PLAN DE GESTION DE INCIDENTES

GOBERNACION DE NORTE DE SANTANDER

SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

AVENIDA 5 CALLES 13 Y 14 PALACIO DE LA GOBERNACIÓN
TEL. 5755656 - 5710510 - FAX: 5710290
www.nortedesantander.gov.co

Contenido

1 INTRODUCION

La Gobernación de Norte de Santander con el fin de proteger todos los activos de información, los cuales son imprescindibles para el desarrollo y/o mejoramiento continuo de cada uno de los procesos existentes en la Entidad.

Actualmente la entidad cuenta con una Política se Seguridad y Privacidad de la información ha implementado políticas de seguridad de la información que busca "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." Y así poder minimizar los riesgos que puedan llegar a afectar de cualquier manera a la entidad.

Para la elaboración del Plan de Gestión de Incidentes de la Gobernación de Norte de Santander, se tomó como la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, la cual fue dispuesta por el Ministerio de las TIC.

2 OBJETIVO GENERAL

Implementar lineamientos que permita a la Gobernación de Norte de Santander estar en capacidad de detectar, evaluar, atender y/o responder de manera adecuada ante la materialización de algún incidente de seguridad de la informacion que afecte cualquier servicio que preste la entidad, mitigando de esta manera cualquier daño que puedo llegar a sufrir los equipos tecnológicos y sistemas de información.

3 OBJETIVOS ESPECIFICOS

- ✓ Definir roles y responsabilidades dentro de la entidad como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.
- ✓ Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- ✓ Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- ✓ Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.
- ✓ Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objetivo incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.
- ✓ Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
- ✓ Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
- ✓ Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.

4 ROLES Y RESPONSABILIDADES

La Gobernación de Norte de Santander creo el equipo de trabajo de arquitectura empresarial (Resolución Nº 0010 del 27 de marzo de 2019), que por las características de conformidad de este grupo hará las veces y asumirá las responsabilidades y/o funciones de **CSIRT (Computer Security Incident Response Team)** el cual estará encargado de definir los procedimientos de atención a los incidentes de seguridad de la información que se presenten en los sistemas y/o plataformas tecnológicas de la entidad, realizar la respectiva atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y de esta manera realizar retroalimentación de nuevos incidentes y/o vulnerabilidades que se puedan presentar y poder minimizar cualquier tipo de evento que nos pudiera afectar.

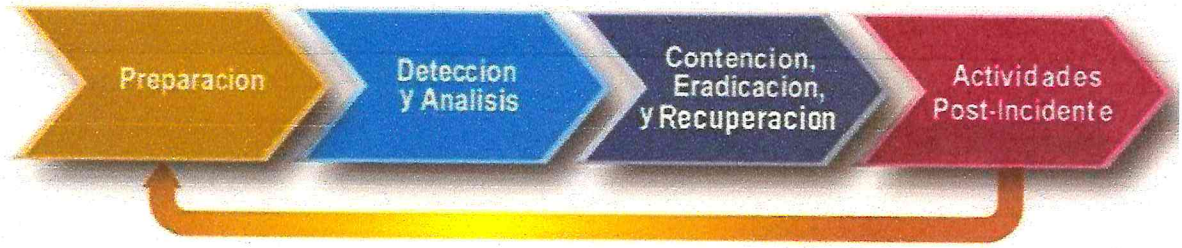
Sus principales funciones serán las siguientes:

- ✓ Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- ✓ Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- ✓ Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- ✓ Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
- ✓ Auditoria y Trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- ✓ Certificación de Productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- ✓ Configuración y Administración de Dispositivos de Seguridad Informática: Se encargaran de la administración adecuada de los elementos de seguridad informática.
- ✓ Clasificación y Priorización de Servicios Expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- ✓ Investigación y Desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección

- Secretario(a) de Tecnologías de la Información y Comunicaciones
- Secretario(a) de Planeación y Desarrollo Territorial
- El profesional master web de la Gobernación de Norte de Santander
- Los ingenieros de sistemas, electrónicos y/o 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 secretarias y oficinas de la entidad.
- Los líderes de las áreas funcionales y de procesos, cuando asi se requiera su participación.

5 GESTION DE INCIDENTES

Imagen 1 Etapas de la Gestión de Incidentes



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Guía Gestión de Incidentes)

para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

5.1 Preparación

En esta etapa es importante para la entidad tener en disposición el recurso tanto humano como económico y herramientas tecnológicas idóneas para la debida atención de incidentes, y de esta manera dar un cubrimiento a las demás etapas del ciclo de vida del mismo, creando y validando los procedimientos necesarios y programas de capacitación.

En esta etapa es importante el total apoyo de la Secretaria de las Tecnologías de la Información y Comunicación quien haga sus veces, incluyendo las mejores prácticas para el aseguramiento de redes, sistemas, aplicaciones y todas las herramientas tecnológicas de la entidad.

- **Gestión de Parches de Seguridad:** La Gobernación de Norte de Santander, garantizara las herramientas necesarias para que los administradores de los sistemas de información y herramientas tecnológicas por medio de las cuales puedan gestionar vulnerabilidades esto con el objetivo de identificar, adquirir, probar e instalar los parches.

- **Aseguramiento de plataforma:** La Gobernación de Norte de Santander, debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Cada uno de los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.

- **Seguridad en redes:** Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls tanto lógicos como físicos deben ser revisadas continuamente.

- **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores, equipos de usuario, redes, switches, y demás que hagan parte de infraestructura tecnológica de la entidad) debe contar con un antivirus activo y antimalware con las firmas de actualización al día.

- **Sensibilización y entrenamiento de usuarios:** Los Secretarios de Despacho, Jefes de Oficina, Altos Consejeros, Funcionarios de Planta y Contratistas de la Gobernación de Norte de Santander, incluidos los administradores de TI deben ser capacitados, sensibilizados con el fin de das a conocer las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad.

Es importante que la entidad suministre capacitaciones y/o actualización continuas para los encargados de los sistemas de información y estos a su vez deben establecer las necesidades de capacitación para las personas encargadas de la protección de los datos.

5.2 Recursos de Comunicación

Es necesario contar con la siguiente información para la oportuna atención de incidentes:

- **Información del contacto:** Se debe publicar, dar a conocer y mantener actualizada la lista de los contactos de todos los funcionarios que conforman el grupo de gestión de incidentes o quienes haga sus veces.

- **Información de escalamiento:** Información del contacto para escalar los incidentes según la estructura.

  - ✓ Información de los administradores de las distintas plataformas tecnológicas (Sistemas de Información, Servidores y Servicios tecnológicos de la entidad).

  - ✓ Información del jefe del área de recurso humano (Por si es necesario realizar acciones disciplinarias)

  - ✓ Contacto con áreas interesadas o grupos de interés (CC-CSIRT Equipo de respuesta de seguridad informática de la Policía Nacional, colCERT Grupo de respuesta se emergencias cibernéticas de Colombia).

5.3 Recursos de Hardware y Software

Para la realización de manera correcta y eficiente es importante que la Gobernación de Norte de Santander cuente con los siguientes equipos y/o elementos:

Teniendo en cuenta que la Gobernación de Norte de Santander es una entidad pública, y actualmente no cuenta con rubro destinado al manejo de incidentes digitales, se considera dejar abierta la opción de usar software licenciado (pago) o software libre.

- Portátiles forenses: Adquisición o disposición de por lo menos un portátil con el software necesario cuyas funciones sean poder realizar un scan completo de la red, puertos, equipos u cualquier dispositivo que se encuentre conectado a la red, análisis de protocolos, detección de servicios y sistemas operativos e identificación de software, que permita analizar unidades en mal estado, y así poder detectar vulnerabilidades.

- Analizadores de protocolos: Adquisición de herramienta que permita el desarrollo y depuración de protocolos y aplicaciones de red, la cual permite capturar diversas tramas de red para analizarlas ya sea en tiempo real o después de haberlas capturado.

- Software de adquisición: Actualmente se cuenta con un módulo de TNS para el manejo de activos de la entidad, donde se identifica a que funcionario está asignado cada equipo y en que secretaria y/o ubicación se encuentra.

- Software para recolección de evidencia: Este proceso de recolección de evidencias cuentas con varias opciones de software libre como (Dd, Air, entre otros) y licenciadas, de igual manera se considera que esta herramienta va de la mano con el software de análisis forense por tal manera se podrá adquirí una solución que supla estos dos componentes.

- Kit de respuesta a incidentes: este kit estará compuesto estará compuesta por el portátil forense, analizadores de protocolos, software de adquisición, software de recolección de evidencia y análisis forense.

- Medios de almacenamiento: se dispondrá de los equipos de almacenamientos necesarios, discos duros, dispositivos externos, entre otros.

5.4 Recursos para el análisis de incidentes

La secretaria de las Tecnologías de Información y Comunicaciones tendrá disponible la siguiente información para el análisis de incidentes:

- Listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Diagrama de red para tener la ubicación rápida de los recursos existentes.
- Información debidamente actualizada de servidores (nombre, IP,

aplicaciones, parches, usuarios configurados, responsables de cambios).

- Contar con el análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

5.5 Recursos para la mitigación y remediación

La Gobernación de Norte de Santander dispondrá de los siguientes medios o recursos para los respaldos de información y de esta manera minimizar y/o mitigar cualquier incidente.

- Discos Duros
- Medios Extraíbles
- Almacenamiento en la nube
- Backups en los servidores
- Se dispondrá de Backup de los sistemas de información

5.6 Detección, Evaluación y Análisis

5.6.1 Detección identificación y gestión de elementos indicadores de un incidente

Las primordiales fuentes de detección de incidentes de la entidad:

- Alertas generadas por los servidores
- Monitoreo periódico de la infraestructura
- Los ingenieros de la entidad
- Los usuarios

El reporte oportuno de los incidentes de seguridad digital permite una pronta respuesta, minimizando de esta manera la perdida de información y el tiempo de interrupción de los servicios afectados, y así obtener una restauración de los servicio de una forma rápida y adecuada.

Los usuarios líderes de los diferentes sistemas de información de la entidad está en la obligación de reportar de manera inmediata la detección de cualquier incidente, a la Secretaria de las TIC o quien haga sus veces, esto puede realizarse de manera telefónica, correo electrónico, o de manera personal.

La Secretaria de Tecnologías de la Información y Comunicaciones debe realizar revisiones periódicas del funcionamiento de todos los equipos tecnológicos y/o activos de información con el fin prevenir cualquier tipo de incidente de seguridad de la información.

Es importante contar con una serie de indicadores que alerten la ocurrencia de algún incidente:

- ✓ Caídas de servidores
- ✓ Reporte de usuarios
- ✓ Informes antivirus
- ✓ Funcionamiento anormal de los sistemas de información
- ✓ Lentitud en la red
- ✓ Intento de inicios de sesión fallidas
- ✓ Aumento de correos spam y/o malware
- ✓ Logs de los servidores
- ✓ Logs de las aplicaciones
- ✓ Otras herramientas que aporten en la identificación de los distintos incidentes

La Secretaria de Tecnologías de la Información y Comunicaciones aplicará las siguientes actividades a fin de garantizar la detección de incidentes:

- ✓ Aplicar la utilidad de visor de eventos de cada uno de los servidores del Datacenter.
- ✓ Verificar y activar el módulo de auditoria de los motores de bases de datos que apliquen.
- ✓ Verificar los intentos de registros y/o autenticaciones fallidas registradas en los logs.
- ✓ Garantizar la continuidad de las Backups de los sistemas de información.
- ✓ Aplicar acciones correctivas sobre cada uno de los incidentes.

5.6.2 Análisis

El análisis de incidentes implican otra serie de componentes, se hacen las siguientes recomendaciones:

- ✓ Tener conocimiento de las características normales a nivel de red y de los sistemas
- ✓ Los administradores de TI deben tener conocimiento total sobre los comportamientos de la infraestructura que se está administrando.
- ✓ Toda información que permita realizar análisis a los incidentes debe estar centralizada.
- ✓ Es importante efectuar correlación de los eventos, ya por medio de estos procesos se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil las causas de los incidentes.
- ✓ Para el correcto análisis de un incidente debe existir una única fuente de tiempo (sincronización de relojes).
- ✓ Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- ✓ Crear matrices de diagnóstico e información para los administradores menos experimentados.
- ✓ Analizar las causas, consecuencias y la magnitud del impacto de los incidentes hacia el normal desarrollo de los procesos, de tal manera que se minimicen las afectaciones para la confidencialidad, integridad y disponibilidad de la información.
- ✓ Determinar los posibles daños físicos que haya causado a la infraestructura tecnológica.
- ✓ Analizar la causa inicial del incidente y de esta manera poder tomar controles correctivos y así mitigar que este tipo de incidentes se repitan.
- ✓ Detectar, analizar e identificar la posible fuente de ataque y el perfil del atacante.

5.6.3 Evaluación

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad.

La severidad del incidente puede ser:

Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de la Entidad. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

Medio Impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

5.6.4 Clasificación de Incidentes de seguridad de la información

- ✓ Accesos no autorizados
- ✓ Modificación de recursos no autorizados
- ✓ Uso no apropiado de recursos
- ✓ No disponibilidad de los recursos
- ✓ Virus y/o malware
- ✓ Multicomponente
- ✓ Otros

5.6.5 Priorización de incidentes y tiempos de respuesta

Nivel de prioridad: Depende del valor o importancia dentro de la Gobernación de Norte de Santander.

Nivel Criticidad	Valor	Definición
Inferior	**0,10**	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	**0,25**	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	**0,50**	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	**0,75**	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	**1,00**	Sistemas Críticos.

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Nivel Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1,00	Impacto alto en uno o más componentes de más de un sistema de información.

Aplicando la siguiente formula obtendremos la respectiva prioridad:

Nivel de Prioridad= (Impacto actual*2,5) + (Impacto futuro *2,5) + (criticidad del sistema *5)

Una vez obtenidos los resultados se deben de comparar con la siguiente tabla para determinar la prioridad de atención:

Nivel Prioridad	Valor
Inferior	00,00 – 02,49
Bajo	02,50 – 03,74
Medio	03,75 – 04,99
Alto	05,00 – 07,49
Superior	07,50 – 10,00

5.6.6 Tiempos de respuesta

El tiempo de respuesta establecido en la siguiente tabla es aproximado al tiempo máximo para que el incidente sea atendido dependiendo del nivel de prioridad no corresponde al tiempo de solución del incidente, dado que la complejidad de la atención varía dependiendo del tipo de incidente y del activo de información impactado.

Nivel Prioridad	Tiempo de Respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 min
Alto	15 min
Superior	5 min

Que Hacer	Como hacerlo	Quien lo Hace	Cuando lo Hace
Reporte del incidente	Correo electrónico tic@nortedesantander.gov.co teléfono 5710510 Ext 1131 O de manera presencial Secretaria TIC	Secretarios de Despacho, Jefes de Oficina, Altos consejeros, personal de plana, contratistas y usuarios y/o terceros	Inmediatamente tiene conocimiento del incidente.
Registro del Incidente	Registrar los respectivos datos, en caso de poder brindar una solución inmediata, registrar o documentar dicha solución.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Momento en el que se reporta el incidente.

Identificar el tipo de incidente	Identificar el incidente de acuerdo a la tabla de clasificación, y asi determinar: Prioridad, criticidad de impacto, impacto actual, impacto a futuro.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Momento en el que se reporta el incidente.(el tiempo va de acuerdo a los calculaos de los tiempos de respuestas)
Escalar el incidente	Informar a la persona correspondiente para atender el incidente esto con el objetivo de tomar las decisiones necesarias.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Momento en el que se reporta el incidente.(el tiempo va de acuerdo a los calculaos de los tiempos de respuestas)
Medidas de contención	Aplicar las medidas correctivas según las decisiones tomadas para la debida contención del incidente	Profesionales que conforman el equipo de trabajo empresarial, que para este caso ara las veces de CSIRT	Momento en el que se reporta el incidente.(el tiempo va de acuerdo a los calculaos de los tiempos de respuestas)
Toma y manejo de evidencias	Aplicando las herramientas forenses y/o kit forense se procede a registrar toda la información concerniente al incidente, la cual debe ser almacenada y resguardada correctamente de tal forma que se garantice su confidencialidad, integridad y disponibilidad.	Profesionales que conforman el equipo de trabajo empresarial, que para este caso ara las veces de CSIRT	Una vez se hayan aplicado las medidas de contención.

Evaluar impacto	Evaluar el impacto del incidente en la infraestructura tecnológica y en la prestación de los servicios que desarrollan cada uno de los procesos. En el caso de que el impacto sea alto y/o superior afectando la confidencialidad, integridad y disponibilidad se debe reportar inmediatamente al CC-CSIRT (Equipo de respuesta a incidentes de seguridad informática de la policía nacional) y al colCERT (Grupo de respuesta a emergencias cibernéticas de Colombia)	Profesionales que conforman el equipo de trabajo empresarial, que para este caso ara las veces de CSIRT	Una vez se hayan tomado las evidencias necesarias
Delegar responsabilidades	Asignar a quien corresponda o al profesional idóneo aplicar las acciones necesarias para erradicar y/o mitigar el tipo de incidencia presentada.	Secretario(a) de las TIC.	Durante las 24 horas siguientes a la evaluación de impacto.
Disposición de logística	Asignar los recursos necesarios, físicos, tecnológicos, comunicaciones, transporte y todo aquel recurso que sea necesario para ejecutar el plan de recuperación.	Secretario(a) de las TIC	Durante las 24 horas siguientes a la evaluación de impacto
Comunicación	Informar a los funcionarios que aplican en el servicio y/o proceso el tiempo probable de suspensión del sistema de información el cual varía dependiendo del nivel de complejidad del incidente según las tablas de valoración.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Una vez se haya evaluado y clasificado tanto el incidente como el impacto.
Aplicar las acciones de recuperación	Realizar las acciones necesarias para la debida recuperación de los sistemas	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Según los tiempos de respuesta

Pruebas	Monitorear el sistema de información afectado por dos horas y hacer el debido registro.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Una vez se haya terminado la fase de recuperacion.
Comunicar el restablecimiento del servicio	Informar a los respectivos funcionarios el normal funcionamiento del sistema de información.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Una vez se hayan realizados las pruebas y todo este en su correcto funcionamiento.
Cierre del proceso	Realizar y/o concluir informe donde quede registrado la respuesta al incidente, acciones correctivas y recomendaciones preventivas para mitigar este tipos de eventos.	Profesional Universitario (Encargado de la Seguridad Informática y/o digital de la entidad) o quien haga sus veces	Una vez se hayan realizado las pruebas y todo este en su correcto funcionamiento.

5.7 Contención, Erradicación y recuperación

La Gobernación de Norte de Santander Con el fin de mitigar el impacto de los incidentes y así poder garantizar confidencialidad, integridad y disponibilidad de la información establece las siguientes acciones:

Contención: Busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura TI.

Una vez se culmine proceso de contención se debe continuar a la debida recolección de evidencia, para lo cual se hacen las siguientes recomendaciones:

- Autenticidad: El profesional encargado de recolectar la evidencia debe mantener su autenticidad, para lo cual se recomienda lo siguiente:
  - ✓ Registrar la información del entorno de la evidencia.
  - ✓ Tomar fotografías del entorno de la evidencia.
  - ✓ Tomar y registrar la evidencia.
  - ✓ Foliar y Almacenar la evidencia de forma segura.
  - ✓ Generar copias de seguridad de la evidencia.
- Cadena de custodia: Registrar detalladamente quienes, como, transporte y análisis de la información con el fin de tener a detalle cada proceso por el

cual paso la evidencia.

- Validación: Brindar las garantías necesarias que la evidencia que se recolecto sea la misma que se presente a las respectivas autoridades.

Erradicación y recuperación: Una vez el incidente haya sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

CLASIFICACION Y TRATAMIENTO DE INCIDENTES		
Incidente	**Concepto**	**Tratamiento**
Denegación del servicio	Este tipo de incidente hacen que un sistemas y/o servicio deje de operar a su capacidad normal y deje sin acceso sin acceso a los usuarios, presentando fallas como: • Demora en los tiempos de respuesta • Interrupción en el servicio • Envió masivo de miles de msj. • Ataque a través de equipos zombie • Ataques contra algunos servicios de Windows • Activación de programas que consume los recursos del equipo	• Bloquear los paquetes del ataque • Buscar nuevos canales de comunicación, servicio – usuario. • Terminar procesos no deseados en servidores • Escaneo del servicio • Restituir el servicio caído • Iniciar el servicio a su estado original

Acceso no autorizado	Consiste en intentos reales no autorizados, para hacer uso indebido del sistema, servicio o red. • Intentos fallidos de acceso a los recursos • Captura de cuentas mediante herramientas de este tipo. • Divulgación no autorizada de datos personales • Acceso físico a las instalaciones • Consultas no autorizadas • Accesos no autorizados a las bases de datos o archivos privados.	• Bloqueo de cuenta • Implementar bloqueas automáticos por intentos fallidos • Uso de contraseñas seguras • Identificar los puntos de acceso del ataque para hacer los respectivos bloqueos. • Control de acceso por firewall • Aumentar las medidas de seguridad tanto lógicas como físicas.
Modificación de recurso no autorizado	Incidente que involucra a un funcionario, sistema o código malicioso que afecta la integridad de la información. • Perdida de información • Alteración de la información • Instalación de software no autorizado	• Bloqueo de cuenta • Contrarrestar de efectos producidos • Sustituir los archivos que puedan estar corruptos • Restaurar copias de seguridad • Actualizar software
Código malicioso (virus)	Programa que tiene como fin modificar el comportamiento normal de un sistema, normalmente con fines maliciosos como robo de información, modificar o destruir información y recursos tecnológicos. • Virus informáticos • Malware	• Aislar el equipo de la red • Remover el código malicioso • Corregir los efectos producidos • Restaurar copias de seguridad (si aplica) • Mejorar las defensas • Análisis de vulnerabilidad
Vandalismo	Alteración de manera intencional a la página web, como cambios en la apariencia visual del sitio web • Ataque por inserción de scripts maliciosos • Modificación del sitio web	• Suspensión del sitio web • Aplicar herramientas de seguridad • Reparar el sitio web • Restaurar el sitio web
Daños físicos	Son los eventos y/o sucesos del entorno o naturaleza que causan daños a los equipos tecnológicos. • Fuego • Inundaciones • Daños en el hardware por fallas en las energía eléctrica	• Uso extintores • Llamar a los bomberos (si aplica) • Desconectar los equipos • Mantenimientos a los equipos afectados • Restauración de copias de seguridad • Reiniciar los equipos y entrar en funcionamiento normal

5.8 Actividades Post-incidente

Las actividades Post-incidente básicamente se componen del reporte apropiado del incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias así como el registro en la base de conocimiento para alimentar los indicadores.

5.8.1 Lecciones aprendidas

Al haberse presentado cualquier tipo de incidente es importante aprender del mismo y mejorar, con el fin de estar preparados para nuevas amenazas, mejorar la tecnología y el debido registro de todo el proceso que se realizó ya que esto nos permite conocer:

- ✓ .Exactamente lo que sucedió, en que momento y como el personal gestionó el incidente
- ✓ Los procedimientos documentados
- ✓ Si se toman las medidas o acciones que podrían haber impedido la recuperación.
- ✓ Cuál sería la gestión de personal y que deberían hacerse la próxima vez que ocurra un incidente similar.
- ✓ Acciones correctivas pueden prevenir incidentes similares en el futuro.
- ✓ Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro

Este proceso de lecciones aprendidas puede poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio.

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