuestos a diferentes tipos de riesgos a través de la Web.

Se realizó el análisis que definió la metodología de estimación del riesgo asignando, valores a la probabilidad de que se materialice alguna amenaza, afectando la seguridad de los activos de información, al igual que el impacto que puede afectar a la entidad producto de la materialización de los riesgos.

Se describen controles para establecer, desarrollar estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas; los cuales se resumen a continuación:

MITIGACION DE RIESGOS Y CALIFICACION					
Riesgos	**Mitigación**	**P**	**I**	**E.R**	**C.I**
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	3	I,D,C,S,E,A
Interrupción del fluido eléctrico	La Gobernación cuenta con respaldo de una planta eléctrica en caso de fallas en fluido eléctrico, adicionalmente existe banco de UPS que respaldan el Data Center durante 3 horas de interrupción de fluido eléctrico.	3	1	3	I,D
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 a las recomendaciones y politicas de Gobierno Digital de MINTIC, quien enfoca el diseño, planificación e implementación de politicas de seguridad digital en la Gobernacion.	3	1	3	S,E
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 lectores de huella para entrada de personal en el edificio, y planes de contingencia de seguridad interna.	2	2	4	I,D,C,S,E
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	4	I,D,S,E

MITIGACION DE RIESGOS Y CALIFICACION					
Riesgos	**Mitigación**	**P**	**I**	**E.R**	**C.I**
Falla en servidores.	La Gobernación contrata profesionales que prestan los servicios de administración de los servidores para actuar ante cualquier falla.	1	3	3	I,D,C,S,E
Virus informáticos.	La Gobernación contrata profesionales que interactúan en la configuración de los equipos, de acuerdo con políticas de seguridad y privacidad de información. Además se cuenta con licencias de antivirus para protección de equipos en tiempo real y servicio de firmware para contrarrestar amenazas externas.	3	1	6	I,D,C,S,E
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	2	I,D,C,S,E
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	2	I,D,C,S,E
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 inversión que sobre la materia de arquitectura TIC, sistemas de información e infraestructura tecnológica adelantan todas las dependencias de la Entidad.	1	3	3	I,D,C,S,E
Atraso en adquisición, actualización y mantenimiento de la Infraestructura tecnológica y nuevas tecnologías.	La Gobernación, tiene gran prioridad en los planes de compra anuales, contando con personal capacitado en la coordinación y desarrollo de trámites administrativos internos y con proveedores.	1	3	3	I,D,E

MITIGACION DE RIESGOS Y CALIFICACION					
Riesgos	**Mitigación**	**P**	**I**	**E.R**	**C.I**
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. Además, desde el área de las TIC, se realizan copias de seguridad diarias con el fin restaurar la información, ante cualquier perdida o daño.	1	3	3	I,D,C,S,E
Activos de información desactualizados.	En trabajo conjunto, Secretaria Tic y oficina de archivo, adelantan acciones bajo el macro proceso de Gestión Documental de la Gobernación, para planear la gestión y clasificación de activos de información.	1	2	2	I,D,C,S,E
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 para establecer lineamientos de adopción del protocolo IPV6, y así estar a la vanguardia del nuevo protocolo a implementar en el país. Igualmente se esta modernizando la arquitectura de red en todas las secretarías de la Entidad.	2	2	6	I,C,E

Matriz de riesgos Residual

Una vez evaluados los controles, se calculó la probabilidad y el impacto para determinar el riesgo residual. La calificación del control determina si se disminuyen o no los niveles de probabilidad e impacto. De ser así, el riesgo inherente se desplaza en el mapa de calor y se obtiene el riesgo residual.

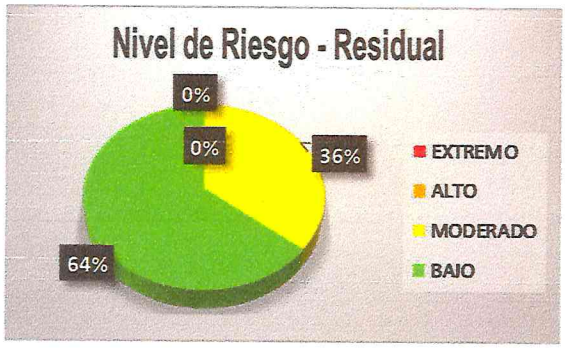
PROBABILIDAD DE IMPACTO

PROBABILIDAD DE OCURRENCIA

Probabilidad \ Impacto	1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrofico
1 Raro	0 BAJO	3 BAJO	5 MODERADO	0 ALTO	0 ALTO
2 Improbable	0 BAJO	3 BAJO	0 MODERADO	0 ALTO	0 EXTREMO
3 Posible	3 BAJO	0 MODERADO	0 ALTO	0 EXTREMO	0 EXTREMO
4 probable	0 MODERADO	0 ALTO	0 ALTO	0 EXTREMO	0 EXTREMO
5 Casi Cierto	0 ALTO	0 ALTO	0 EXTREMO	0 EXTREMO	0 EXTREMO

TOTAL	BAJO	MODERADO	ALTO	EXTREMO
	8	6	0	0

DISTRIBUCION DE RIESGOS - RESIDUAL	
ZONA DE RIESGO	TOTAL
EXTREMO	0
ALTO	0
MODERADO	5
BAJO	9
TOTAL	14



6.6.5 Tratamiento de los Riesgos de Seguridad Digital

En atención a la valoración de los riesgos de seguridad digital realizada, se determinarán las posibles acciones para tratar los riesgos a través de políticas que permitan controlar y hacer seguimiento sobre la gestión, implementando estrategias de tratamiento en donde se tomen las decisiones necesarias para mitigar, eliminar, o asumir los riesgos. En razón a esto, las formulaciones de políticas deberán contemplar los objetivos a alcanzar, una estrategia de cómo se desarrollarán las políticas a corto y mediano plazo, indicando a qué riesgos se les debe dar prioridad y control, de igual forma definir los recursos necesarios y finalmente hacer seguimiento a la efectividad de las políticas de administración de riesgos de seguridad digital definidas. Se definirá el documento de Plan de tratamiento de riesgos de seguridad y privacidad de la información.

6.7 Fase de Monitoreo y Revisión

Determinando que los orígenes y tipos de riesgos son variables, el seguimiento continuo es importante para determinar alguna variación hacia cualquier activo de la información, nuevos macro procesos o procesos, ya que puede existir la aparición de nuevas amenazas que afecten los sistemas de información y así acarrear nuevas vulnerabilidades, incrementando el impacto en la entidad.

6.7.1 Registro y Reportes de Incidentes de Seguridad Digital

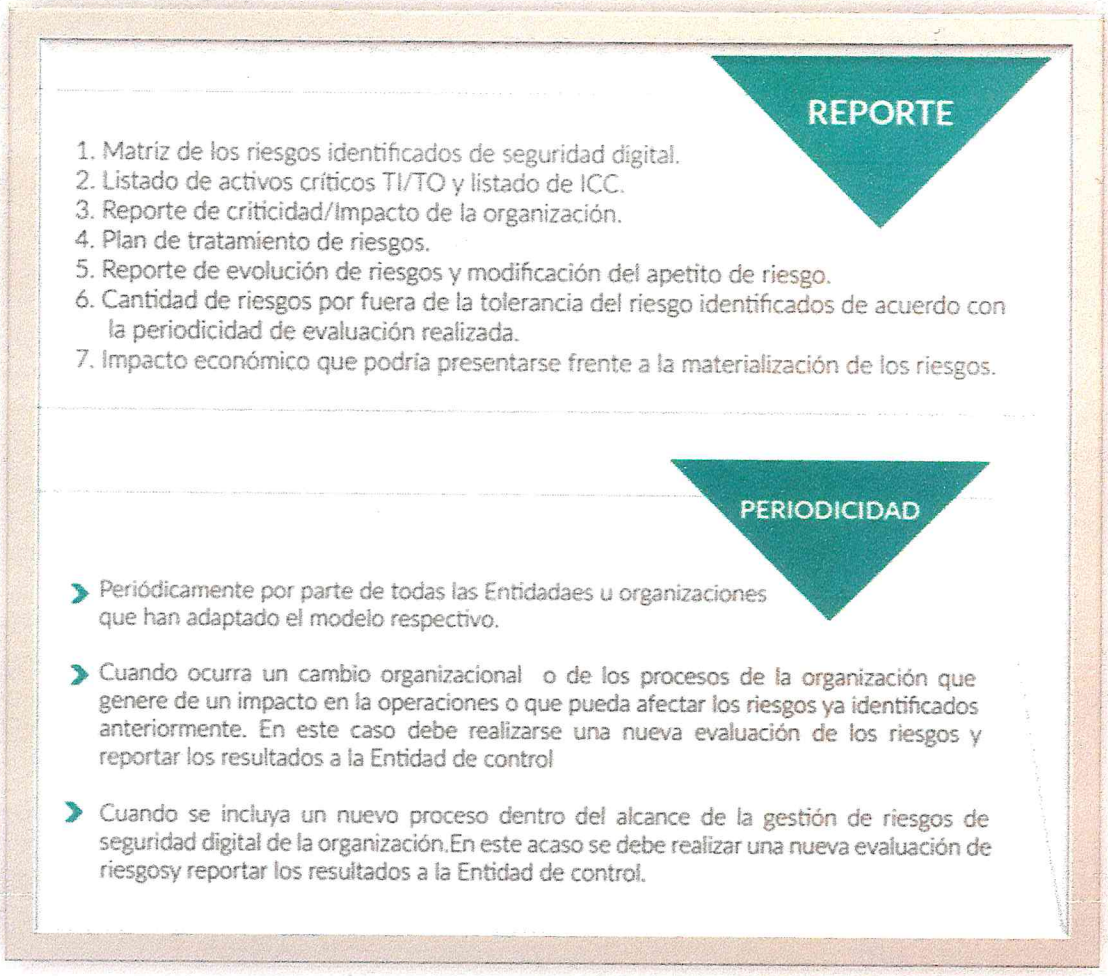
Actualmente la Secretaria de las Tecnologías de la Información y Comunicaciones le ha dado el respectivo manejo a los incidentes que han afectado la seguridad digital en la entidad, minimizando su impacto por lo que hasta el momento no se ha visto o no ha sido necesario realizar reporte al Centro Cibernético Policial y al Equipo de Respuesta a Incidentes de Seguridad Informática **CSIRT.** Pero en atención a todo lo anterior expuesto, durante esta y las anteriores etapas se trabajará mancomunada para para detectar cualquier tipo de incidente de seguridad digital de manera anticipada, se es indispensable la realización de un diagnóstico de incidentes, con el fin de implementar estrategias para contener y minimizar del impacto que estos puedan generar. Se deberá trabajar de manera conjunta con los usuarios, líderes de proceso, Secretarios de Despacho y la Secretaria de las Tecnologías de la Información y Comunicaciones, para la reparación de los activos de información impactados y como accione de mejora para evitar futuros incidentes, se evaluará la posible causa y se implementaran mejoras y revisiones que ayuden a la protección de los distintos activos de información.

Se deberá reportar de manera oportuna a las entidades competentes la afectación causada por los incidentes de modo que se pueda recibir colaboración por parte de dicha Entidad.

6.7.1.1 Reporte de la Gestión de Riesgos de Seguridad Digital al Interior de la Entidad

La Gobernación de Norte de Santander implementara estrategias de comunicación y administración de los riesgos de seguridad digital asignando responsables, acciones, controles y orientación sobre los riesgos que se deban tratar.

Imagen 4 Reporte de Información



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

La imagen anterior detalla las actividades necearías para realizar el reporte y la periodicidad con que se deberá llevar a cabo los reportes de información.

6.7.1.2 Reportes de la Gestión de Riesgos de la Seguridad Digital a Autoridades o Entidades Especiales

La Gobernación de Norte de Santander y encargados de los riesgos de seguridad digital reportaran de manera oportuna a las entidades competentes, con el único objetivo que esta información pueda servir y/o contribuir con el Gobierno Nacional a mejorar la seguridad de la información en el ámbito cibernético y digital.

6.7.2 Auditorías Internas y Externas

Control Interno se debe encargar de realizar seguimiento a las acciones de mejora para lograr una oportuna y efectiva gestión de riesgos de seguridad digital y se permita de esta manera proteger los activos de información de la Entidad.

6.7.3 Medición del Desempeño

Se formularán indicadores que permita medir los avances realizados sobre la gestión de riesgos de seguridad digital, evaluando la eficacia de los controles dispuestos a fin de poder tomar decisiones.

6.8 Fase de Mejoramiento Continuo de la Gestión de Riesgos de Seguridad Digital

La Gobernación de Norte de Santander velara por un mejoramiento continuo en la gestión de riesgos de seguridad digital, de esta manera minimizando las debilidades, amenazas, riesgos, incidentes que atenten contra la disponibilidad, integridad y confidencialidad de los datos e información asociada a los distintos sistemas de información y se llevaran a cabo las acciones necesarias para tener en cuenta hallazgos y no conformidades que pudieran ser resultado de auditorías internas y externas.

MARINA LOZANO ROPERO
Secretaria de Tecnologías de la Información y Comunicaciones

ELABORADO POR:
ING CHRISTIAN ALFONSO SARAVIA URIBE
Secretaria de Tecnologías de la Información y Comunicaciones

Colaboradores:

JE LUIS RAGUA
ING DE SISTEMAS

YORYIN ALFONSO BECERRA REYES
ING DE SISTEMAS