PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

La Gobernación de Bolívar, cuya función misión es: "El gobierno del Departamento de Bolívar asume como su responsabilidad primigenia, la construcción de las condiciones para generar bienestar y desarrollo humano, a nivel regional y local en su territorio y comunidad, y ejercer con eficiencia, equidad y probidad la orientación del desarrollo del Departamento de Bolívar, la complementación de los esfuerzos de las administraciones locales, para la asignación de los recursos productivos entre los distintos grupos de la sociedad, involucrando a la totalidad de los actores públicos, privados y comunitarios.", en su propósito de salvaguardar la información mediante buenas prácticas de seguridad y privacidad de esta, como el activo más importante en la cuarta revolución industrial; contempla lo necesario para desarrollar un procedimiento de gestión de incidentes de seguridad informática, el cual permitirá utilizar instrumentos que minimicen el número de incidentes y el posible impacto en las actividades del manejo de la infraestructura tecnológica.

A partir de lo anterior, se analizan estándares de buenas prácticas y regulaciones como lo es, el **Modelo Nacional de Gestión de Riesgos de Seguridad Digital**; la **Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia Primera Edición**; **la "Guía de Orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público**, basada entre otros en el documento **NIST 800-30/-39** el cual establece que las entidades gubernamentales y el Sector TI tienen componente que hacen parte de las infraestructuras críticas del país. Por consiguiente, se establecen los siguientes objetivos específicos:

Objetivos

- Conformar un equipo de respuesta a incidentes y definir las responsabilidades de sus integrantes en la gestión de esos incidentes.
- Definir un procedimiento de gestión eficiente de los incidentes de seguridad desde las etapas más tempranas de tal manera que se minimice el impacto en los activos de información

Equipo de respuesta a incidentes de la Gobernación de Bolívar

Para conformar un equipo de gestión de incidentes se deben seguir las siguientes fases:

- **Fase Preparación**

  En esta fase se recogen los elementos presentes que pueden ser utilizados, se establece y capacita un Csirt (Computer Security Incident Response Team o Equipo de Respuesta a Incidentes de Seguridad Informática), se obtienen los recursos.

- **Dirección de TICs**

  El Artículo 80 del Decreto 54 de 2017 indica las funciones de la Dirección de Tecnologías de la Información y las Comunicaciones:

Artículo 80 Funciones principales de la Dirección de Tecnologías de la Información y de las Comunicaciones. Las funciones de la Dirección de Tecnologías de la Información y de las Comunicaciones, son las siguientes:

1. *Formular, orientar y coordinar la formulación del Plan Estratégico de TIC y realizar su seguimiento y evaluación;*
2. *Formular políticas encaminadas a establecer y/o mantener una plataforma informática (infraestructura de servidores, software de base, aplicativos, servicios*

informáticos de valor agregado y estaciones de trabajo) adecuada, para el normal funcionamiento de la operación de la Administración departamental;

3. *Formular las políticas de custodia, administración, backup y seguridad de la información de la Administración departamental;*
4. *Formular las políticas de administración, seguridad y control necesarias para garantizar la eficacia, eficiencia y confiabilidad de los recursos informáticos de la Administración departamental;*
5. *Formular el plan de capacitación en informática dirigido al personal de sistemas y usuarios de los servicios y recursos informáticos;*
6. *Elaborar los estudios para la adquisición de equipos y programas de informática adecuados a las necesidades de la Gobernación de Bolívar;*
7. *Coordinar y gestionar la conectividad entre los organismos del sector central, incluyendo a las Instituciones Educativas y entidades del sector descentralizado de la administración departamental;*
8. *Garantizar la seguridad informática y de los sistemas de información del sector central y entidades del sector descentralizado de la administración departamental;*
9. *Informar, gestionar y tramitar las acciones necesarias para mantener actualizada la infraestructura tecnológica de hardware que soporta la operación de la Gobernación de Bolívar;*
10. *Establecer mecanismos para la actualización del inventario de la infraestructura tecnológica que soporta la operación en la Entidad;*
11. *Establecer y verificar el cumplimiento de políticas de administración de la tecnología (servidores, software de base, aplicaciones, servicios informáticos de valor agregado y estaciones de trabajo, entre otros;*

12. *Establecer e implementar metodologías para la evaluación, instalación y mantenimiento de los componentes de la infraestructura tecnológica de la Gobernación de Bolívar;*
13. *Formular el plan de contingencia que garantice la disponibilidad de los servicios informáticos de la Gobernación de Bolívar;*
14. *Asesorar a las áreas usuarias de la entidad en la elaboración, de los procedimientos asociados a la definición y puesta en marcha de los sistemas de información implementados;*
15. *Establecer y verificar el cumplimiento de políticas de servicios informáticos de conectividad y seguridad para el transporte de la información;*
16. *Las demás que le sean propias o asignadas de acuerdo con la naturaleza de la dependencia.*

Del documento Buenas Prácticas para establecer un CSIRT nacional de la OEA el cual a su vez está basado en los trabajos del CERT, ENISA, entre otros, el objetivo con este equipo es conformar un Csirt.

Un equipo de respuesta a incidentes en seguridad informática (CSIRT por sus siglas en inglés) es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular. (SIC) Los equipos que surgieron principalmente para responder a incidentes han evolucionado y ahora con frecuencia están orientados a ser un modelo integral de gestión de seguridad de la información. (*Buenas Prácticas para establecer un CSIRT nacional. Owasp)*[1]

[1] http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Definición de interesados

Los interesados identificados en la ejecución del proyecto son:

- Gobernación de Bolívar
- Secretarías
- Direcciones
- Colcert
- Equipo de apoyo mesa de ayuda
- Usuarios internos
- Usuarios del portal
- Contribuyentes
- Ciudadanos
- Bancos
- Entes de control
- Ministerio de defensa
- Cai Virtual
- Empresas contratistas
- Desarrolladores
- Fabricantes de soluciones de seguridad

Definición del CSIRT

Csirt Gobernación de Bolívar: Se establece como una unidad en la entidad integrada por los actores interesados, responsables, encargados o titulares de los activos de información que reposan en la entidad.

Se definen las responsabilidades de los perfiles que intervienen en el proceso, las decisiones, el flujo de información, los recursos humanos asignados, los equipos de seguridad y de respaldo o recuperación.

La entidad ha establecido políticas de seguridad que controlen las acciones que se pueden realizar con la infraestructura y las que no.

El CSIRT Gobernación de Bolívar integra:

- Dirección de TICs
- Contratistas de seguridad
- Fabricantes de Seguridad
- Equipo de Soporte
- Administradores de plataformas
- Empresas Contratistas
- Desarrolladores
- Fabricantes de Infraestructura
- Profesional Universitario (Asesor(a) Legal)

El CSIRT Gobernación de Bolívar se rige por:

- Política de Seguridad informática
- Políticas de Seguridad Informática
- Legislación Colombiana Aplicable
- Disposiciones de Seguridad y Defensa Nacional

La Gobernación de Bolívar por intermedio de la Dirección de TICs asignará los recursos humanos necesarios al conformar el CSIRT Gobernación de Bolívar, tal como anualmente asigna presupuesto para nuevas adquisiciones, actualización y soporte de plataforma.

El Alcance del proyecto está determinado por los activos de información descritos en el inventario de activos de información de TI.

La Comunidad objetivo del CSIRT Gobernación de Bolívar está conformada por:

- Gobernación de la entidad.
- Secretarías.
- Usuarios internos.
- Usuarios del Portal.
- Contribuyentes.
- Ciudadanos.
- Empresas contribuyentes.

El CSIRT Gobernación de Bolívar ostenta completa autonomía para prevenir, analizar, detectar, gestionar y hacer tratamiento de todos los incidentes de seguridad informática de la entidad, además, participa en la recuperación del sistema en los casos que sea necesario.

Los documentos guías coinciden en los servicios mínimos que debe prestar el Csirt son:

- Servicios proactivos.
- Servicios reactivos.
- Servicios de gestión de calidad de seguridad. (West-Brown et al., 2003)

Servicios proactivos

Los servicios proactivos que brindará el CSIRT del Gobernación de Bolívar son:

- Anuncios.
- Monitoreo de actividades.
- Correlación de eventos.

- Reportes e informes a los interesados.
- Detección de anomalías de comportamiento.
- Publicación de alertas.
- Investigación de vulnerabilidades, amenazas, vectores de ataque (emergentes).
- Investigación del estado del arte, normas y mejores prácticas de seguridad.
- Instalación, configuración y operación de tecnologías de seguridad informática.
- Auditorías de seguridad, hacking ético, ingeniería social.
- Revisión de políticas.
- Evaluación de implementaciones.
- Evaluación de medidas.

Servicios reactivos

Los servicios reactivos que brindará el CSIRT del Gobernación de Bolívar son:

- Alertas a personal asignado.
- Detección de eventos de seguridad.
- Gestión los incidentes de seguridad de la población y alcance del proyecto.
- Análisis y gestión de vulnerabilidades de activos de información.
- Notificación y recepción de un incidente.
- Clasificación o triage determinar el tipo, el impacto potencial y la gravedad de un incidente.
- Análisis del incidente.
- Tratamiento de incidente.
- Respuesta a incidente.
- Manejo de instancias: El manejo de instancias hace referencia al manejo de elementos utilizados entre otros para realizar los ataques, en este trabajo solo se

tendrá en cuenta en la función de responder en la entrega de muestras de malware a fabricante.

- Remediación a vulnerabilidades detectadas.
- Respuesta a elementos maliciosos.

Servicios de gestión de calidad de seguridad

Los servicios de gestión de calidad que brindará el CSIRT del Gobernación de Bolívar son:

- Capacitación, educación, concientización y entrenamiento.
- Análisis de riesgos y continuidad de negocio.

EL CSIRT de la Gobernación de Bolívar se organiza como Equipo de respuesta a incidentes centralizado, hay un equipo responsable de la gestión y respuesta de incidentes de seguridad definido con personal dedicado y capacitado en seguridad informática y respuesta a incidentes de seguridad.

Funciones y responsabilidades

Las funciones y responsabilidades definidas para el CSIRT son:

Director(a): La dirección está a cargo del (la) Director(a) de TICs, quien tiene las funciones de:

- Dirigir y supervisar las actividades del CSIRT.
- Informar a la alta dirección.
- Autorizar acceso a la información de incidentes.
- Autorizar información de incidentes a publicar.
- Asistir o delegar miembro al Consejo de seguridad informática.
- Informar sobre el CSIRT.

- Apoyar en la gestión y tratamiento de incidentes.
- Gestionar recursos para el proceso de manejo de incidentes.

Gestor de incidentes: Profesional universitario /Especializado de la dirección de TICs, quien tiene las funciones de:

- Recibir información inicial.
- Analiza registros.
- Analizar incidentes.
- Coordinar gestión y respuesta a incidentes.
- Proyectar comunicaciones.
- Colaborar con otros Csirt.
- Custodiar registros.

Profesional Especializado de dirección de TICs: Quien tiene las funciones de:

- Apoyar en la gestión y tratamiento de incidentes.
- Establecer políticas de seguridad informática.
- Informar sobre temas de seguridad y controles.
- Establecer controles de seguridad.
- Entregar sistemas de alertas.
- Gestionar vulnerabilidades.
- Autorizar procedimientos.
- Asignar recursos.
- Realizar consultoría de controles.
- Enseñar temas de seguridad informática.

Analista: Ingeniero de la mesa de ayuda, quien tiene las funciones de:

- Monitorear soluciones de seguridad y elementos controlados.
- Implementar controles de seguridad.
- Instalar, configurar y operar soluciones.
- Monitorear tratamiento de incidentes.
- Investigar tratamientos de incidentes.
- Documentar tratamiento de incidentes.
- Detectar vulnerabilidades.

Contratista de Infraestructura: Ingeniero de la mesa de ayuda de Servidores, Telecomunicaciones o Soporte, quienes tienen las funciones de:

- Monitorear soluciones infraestructura.
- Implementar soluciones infraestructura.
- Instalar, configurar y operar soluciones infraestructura.
- Apoyar la gestión y tratamiento de incidentes.
- Remediar vulnerabilidades.

Agentes que intervienen en el manejo de un incidente son:

- Profesionales Dirección TICs
- Contratista Infraestructura
- Director de TICs
- Usuario final
- Legal

Las políticas de seguridad Informática, infraestructura y marco legal nacional aplican para el CSIRT, la información confidencial y sensible debe asegurarse conforme las disposiciones legales vigentes.

Cada una de las personas involucradas en el proceso cuenta con:

- Computador personal.
- Teléfono.
- Acceso a internet.
- Servicio de correo electrónico corporativos.
- Acceso administrativo a las plataformas asignadas.
- Acceso a alertas y reportes de equipos de seguridad.
- Monitoreo de actividades en tiempo real de las plataformas asignadas.
- Sistema de tickets para incidentes, remediación de vulnerabilidades y casos.
- Acceso a servicios de almacenamiento y copias de seguridad.

El CSIRT Gobernación de Bolívar sigue políticas de retención documental establecidas por la Unidad de Gestión Documental.

Los datos personales serán tratados conforme lo ordena la Ley 1581 del 2012, la Ley 1266 de 2008 y los decretos que las modifiquen.

EL CSIRT del Gobernación de Bolívar contempla funciones de Threat Hunter o Cacería de amenazas con el objetivo de mejorar su posición ante posibles ataques, que darán como resultado perfilamiento de ataques los cuales en la medida que se vayan cumpliendo actividades anómalas se obtendrá un mejor tiempo de respuesta ante un ataque predefinido:

Threat Hunter: Del documento Scalable Methods for Conducting Cyber Threat Hunt Operations, se extrae el siguiente texto

Este marco incluye cuatro pasos específicos que se realizan de forma cíclica:

1. **Crear hipótesis:** Responde a las preguntas: ¿dónde estaría un adversario dentro de la red? ¿Cuáles serían sus objetivos? Esta hipótesis debe basarse en el análisis de riesgos, la inteligencia de amenazas y las prioridades de la organización.
2. **Investigar a través de instrumentos y Técnicas**: Las hipótesis se investigan a través de varios instrumentos y técnicas, incluidos el análisis de datos vinculados y las visualizaciones.

   Las diversas colecciones de registros permiten a los Threat Hunters examinar de manera integral la actividad en su red y correlacionar y visualizar indicadores sutiles de compromiso como son análisis de log's, análisis de red y análisis de host.
3. **Descubrir nuevos patrones y tácticas, técnicas y procedimientos (TTP):** En la práctica, esto significa detectar y combatir técnicas como los ataques de conocidos en lugar de descubrir evidencias de incidentes de las amenazas que conducen esos ataques.
4. **Informar y enriquecer los análisis:** Sirve para retroalimentar el sistema. Estos pasos describen la esencia de realizar operaciones de búsqueda de amenazas cibernéticas; sin embargo, los detalles específicos, como la planificación, la implementación y los TTP específicos, se dejan a la organización para que los determine." (*Scalable Methods for Conducting Cyber Threat Hunt Operations*)

El equipo de caza de amenazas tendrá cuatro roles clave con habilidades de apoyo y complementarias que pueden ser realizadas por dos personas:

Supervisor: Sirve como el nodo principal de comando y control responsable de la planificación y ejecución de las operaciones de búsqueda de amenazas. Este rol será desempeñado por el director.

Hunter de Host: examina los sistemas de información y los puntos finales para los indicadores de compromiso.

Hunter de red: Examinan la actividad de la red a través del flujo de la red, el análisis de paquetes y los registros de dispositivos de red.

Analista de inteligencia de amenazas: Examinará la inteligencia de amenazas de fuentes privadas y públicas e identificará las amenazas que sean relevantes para su organización. Este rol será desempeñado por el gestor de incidentes." (*Scalable Methods for Conducting Cyber Threat Hunt Operations*)

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

En la siguiente sección se representan los incidentes, los precursores o indicadores y la manera en la cual se debe proceder ante su detección.

Los precursores e indicadores se identifican según el orden que se presentan en una situación real.

El objetivo principal es determinar cuáles son los precursores e indicadores que informan que puede darse un incidente antes de que este se presente.

Las representaciones constan de los siguientes elementos:

Nombre del incidente: Es la construcción de un identificador del incidente constituido por:

Amenaza de Alto Nivel es una superclase de amenaza, indica si es una amenaza física, involuntaria, escucha, maliciosa o legal.

Amenaza es la clase amenaza.

Detalle de la Amenaza es el objeto de amenaza, indica la forma en la cual la amenaza actúa sobre el activo de información.

Tipo de incidente indica en que dimensión de seguridad es afectado el activo.

Descripción del incidente: Describe la forma como un incidente puede presentarse en la entidad ya sea porque se ha presentado en el pasado o porque se ha identificado la posibilidad ya sea por un interesado en el activo o por el equipo de cacería de amenazas.

Situación Inicial: Es una gráfica del recorrido de las actividades en la infraestructura a través de las interacciones con los activos, la cual parte de una situación normal, esto es necesario debido a que posibilita a los actores a reconocer los activos afectados utilizados en un

incidente, el orden en que son afectados, para identificar los activos que deben ser administrados en la fase de contención, se indica de verde en la gráfica que elementos permiten concluir que hay operación normal.

Precursores: indica que hay una situación en la cual podría presentarse un incidente, normalmente porque en una operación normal debe permitirse cierto grado de riesgo, esta es necesaria ya que permite comenzar a monitorear actividades que aunque están permitidas se puede concluir que podría presentarse un incidente en el futuro próximo, se indica de amarillo en la gráfica que actividades y activos son indicadores de un futuro incidente.

Indicadores: Indica que se ha presentado actividades que configuran un incidente, por lo cual es necesario iniciar el protocolo de remediación de manera inmediata, se identifican también los controles en los cuales pueden ser identificadas las actividades maliciosas.

Descripción de si son actividades intencionales, identificar si son actividades intencionales permite priorizar el incidente.

Contención: Describe las actividades automatizadas o manuales que deben ser ejecutadas para bloquear el incidente y que no aumente su impacto.

Erradicación: Describe las actividades que deben ser ejecutadas por los agentes para erradicar el incidente y establecer controles adicionales.

Recuperación: Describe las actividades que deben ser ejecutadas para restablecer el sistema a su estado inicial, de proyectan los documentos para reportear a entes de control e interesados.

Definición de incidentes de seguridad de la información

El plan General para el Tratamiento de Riesgos de Seguridad de la Información de la Gobernación de Bolívar define como Incidente "Evento único o serie de eventos de seguridad de la información no deseados o inesperados, que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información."

Señales de un incidente

Para hacer un eficiente manejo de incidentes es necesario establecer cuando se ha presentado o se está gestando uno, se debe clasificar y medir su alcance e impacto, elemento que lo detectó, entre otros.

Las señales ante un incidente son dos:

Precursor: Señal de que un incidente puede ocurrir en el futuro, se debe monitorear la actividad del objetivo.

Indicador: Señal que un incidente puede haber ocurrido o está ocurriendo.

Las soluciones que se han instalado y los controles establecidos en la entidad sirven como fuente de precursores e indicadores, como son:

- Firewall.
- WAF.
- Proxy.
- Firewall de BD.
- Antimalware.
- Antispam.

- Logs de sistemas operativos.
- Logs de dispositivos.
- Netflows.
- Soluciones de análisis de vulnerabilidades.
- Csirt de la policía.
- Usuarios internos.
- Delegados datos personales.
- Usuarios externos.

El protocolo se activa ante un precursor o indicador ya sea automatizado desde un equipo de seguridad o por un mensaje de un usuario de los cuales no se puede prescindir.

Documentación

Cuando se recibe comunicación (Precursor o indicador) sobre incidente, el **gestor del incidente** deberá revisar los datos iniciales del incidente del **formato de registro de incidentes** de un sistema de gestión tickets.

Las comunicaciones sobre los posibles incidentes se reciben por cualquiera de las personas del CSIRT por lo diferentes canales:

- Alertas automáticas de los controles.
- Registro en solución de gestión de incidentes.
- Cualquier otro medio que pueda servir para el fin.

En los casos en los cuales el reporte de incidente provenga de un usuario, la información de quien reporta permanecerá anónima en la medida que pueda representar riesgo a su integridad, como en los casos de fraude.

Todos los incidentes deben ser gestionados dentro de la entidad o transferidos cuando debe ser manejado por un externo según sea el caso.

La persona del CSIRT quien reciba la comunicación debe comunicarse con el **Gestor de incidente** personalmente, telefónicamente o por correo electrónico para darle conocimiento del posible incidente, esta persona debe confirmar que el gestor de incidente ha recibido el mensaje.

El gestor de incidente debe determinar en lo posible si el evento o incidente corresponde a una actividad accidental o deliberada.

El Gestor de incidentes verifica los datos del incidente:

- Descripción del incidente.
- Configuración del sistema afectado y datos de los otros elementos conectados.
- Cada nuevo dato relacionado con el incidente.
- Estado del incidente.
    - Registrado
    - En progreso
    - En investigación o prueba
    - Asignado a proveedor
    - Tramitado
    - Cerrado
- Reasignaciones de los incidentes y la custodia.
- Evaluación inicial de impacto.

Fase de Priorización

Los registros de incidentes automáticos realizados por las soluciones serán registrados en la solución de gestión de tickets y cuando sean categorizados por las soluciones de seguridad de nivel alto o crítico generar alerta.

El gestor de incidentes debe revisar la prioridad del ticket según el Plan General de Tratamiento de Riesgos de la Gobernación de Bolívar:

- Impacto funcional teniendo en cuenta la prioridad del activo afectado:
  - Alta
  - Media
  - Baja
- En el caso de los incidentes con datos personales, la metodología para determinar el nivel de impacto posible para los titulares:
  - Alta: Datos de menores, datos sensibles, datos de identificación, datos de ubicación.
  - Media: Datos de contenido socioeconómico.
  - Baja: Otros datos.
- Impacto en la dimensión de seguridad: Confidencialidad, la integridad y la disponibilidad:
  - Leve
  - Menor
  - Moderado
  - Mayor
  - Catastrófico

- Tipo de incidente:
  - Contenido abusivo.
  - Código malicioso.
  - Recopilación de información.
  - Intentos de intrusión.
  - Intrusiones.
  - Incidente de Disponibilidad.
  - Incidente de seguridad del Contenido de la Información.
  - Fraude.
  - Incidente por Vulnerabilidad.
  - Otro.
  - Incidente por Prueba.
- Tiempo máximo de atención a incidentes

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

- Recuperabilidad de estado óptimo después del incidente.

Entre más alto es el producto del impacto funcional y el impacto en la dimensión, mayor prioridad deberá tener para tratamiento.

Notificación del incidente

El gestor de incidentes verifica las notificaciones de alerta en el ticket y por correo electrónico según sea el caso y envía toda la información recopilada a:

- Administrador de infraestructura.
- Director(a).

Fase Contención y Erradicación

Contención

En esta subfase se evita que la amenaza siga produciendo daños.

Las actividades que se deben realizar para contener el incidente son:

1. Cambiar contraseñas de activos comprometidos.
2. Bloquear IP's de origen.
3. Termina conexiones sospechosas.

Erradicación y recuperación

En esta subfase se elimina la causa el incidente y los daños causados.

Las actividades que se deben realizar para erradicar el incidente son:

1. Bloquear y/o eliminar cuentas utilizadas.
2. Responsable realiza consultoría para indicar a Líder de área los controles a establecer adicionales. (reglas de bloqueo y acceso a activos)
3. Líder de área solicita creación de controles adicionales.
4. Analista de seguridad o desarrollador implementa controles adicionales.
5. Gestor de incidentes verifica actividades.

Función Recuperar

El documento Incident Handler's Handbook (Libro de mano de incidentes) define como la intención de esta función restaurar los sistemas afectados al entorno de producción cuidadosamente, para asegurarse de que no provocará otro incidente. Es esencial probar, monitorear y validar los sistemas que están siendo puestos nuevamente en producción para verificar que no están siendo infectados por malware o comprometidos por otros medios. (Kral, 2019)

Las actividades que se deben realizar para recuperar ante el incidente son:

1. Analistas restauran datos modificados, si aplica.

2. Asistente legal en compañía de Líder de área proyecta análisis del caso y reportan a entidades de control y judiciales.

3. Contratistas de infraestructura y seguridad validan operatividad de todos los elementos.

4. Gestor de incidentes documenta caso.

Fase Declaración

Esta fase define las actividades tendientes a informar a los interesados, entre ellos los entes de control cuando sea pertinente:

1. Gestor de incidentes proyecta informes finales según destinatario.

2. Asistente legal apoya en la proyección de los informes.

3. Asistente legal proyecta informes a entidades judiciales, disciplinarias o administrativas según sea el caso.

4. Director TIC revisa informes finales y presenta informes a los interesados.

En caso de incidentes cibernéticos graves o muy graves deberán reportar dentro de los 15 días calendario siguientes a su detección al COLCERT

1. **Información de contacto:**

1. Nombre(s) y Apellido(s)
2. País
3. Zona horaria
4. Número de Teléfono
5. Correo electrónico
6. Nombre de la Entidad (si aplica)
7. Número de Teléfono de la entidad (si aplica)
8. Número de Móvil
9. Tipo de Organización:
    a. Gobierno
    b. Privada
    c. Operador de Infraestructura Crítica
10. Tipo de Sector https://enciclopedia.banrepcultural.org/index.php?title=Sectores_econ%C3%B3micos

2. **Información del host(s) objetivo(s):**

1. Nombres de los hosts y direcciones IPs
2. Función del sistema (web server, mail server, etc.)
3. Sistema(s) Operativo(s)
4. Aplicaciones involucradas en el incidente

3. **Información del host(s) origen:**

1. Nombres de los hosts y direcciones IPs
2. Función del sistema (web server, mail server, etc.)
3. Sistema(s) Operativo(s)
4. Aplicaciones involucradas en el incidente

4. Información del Incidente:

1. Fecha y hora (Timestamp)
2. Zona horaria del Incidente
3. Tipo de Incidente:
4. Taxonomía (seleccione la clase y el tipo que aplique al incidente):

También es necesario reportar a CAI VIRTUAL de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092

Todos los incidentes que comprometan datos personales deberán ser reportados a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a su detección, indicando:

- Tipo de incidente
- Fecha en que ocurrió
- Fecha en la que se tuvo conocimiento de este
- Causal
- Tipo de datos personales comprometidos
- Cantidad de titulares afectados

Todos los incidentes que comprometan datos personales deberán ser reportados a los Titulares dentro de los 30 días hábiles siguientes a su detección, e informarles:

- El incidente de seguridad relacionado con sus datos personales las posibles consecuencias.
- Proporcionar herramientas a dichos Titulares afectados para minimizar el daño potencial o causado.

La información correspondiente a la identificación, análisis, tratamiento de incidente debe ser socializada con el delegado de datos personales de la dependencia para aprovechar su conocimiento y establecer los posibles controles para los activos.

Fase Retroalimentación

Esta fase se documenta en la base de conocimiento del sistema de gestión de casos, entregando un informe cronológico de lo sucedido.

Se programan reuniones de socialización de lecciones aprendidas (Se utilizan los espacios de grupo de trabajo), se dispone de los casos para aprender y se trabaja en la disposición a mejorar.

En las reuniones se deben responder las preguntas:

- ¿Exactamente lo que sucedió y en qué momentos?
- ¿Qué tan bien funcionaron los elementos al contener con el incidente?
- ¿Cómo se pudo mejorar el intercambio de información con otras organizaciones?
- ¿Qué medidas correctivas pueden prevenir incidentes similares en el futuro?
- ¿Qué precursores o indicadores deberían vigilarse en el futuro para detectar incidentes similares?
- ¿Qué instrumentos o recursos adicionales se necesitan para detectar, analizar y mitigar futuros incidentes?

Director TIC establece que información se puede compartir y con quien.

Si es reincidente, es necesario registrarlo en el aplicativo de gestión de tickets como **Problema** para darle el respectivo tratamiento.

Del documento Manual de Usuario del Registro Nacional de Bases de Datos RNBD se indica que se debe reportar a la sic cuando haya incidentes con bases de datos con datos personales.

Se establecerán unos indicadores mínimos como:

- Número de incidentes manejados separados por categorías.
- Tiempo inactivo por incidente.
- Tiempo de respuesta.
- Tiempo total de incidente.
- Cantidad de precursores e indicadores.