# Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos

**Presidencia de la República**
**Coordinación de Estrategia Digital Nacional**

**Secretaría de Seguridad y Protección Ciudadana**
**Guardia Nacional**

**Octubre 2021.**

Versión 1.0.7
11 Octubre 2021

# ÍNDICE

## 1. Objetivo

Establecer y operar el **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos**, que permita fortalecer la Ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país, con la finalidad de alcanzar los niveles de riesgo aceptables en la materia, contribuyendo al mantenimiento del orden constitucional, la preservación de la democracia, el desarrollo económico, social y político del país, así como al bienestar de las mexicanas y los mexicanos.

## 2. Alcance

Gestionar de forma coordinada los incidentes cibernéticos de mayor criticidad e impacto en activos esenciales de información, mediante la aplicación de procedimientos y mejores prácticas de Ciberseguridad, para la contención y mitigación de amenazas cibernéticas, a fin de mantener niveles de riesgo aceptables.

Para los fines del **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos,** a las Instituciones de la Administración Pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país involucradas, se les denominará en lo sucesivo como los "*Múltiples Involucrados*".

## 3. Introducción

La adopción de tecnologías de la información y comunicación a nivel global, ha generado un crecimiento de servicios que van desde el suministro de información hasta operaciones financieras complejas,

generando nuevos modelos de negocio que se traducen en la diversificación de las relaciones entre los gobiernos y sus habitantes, creando una dependencia cada vez mayor en algunos sectores, cuya interrupción de servicios esenciales podría ocasionar problemáticas en términos de bienestar económico, político y social.

En virtud de lo anterior, es imperante fortalecer las capacidades técnicas, operativas, de gestión de incidentes de los *Múltiples Involucrados,* a fin de mantener los niveles de riesgo aceptables en sus activos esenciales de información, a través de un protocolo que defina las acciones necesarias de preparación ante incidentes cibernéticos; la detección y manejo de incidentes de ciberseguridad, la contención, respuesta y recuperación de los servicios; así como la coordinación y el intercambio de información.

En ese orden de ideas, el presente **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos** establece las actividades para las fases de preparación, detección, respuesta y recuperación ante incidentes cibernéticos en activos esenciales de información a cargo de los *Múltiples Involucrados*.

Para la elaboración del **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos,** se han analizado diversos marcos de referencia internacionales, guías y documentos relacionados con mejores prácticas, así mismo, se han determinado como base para su aplicación las que se describen a continuación.

**Marco de Referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología (CSF NIST)**

Como metodología de aplicación, se ha establecido el marco de referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos de América (Cybersecurity Framework CSF, por sus siglas en inglés[1]) en virtud de que recopila algunas de las mejores prácticas de estándares como la Organización Internacional de Estandarización (ISO, por sus siglas en inglés) y la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés). El Marco de Referencia de Ciberseguridad de NIST permite a cualquier organización:

a) describir la postura actual de ciberseguridad
b) describir el objetivo deseado de la ciberseguridad
c) identificar y priorizar las áreas de oportunidad
d) evaluar el progreso hacia el objetivo de ciberseguridad deseado, y
e) establecer la comunicación entre las partes interesadas.

El presente Protocolo está orientado principalmente en las funciones establecidas por el CSF que comprenden:

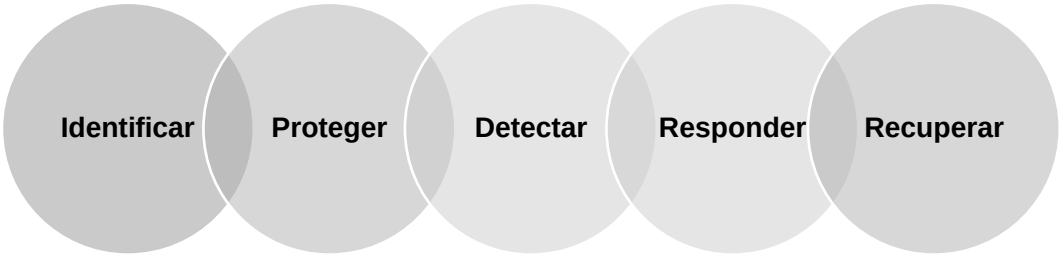


**Gráfico 1. Funciones del Marco de Referencia de Ciberseguridad de NIST.**

La fase de preparación que incluye las actividades de identificación y protección, se realizarán de manera permanente a fin de determinar y

[1] Fuente: Organización de Estados Americanos (OEA), 2018 https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

mejorar el nivel de implementación en las Instituciones de la Administración Pública Federal, y son marco de referencia y guía de colaboración con las Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país; los niveles están definidos conforme al CSF descritos a continuación:


**Gráfico 2. Niveles de implementación del Marco de Referencia de Ciberseguridad de NIST.**

**Marco para mejorar la Ciberseguridad de la Infraestructura Crítica (Framework for Improving Critical Infrastructure Cybersecurity) del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology,NIST).**

Por otra parte, la Guía para el Manejo de Incidentes de Seguridad en Cómputo, del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) Versión 1.1 del 16 de abril de 2018, permite establecer las Fases que involucran las mejores prácticas en el manejo de incidentes cibernéticos a través del ciclo de vida como se muestra a continuación:

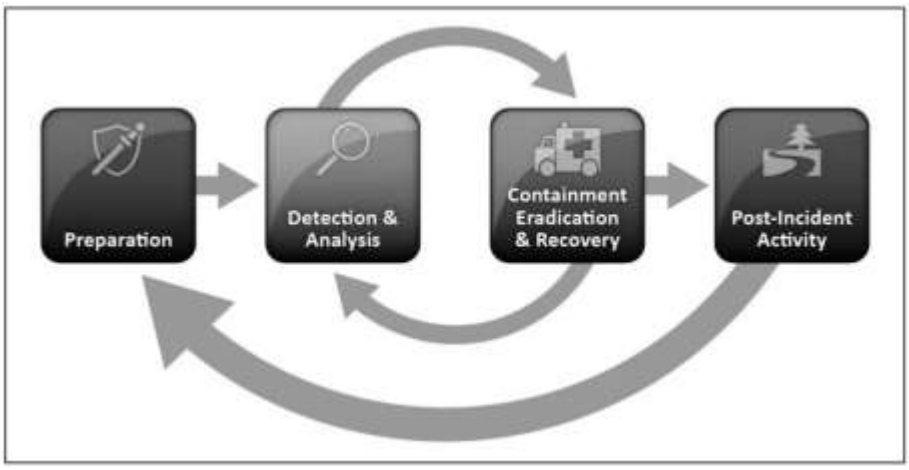


**Gráfico 3. Ciclo de vida de la respuesta a incidentes NIST 800-61.**

## Guía de Mejores Prácticas para la Gestión de Incidentes (ENISA)

Por último, la Guía de Mejores Prácticas para la Gestión de Incidentes o "Good Practice Guide for Incident Management de la European Network and Information Security Agency" (ENISA, 2010) provee los procedimientos específicos que serán aplicables para reaccionar ante un riesgo manifiesto y lograr la contención, erradicación y recuperación a fin de mantener los niveles aceptables de riesgo definidos por *Múltiples Involucrados* a cargo de Servicios de Información Esenciales en el país. En el siguiente gráfico se muestra el flujo de trabajo general durante la gestión de un incidente:

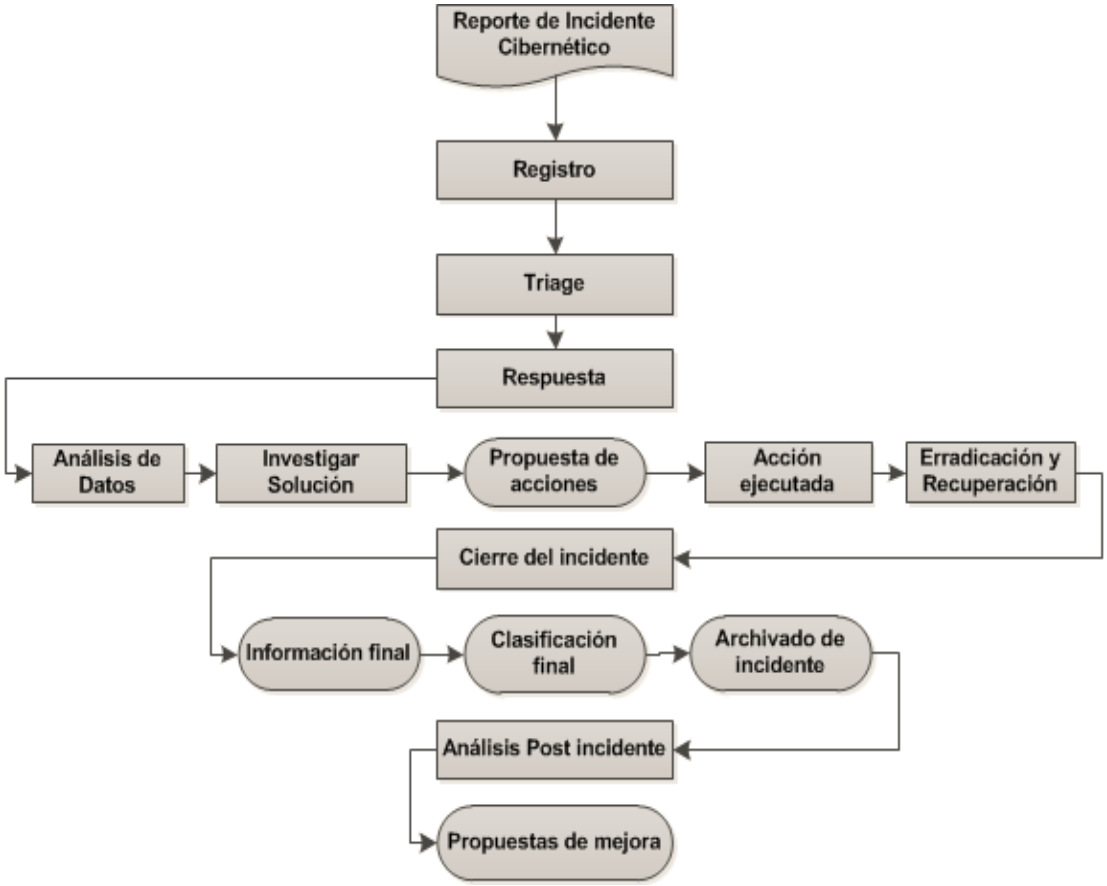


**Gráfico 4. Procedimiento general de gestión de incidentes cibernéticos de ENISA.**

# 4. Marco Jurídico

- Constitución Política de los Estados Unidos Mexicanos.
- Ley de Seguridad Nacional.
- Ley General del Sistema Nacional de Seguridad Pública.
- Ley de la Guardia Nacional y su Reglamento.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Austeridad Republicana.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley Orgánica de la Administración Pública Federal
- Reglamento de la Oficina de la Presidencia de la República
- Plan Nacional de Desarrollo 2019 – 2024.
- Programa Nacional de Seguridad Pública.
- Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024.
- Estrategia Digital Nacional 2021 - 2024
- Códigos Penales Federal y de las Entidades Federativas
- Código Nacional de Procedimientos Penales
- Acuerdo A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal

## 5. Modelo de Gobierno

El **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos**, está basado en el compromiso de los *Múltiples Involucrados* para su implementación y estará integrado por:

En lo general, hacia afuera de la Administración Pública Federal:

> **Un Grupo Coordinador** que articule los esfuerzos en materia de ciberseguridad entre los *Múltiples Involucrados*. El cual coordinará las acciones necesarias para la preparación, detección, respuesta y recuperación de incidentes cibernéticos, así como revisar periódicamente los avances e impulsar las acciones de mejora continua e intercambio permanente de información.
>
> El grupo coordinador podrá ser asistido por expertos en la materia, la industria de tecnologías de información y comunicación, así como organismos internacionales a efecto de mejorar las capacidades de los *Múltiples Involucrados* y fortalecer la toma de decisiones en materia de ciberseguridad.

En lo particular, dentro de la Administración Pública Federal:

1. El Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, establece como directriz que las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI), alineado a la política general de SI que cada Institución establezca de conformidad con sus objetivos y dimensionamiento, dicho MGSI debe conformarse entre otros elementos, por un protocolo de respuesta ante incidentes de seguridad de la información, que contemple la conformación de un ERISC, acciones de preparación, detección y análisis, contención, erradicación y recuperación, así como actividades posteriores

al incidente, de conformidad con el **Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.**

2. Un órgano interinstitucional en materia de Tecnologías de la Información y Comunicación y Seguridad de la Información que articule los esfuerzos de las dependencias de la Administración Pública Federa bajo la conducción de la Coordinación de Estrategia Digital Nacional. Este órgano coordinará las acciones necesarias para la prevención y protección de los activos de información, detección, respuesta, contención y mitigación de los incidentes cibernéticos y sus impactos negativos y/o la recuperación de los activos de información clave afectados; así como la revisión periódica de las recomendaciones y sus avances, impulsando el constante y permanente intercambio de información y la mejora continua.
3. Las instancias del Sector Financiero se coordinarán a través de los mecanismos establecidos con la Comisión Nacional Bancaria y de Valores (CNBV) y el Banco de México (Banxico), quienes se apoyarán, conforme a las atribuciones establecidas en la Ley de la Guardia Nacional y su Reglamento, de la Dirección General Científica a través del CERT-MX.
4. Los diversos sectores de infraestructura esencial y la Academia se coordinarán a través de los mecanismos establecidos o los que se definan para tal fin, quienes se apoyarán, conforme a las atribuciones establecidas en la Ley de la Guardia Nacional y su Reglamento, de la Dirección General Científica a través del CERT-MX.
5. Las Entidades Federativas y la Federación se coordinarán a través del Comité de Ciberseguridad en el marco del Sistema Nacional de Seguridad Pública. Por parte del Gobierno Federal, la Guardia Nacional efectuará esta coordinación a través de la Dirección General Científica y en las Entidades Federativas, por conducto de las Unidades de Policía Cibernética.

## 6. Modelo de Operación

El Modelo de Operación del **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos,** está definido conforme al siguiente diagrama:

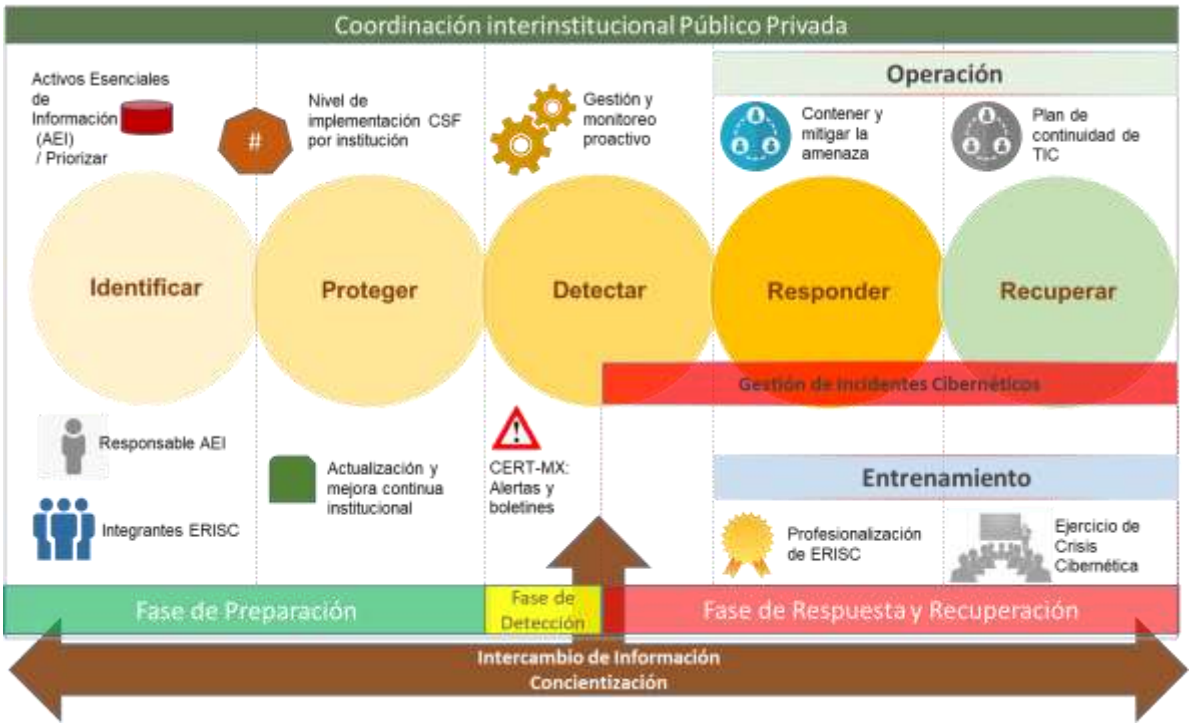


**Gráfico 5. Modelo de Operación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.**

**El Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos considera las fases de preparación, detección, respuesta y recuperación; con las siguientes funciones:**

- **Identificar**, orienta en la identificación del contexto del Múltiple Involucrado, los activos esenciales de información que soportan los servicios esenciales, y los riesgos en materia de Ciberseguridad para la construcción de una estrategia de gestión de riesgos alineada a las necesidades de la institución.
- **Proteger**, orienta en el desarrollo de un plan apropiado de seguridad que garantice la entrega de los servicios esenciales proporcionados por los activos esenciales de información. Esta función tiene la finalidad de establecer estrategias para limitar o contener el impacto de un eventual ataque cibernético.

- **Detectar**, orienta en el desarrollo de acciones apropiadas para la detección de eventos que afecten la Ciberseguridad de los activos esenciales de información y en consecuencia puedan afectar los servicios esenciales que prestan. La función de detección permite el descubrimiento oportuno de incidentes de Ciberseguridad.
- **Responder**, orienta en el desarrollo e implementación de acciones apropiadas respecto de la atención de eventos de Ciberseguridad que puedan afectar los servicios esenciales. La función soporta la habilidad para contener el impacto de un ataque cibernético.
- **Recuperar**, orienta en el desarrollo e implementación del plan de resiliencia que permita la restauración en el menor tiempo posible de cualquier capacidad o servicio esencial que haya sido impactado por un ataque cibernético para reducir la afectación en los activos esenciales de información.

**Roles y responsabilidades de los *Múltiples Involucrados* y de la Dirección General Científica a través del CERT-MX de la Guardia Nacional y de la Comisión Intersecretarial en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos**

El Modelo de Operación del **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos** incluye las siguientes actividades conforme a la asignación de responsabilidades:

| **Actividades a cargo de los *Múltiples Involucrados*** | **Apoyos de la Dirección General Científica a través del CERT-MX de la Guardia Nacional y de la Coordinación de Estrategia Digital Nacional, a través del órgano interinstitucional** | **Actividades de la Dirección General Científica a través del CERT-MX de la Guardia Nacional** |
|---|---|---|
| **Fase de Preparación** | | |
| • Identificación y actualización de activos esenciales de información.<br>• Elaboración y actualización del Plan de Continuidad de TIC.<br>• Designación de responsable ejecutivo y responsables de Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC).<br>• Integración del Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC).<br>• Campañas de concientización sobre seguridad de la información. | • Actualización del catálogo de activos esenciales de información (en el caso de la APF, estará a cargo de cada Institución).<br>• Asistencia en la integración de Equipos de Respuesta a Incidentes de Seguridad en TIC (ERISC) y designación de Responsables de Seguridad de la Información (RSI) de cada Institución.<br>• Actualización en la base de datos de contactos, de los responsables ejecutivos y responsables de Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC), así como RSI.<br>• Asistencia en campañas de concientización sobre seguridad de la información. | • Actualización de los reportes de análisis de impacto a nivel nacional.<br>• Habilitar y mantener las plataformas para la gestión de incidentes y el intercambio de información a través del CERT-MX de la Dirección General Científica de la Guardia Nacional. |

| Actividades a cargo de los *Múltiples Involucrados* | Apoyos de la Dirección General Científica a través del CERT-MX de la Guardia Nacional y de la Coordinación de Estrategia Digital Nacional, a través del órgano interinstitucional | Actividades de la Dirección General Científica a través del CERT-MX de la Guardia Nacional |
|---|---|---|
| **Fase de Detección** | | |
| • Gestión y monitoreo proactivo.<br>• Reporte de incidentes cibernéticos de alto nivel de criticidad e impacto al CERT-MX de la Dirección General Científica. | • Registro y Triage.<br>• Coordinación para el monitoreo proactivo y reactivo. | • Emisión de alertas de amenazas cibernéticas y boletines de vulnerabilidades. |
| **Fase de Respuesta y Recuperación** | | |
| • Contención y mitigación de la amenaza con recursos institucionales o externos.<br>• Recuperación de servicios esenciales.<br>• Identificación de indicadores de compromiso.<br>• Desarrollo de las actividades Post-incidente que incluyen la presentación de denuncias ante el Ministerio Público.<br>• Intercambio de información con CERT-MX de la Dirección General Científica. | • Contención y mitigación de la amenaza en colaboración con los *Múltiples Involucrados*.<br>• Asistencia técnica en la recuperación de servicios esenciales.<br>• Asistencia técnica y legal en las actividades Post-incidente que incluyen la obtención de evidencias digitales y presentación de denuncias ante el Ministerio Público. | • Emisión de alertas de amenazas cibernéticas y boletines de vulnerabilidades específicas.<br>• Difusión de indicadores de compromiso a través de medios y/o plataformas digitales.<br>• Difusión de Actividades Post-incidente.<br>• Intercambio de información con los *Múltiples Involucrados*. |
| **Actualización y Mejora continua institucional** | | |
| • Implementación de Sistema de Gestión en Seguridad de la Información, o MGSI para las instituciones de la AFP.<br>• Implementación de herramientas de monitoreo y detección de incidentes.<br>• Capacitación especializada continua de Equipos de Respuesta institucional. | • Actualización permanente del Protocolo Nacional de Gestión de Incidentes Cibernéticos.<br>• Asistencia en la formación de Equipos de Respuesta institucional.<br>• Actualización del nivel de Implementación de los *Múltiples Involucrados.* | • Actualización permanente de criterios, niveles de servicio y procedimientos para la gestión de incidentes cibernéticos en el CERT-MX de la Dirección General Científica de la Guardia Nacional<br>• Generación de estadísticas oficiales de incidentes en el país en coodinación con el Secretariado Ejecutivo del |

| Actividades a cargo de los *Múltiples Involucrados* | **Apoyos de la Dirección General Científica a través del CERT-MX de la Guardia Nacional y de la Coordinación de Estrategia Digital Nacional, a través del órgano interinstitucional** | **Actividades de la Dirección General Científica a través del CERT-MX de la Guardia Nacional** |
|---|---|---|
| | | Sistema Nacional de Seguridad Pública, y seguimiento de indicadores de Ciberseguridad. |

# 7. Fase de Preparación

### i. Sectores de infraestructura informática esencial

Para efectos del **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos,** los *Múltiples Involucrados* identificarán sus activos esenciales de información de conformidad con el Marco de Referencia de Ciberseguridad de NIST, dentro de los 16 sectores de infraestructuras esenciales, conforme a los siguientes:

1. Químico
2. Comunicaciones.
3. Presas
4. Servicios de Emergencia
5. Servicios Financieros
6. Instalaciones de Gobierno
7. Tecnologías de Información
8. Sistemas de Transporte
9. Instalaciones comerciales
10. Manufactura crítica
11. Industria de defensa
12. Energético
13. Alimentación y Agricultura
14. Salud Pública
15. Materiales, desechos y reactores nucleares
16. Sistemas de aguas y aguas residuales

El **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos** opera de manera permanente con los *Múltiples Involucrados* con estricto apego al alcance y procedimientos del mismo.

Los *Múltiples Involucrados* establecerán los aspectos relativos a la fase de preparación del presente protocolo en el marco de sus competencias y atribuciones; y la designación de personal para las actividades de coordinación e intercambio de información.

Es **altamente recomendable** que los *Múltiples Involucrados* establezcan y operen un Equipo de Respuesta a Incidentes de Seguridad en TIC en su organización, al que se le denominará como **ERISC** para efectos del presente Protocolo; para lo cual, se sugiere considerar la existencia de los roles y responsabilidades que se describen en el **"Anexo 1"** dentro de la institución. Para la integración de los ERISC, el Centro de Respuesta a Incidentes Cibernéticos (CERT-MX) de la Dirección General Científica de la Guardia Nacional, ofrece asistencia a los *Múltiples Involucrados* en cuanto a perfiles, procedimientos, operación y colaboración, entre otros aspectos.

Las instituciones de la Administración Pública Federal, contarán con un Marco de Gestión de Seguridad de la Información (MGSI) cuyo seguimiento, implementación y cumplimiento estarán a cargo de la persona que desempeñe el rol de Responsable de Seguridad de la Información, que recaerá en la persona titular de la Unidad de Tecnologías de Información y Comunicaciones (UTIC), a excepción de aquellas instituciones que por su legislación específica o estructura organizacional cuenten con un área de Seguridad de la Información que no dependa de la UTIC, en dichos casos, el rol de Responsable de Seguridad de la Información recaerá en la persona titular del área de Seguridad de la Información de que se trate.

Para los fines del **Protocolo Nacional de Gestión de Incidentes Cibernéticos,** el CERT-MX de la Dirección General Científica de la Guardia Nacional, fungirá como la única instancia de coordinación entre los *Múltiples Involucrados*.

**ii. Base de datos de contactos**

El **Protocolo Nacional de Gestión de Incidentes Cibernéticos** requiere establecer y actualizar de manera permanente la Base de Datos de Contactos, para la identificación de los responsables a nivel ejecutivo, así como de los Equipos de Respuesta a Incidentes de Seguridad en TIC (ERISC), o de los RSI, en su caso. Los *Múltiples Involucrados* serán responsables de mantener actualizada esta información, proporcionando al CERT-MX de la Dirección General Científica de la Guardia Nacional, cuando menos dos contactos, siendo uno de carácter técnico y otro contacto ejecutivo para la toma de decisiones de conformidad con el **"Anexo 2"**.

Ante cualquier incidente en los activos esenciales de información identificados por los *Múltiples Involucrados*, el CERT-MX de la Dirección General Científica de la Guardia Nacional establecerá comunicación a través de los responsables designados en la lista de contactos. La información no podrá ser difundida ni compartida sin previa autorización del Múltiple Involucrado.

De conformidad con la Ley General de Transparencia y Acceso a la Información Pública vigente y de la Ley Federal de Transparencia y Acceso a la Información Pública, la Dirección General Científica de la Guardia Nacional realizará el procedimiento de clasificación de la información relacionada con la información que derive de la implementación del presente Protocolo como reservada, asimismo, el manejo de los datos personales tendrá el tratamiento de conformidad con lo establecido en la Ley de Protección de Datos Personales en posesión de los Sujetos Obligados.

**iii. Identificación de Activos Esenciales de Información**

Para la identificación de activos esenciales de información por los *Múltiples Involucrados*, se desarrollará la metodología que al efecto se determine en coordinación con diversas instituciones en el país; para los fines del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, los *Múltiples Involucrados* deberán elaborar y proporcionar la información mínima que se describe en el **"Anexo 3"** para la integración de un catálogo básico:

La integración y actualización del catálogo básico de activos esenciales de información estará a cargo del CERT-MX de la Dirección General Científica de la Guardia Nacional.

En el caso de la Administración Pública Federal, la integración y actualización de dicho catálogo estará a cargo de la persona con el rol de Responsable de Seguridad de la Información en cada Institución, de conformidad con la normativa aplicable, para lo cual, la Coordinación de Estrategia Digital Nacional definirá los formatos o mecanismos de integración de la información.

**iv. Nivel de implementación del Marco de Referencia**

Los Múltiples Involucrados determinarán el nivel de implementación actual del marco de referencia con base en la aplicación del cuestionario metodológico del **"Anexo 4",** que será proporcionado para su elaboración a través del CERT-MX de la Dirección General Científica de la Guardia Nacional. El cuestionario será de uso exclusivo de los *Múltiples*

*Involucrados*, y para los fines del **Protocolo Nacional de Gestión de Incidentes Cibernético** los Múltiples Involucrados proporcionarán la postura de seguridad actual y de manera general, mediante la siguiente información:

Los Niveles de implementación se han adaptado al Marco de Referencia de Ciberseguridad de NIST, y de los fines del presente Protocolo, deberán considerarse los siguientes:

- **Nivel 0**: Acciones vinculadas a Ciberseguridad casi o totalmente inexistentes.
- **Nivel 1**: Existen algunas iniciativas sobre Ciberseguridad. Enfoques ad hoc. Alta dependencia del personal. Actitud reactiva ante incidentes de seguridad.
- **Nivel 2**: Existen ciertos lineamientos para la ejecución de las tareas. Existe dependencia del personal. Se ha avanzado en el desarrollo de los procesos y documentación de las tareas.
- **Nivel 3**: Se caracteriza por la formalización y documentación de políticas y procedimientos. Gobernanza de la ciberseguridad. Métricas de seguimiento.
- **Nivel 4**: El Responsable de Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del SGSI, o del MGSI en la APF. Se realiza control interno. Se trabaja en la mejora continua. La ciberseguridad está alineada con los objetivos y estrategias de la organización.

La recopilación y actualización de la información referente al nivel de implementación y la aplicación del cuestionario metodológico con los *Múltiples Involucrados* estará a cargo del CERT-MX de la Dirección General Científica de la Guardia Nacional.

El Cuestionario metodológico es el proporcionado como parte del Marco de Referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) cuya finalidad es facilitar a los *Múltiples Involucrados* una

herramienta para el desarrollo de los programas de ciberseguridad, la gestión de riesgos y la mejora continua de sus controles de operación.

**v. Servicio de alertas y boletines de vulnerabilidades y amenazas cibernéticas del CERT-MX de la Dirección General Científica de la Guardia Nacional.**

Los *Múltiples Involucrados* recibirán, previa suscripción, el servicio de alertas y boletines de vulnerabilidades y amenazas cibernéticas del CERT-MX de la Dirección General Científica de la Guardia Nacional, la cuenta destino deberá corresponder a una cuenta institucional; en caso de actualización, deberá reportarse al correo cert-mx@sspc.gob.mx por el responsable ejecutivo o del responsable del ERISC en su caso, registrados en la lista de distribución.

**vi. Elaboración y actualización del Plan de Continuidad de Tecnologías de la Información y Comunicación**

Los *Múltiples Involucrados* deberán establecer y mantener en su Plan de Continuidad de Tecnologías de la Información y Comunicaciones las acciones necesarias que se aplicarán en la Infraestructura de servicios de información esenciales a su cargo. Las instituciones de la APF, deberán integrar su Plan de Continuidad de Operaciones y de Recuperación ante Desastres en el MGSI.

**vii. Actualización y mejora continua institucional**

Los *Múltiples Involucrados* realizarán las actividades de actualización y mejora continua en relación a los activos esenciales de información que hayan identificado, lo que incluye:

- Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la institución (Sistema de Gestión de Seguridad de la Información o SGSI), o Marco de Gestión de Seguridad de la Información (MGSI) para las Instituciones de la APF, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos o constituir una amenaza para los activos esenciales de información.

- Implementar y operar los controles de seguridad de la información de acuerdo al programa de implementación del SGSI, o MGSI, según corresponda, así como a la capacidad de respuesta a incidentes.

## 8. Mecanismos y criterios para la notificación de incidentes cibernéticos

El presente protocolo, establece las directrices que deberán observar los *Múltiples Involucrados* para realizar el reporte de incidentes cibernéticos al CERT-MX de la Dirección General Científica de la Guardia Nacional, y que estén relacionadas con los activos esenciales de información previamente identificados.

### Mecanismos de notificación de incidentes cibernéticos[2]

La notificación de incidentes cibernéticos por parte de los *Múltiples Involucrados* se llevará a cabo utilizando los mecanismos disponibles conforme a lo siguiente:

Cuando se identifiquen incidentes cibernéticos clasificados como de **"Nivel Alto"**, **"Muy Alto"** o **"Crítico"**, o cuando existan condiciones en el ciberespacio que estén afectando o pudieran afectar uno o más de uno de los activos esenciales de información.

Las instituciones de la Administración Pública Federal deberán notificar mediante la siguiente página web: **https://www.gob.mx/gncertmx**, además de informar inmediatamente a la CEDN.

[2] Guía Nacional de Notificación y Gestión de Ciberincidentes, Consejo Nacional de Ciberseguridad del Gobierno de España (2019)
https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

**En lo referente a los incidentes cibernéticos correspondientes a la Entidades Federativas, se llevará a cabo su registro a través del módulo automatizado de registros de incidentes del Formato Homologado de Incidentes del Sistema Nacional de Seguridad Pública.**

Se utilizará la notificación por correo electrónico institucional de manera alternativa a la cuenta cert-mx@sspc.gob.mx cuando exista información sensible o confidencial. Debido a la naturaleza de la información, el correo deberá ser enviado utilizando la clave PGP del CERT-MX de la Dirección General Científica de la Guardia Nacional, llave pública PGP: 1DA0 5303 B9E7 705C ECA6 F706 F5BF 9C09 4916 4C40.

En el **"Anexo 5"** se proporciona una Guía para el cifrado y descifrado de información utilizando llaves públicas y privadas.

### Formato de Notificación y Registro de Incidentes Cibernéticos

El Formato de Notificación y Registro de Incidentes Cibernéticos del **"Anexo 6"** se utilizará en cualquier evento cuya criticidad y nivel de impacto lo ameriten.

a) **Clasificación de incidentes cibernéticos**

Para efectos del presente protocolo, los incidentes cibernéticos que estarán incluidos en el procedimiento de gestión se ajustarán a la clasificación del **"Anexo 7"**.

b) **Nivel de Criticidad de incidentes cibernéticos**

Para efectos del presente protocolo los criterios que se utilizarán para determinar el nivel de criticidad de los

incidentes cibernéticos serán los establecidos en el **“Anexo 8”**.

**c) Nivel de Impacto de los incidentes cibernéticos**

Para efectos del presente Protocolo los criterios que se utilizarán para determinar el nivel de impacto de los incidentes cibernéticos serán los establecidos en el **“Anexo 9”**.

## 9. Fase de detección

**Semaforización del Protocolo Nacional de Gestión de Incidentes Cibernético respecto al entorno de amenazas y riesgos**

De acuerdo con las condiciones del entorno cibernético, el CERT-MX de la Dirección General Científica de la Guardia Nacional mantendrá un estado semaforizado consistente en los siguientes niveles:

| Color Semáforo | Nivel de Criticidad de las condiciones en el entorno |
|---|---|
| Rojo | **Crítico** |
| Naranja | **Muy Alto** |
| Amarillo | **Alto** |
| Verde | **Medio** |
| Gris | **Bajo** |

El CERT-MX realizará la actualización del estado que guarda el entorno, de manera atemporal, es decir, se modificará cuando las condiciones en el entorno se intensifiquen o disminuyan, por lo que, no dependerá de un horario o fechas específicas para su difusión. Con base en el monitoreo de la red pública de internet y los procedimientos de detección de los *Múltiples Involucrados*, el semáforo se mantendrá usualmente en Nivel **"Medio"** (Color verde) y se actualizará cuando se identifiquen incidentes cibernéticos clasificados como de **"Nivel Alto"**, **"Muy Alto"** o **"Crítico"**, o cuando existan condiciones en el ciberespacio que estén afectando o pudieran afectar uno o más de uno de los activos esenciales de información a cargo de los *Múltiples Involucrados*.

El CERT-MX de la Dirección General Científica de la Guardia Nacional difundirá a través de medios digitales el estado de la **“Semaforización del protocolo respecto al entorno de amenazas y riesgos”**, por lo que, a partir del Nivel **“Alto”**, los *Múltiples Involucrados* deberán adoptar las medidas necesarias como situación de emergencia.

## Gestión y monitoreo proactivo de los *Múltiples Involucrados*

Los *Múltiples Involucrados*, realizarán monitoreo proactivo y reactivo a sus activos esenciales de información y la gestión de incidentes cibernéticos como primer nivel de atención, considerando las siguientes actividades:

- Determinar y actualizar los vectores de ataque más comunes.
- Establecer indicadores y precursores tales como alertas y bitácoras de dispositivos, información pública y otras fuentes externas disponibles así como reportes de usuarios.
- Analizar incidentes cibernéticos mediante técnicas y herramientas.

## Servicio de monitoreo en la red pública de internet del CERT-MX de la Dirección General Científica de la Guardia Nacional

El CERT-MX de la Dirección General Científica de la Guardia Nacional realiza el monitoreo en la red pública de internet a fin de prevenir conductas delictivas, obtiene información de diversas fuentes de agencias nacionales e internacionales y colabora con otros equipos de respuesta que conforman la comunidad global del Forum for Incident Response and Security Teams (FIRST)[3] con más de 500 miembros en más de 90 países. El servicio permite la detección de incidentes y el intercambio de información técnica para el manejo adecuado de incidentes cibernéticos, el servicio está disponible mediante los mecanismos descritos en el apartado "***v. Servicio de Alertas y boletines de vulnerabilidades y amenazas informáticas del CERT-MX***". El servicio de monitoreo servirá como una de las fuentes de información que permitirá la actualización del estado de Semaforización del Protocolo.

[3] Forum for Incident Response and Security Teams (FIRST): https://www.first.org/

## Registro y Triage[4]

La etapa de Registro y "Triage" consta de tres actividades: verificación, clasificación inicial y asignación. Mediante estas subfases, el CERT-MX de la Dirección General Científica de la Guardia Nacional determinará:

- Importancia del incidente cibernético en la institución afectada o en el contexto nacional
- Experiencia del personal que reportó el incidente
- Gravedad del incidente
- Limitaciones de tiempo
- A partir de las anteriores, realizará la clasificación y asignación inicial.

Para la clasificación y asignación de incidentes, así como el seguimiento y medición de los acuerdos de niveles de operación (**"Anexo 10"** Operation Level Agreement, OLA) con el CERT-MX, la Guardia Nacional dispone de una plataforma para la gestión de incidentes cibernéticos basada en código abierto (Open Source) que permitirá la sistematización del procedimiento hasta el cierre del evento.

[4] El nombre de "triage" proviene de un término médico francés, que describe una situación en la que tiene recursos limitados y tiene que decidir sobre las prioridades de sus acciones en función de la gravedad de los casos particulares (ENISA 2010).

## 10. Fase de respuesta y recuperación

Los múltiples involucrados ejecutarán las actividades de respuesta y recuperación considerando al menos las siguientes:

a) Detección y registro de los incidentes
b) Priorización de los incidentes
c) Investigación técnica de los incidentes
d) Aplicar los criterios técnicos de contención de los incidentes, de acuerdo con la criticidad de los activos de información
e) Obtención, preservación y destino de los indicios de los incidentes
f) Erradicación de los incidentes
g) Recuperación de la operación
h) Documentación de las lecciones aprendidas

Los *Múltiples Involucrados* deberán, además:

- Establecer el mecanismo de registro de los incidentes de seguridad de la información, que incluya un repositorio para contener los datos de éstos y crear una base de conocimiento.
- Reportar al responsable de seguridad de la información en la institución, los incidentes de seguridad de la información que se presenten.
- Reportar vía telefónica al CERT-MX de la Dirección General Científica de la Guardia Nacional los que estén relacionados a los activos esenciales de información que se hayan identificado de conformidad con el **"Anexo 3"**.
- Solicitar el apoyo técnico al CERT-MX de la Dirección General Científica de la Guardia Nacional cuando sea necesaria su intervención mediante el Formato de Notificación y Registro de Incidentes Cibernéticos del **"Anexo 6"**.
- Coordinarse con el CERT-MX y otras instituciones en términos del presente protocolo.

**Respuesta a incidentes cibernéticos a cargo del CERT-MX de la Dirección General Científica de la Guardia Nacional**

Una vez recibida la notificación del incidente mediante el Formato de Notificación y Registro de Incidentes Cibernéticos del **"Anexo 6"**, y cuando hayan sido verificados en el procedimiento de **"Triage"**, el CERT-MX de la Dirección General Científica de la Guardia Nacional iniciará la atención del incidente cibernético conforme a las siguientes etapas, en los incidentes correspondientes a las Instituciones de la APF, estas actividades se desarrollarán en coordinación con el órgano interinstitucional encabezado por la Coordinación de Estrategia Digital Nacional.

- **Análisis de datos**

  En esta etapa, el CERT-MX de la Dirección General Científica de la Guardia Nacional primero, notificará a las partes involucradas y recopilará datos de los contactos. En caso de existir más de un área afectada, se identificará y notificará en primera instancia a los contactos donde hubo mayor afectación. De haber acciones inmediatas, se brindarán consejos iniciales y de existir, se proporcionará información sobre procedimientos aplicables para el incidente en particular para su resolución. En esta etapa se recopilará la mayor cantidad de información posible para su análisis.

- **Investigación de la solución**

  El CERT-MX de la Dirección General Científica de la Guardia Nacional documentará las alternativas de solución y llevará a cabo reuniones de trabajo para identificar la viabilidad de su aplicación, conforme a la criticidad del incidente, las reuniones podrán ser en tiempos de cada dos horas para los incidentes de mayor criticidad e impacto. En la

discusión de propuestas podrán participar los integrantes del ERISC de los *Múltiples Involucrados* y otros expertos previamente acordados. Para el caso de la Administración Pública Federal, el órgano interinstitucional encabezado por la Coordinación de Estrategia Digital Nacional participará en la toma de decisiones.

- **Propuestas de acciones**

Cada alternativa de solución acordada se documentará para la asignación de tareas específicas entre los múltiples involucrados, se definirán con claridad las actividades para evitar fallas de interpretación por los ejecutores.

- **Acciones ejecutadas**

El CERT-MX de la Dirección General Científica de la Guardia Nacional verificará la ejecución de las tareas previamente definidas por los medios tradicionales como correo electrónico, teléfono o cualquier otro tipo de contacto directo. En los casos que así lo permita la verificación se realizará a través de consolas de monitoreo o directamente en el dispositivo en cuestión.

- **Erradicación y recuperación**

El CERT-MX de la Dirección General Científica de la Guardia Nacional continuará con el apoyo hasta que las acciones ejecutadas hayan logrado restablecer o recuperado las condiciones normales de operación, en caso de no haber conseguido el objetivo, se revisarán de nueva cuenta las alternativas de solución a partir del análisis de datos y las etapas subsecuentes.

- **Cierre del incidente**

En esta actividad se documentará una breve descripción del incidente (incluida información sobre la clasificación del incidente), los resultados del trabajo realizado, si el incidente se resolvió o no, y sus principales hallazgos y recomendaciones.

- **Información final**

En esta actividad se documentarán las lecciones aprendidas y se mostrará a los *Múltiples Involucrados* lo que sucedió y cómo evitar tal problema en el futuro. Se proporcionará información del incidente y el mecanismo utilizado a otros involucrados para ayudar a mejorar la seguridad de su infraestructura.

Se podrá compartir información técnica no clasificada del incidente (por ejemplo, Indicadores de compromiso) con otros Equipos de Respuesta a través de las plataformas de intercambio de información autorizados.

De existir una denuncia ante la autoridad competente, se desarrollará la cooperación y procedimientos efectivos con las autoridades involucradas, lo anterior, en el ámbito de competencia de los *Múltiples Involucrados* ya sea federal o estatal.

- **Clasificación final**

En esta actividad se realizará, de ser necesario, la reclasificación del incidente con base en la información final para registro histórico.

- **Archivado**

En esta actividad se llevarán a cabo las acciones para proteger el registro en un repositorio que cuente con las medidas de seguridad física y

lógica que permita contar con niveles aceptables de disponibilidad, integridad y confidencialidad de datos y accesos.

El CERT-MX de la Dirección General Científica de la Guardia Nacional opera el Nodo Central de México para el intercambio de información de códigos maliciosos (Malware Information Sharing Plattform, MISP), para su acceso y consulta por los múltiples involucrados, es necesario que cada participante habilite una plataforma similar, mediante la cual se tendrá visibilidad de la información relacionada con otras instituciones sin exponer información sensible o confidencial. El CERT-MX de la Dirección General Científica de la Guardia Nacional ofrece la asesoría técnica para la implementación de la plataforma MISP por parte de los involucrados, una ventaja que ofrece MISP es que se trata de una solución de código abierto (Open Source) que no implica costos por licenciamiento, limitando su implementación a los recursos disponibles de hardware e interconexión vía internet.

- **Análisis Post-Incidente**

Una vez cerrado el incidente y habiendo sido archivado, el CERT-MX de la Dirección General Científica de la Guardia Nacional podrá organizar reuniones de trabajo con los *Múltiples Involucrados* para analizar desde otras perspectivas los acontecimientos en torno a un incidente que por su relevancia lo amerite.

- **Propuestas de mejora**

A partir del análisis Post-incidente, es posible que surjan algunas propuestas de mejora a las condiciones y características de seguridad implementadas, las cuales podrán formar parte de las acciones

correctivas de un Plan de Tratamiento de Riesgos no sólo en la institución afectada sino para el resto de los *Múltiples Involucrados*.

Los acuerdos de niveles de operación (OLA) a los que estará sujeto el CERT-MX de la Dirección General Científica de la Guardia Nacional están definidos en el **“Anexo 10”** del presente protocolo.

## 11. Evidencia Digital

La metodología para el cumplimiento de los criterios de preservación, obtención y destino de las evidencias relacionadas con los incidentes cibernéticos se deberá aplicar observando las medidas necesarias que garanticen en todo momento la integridad y autenticidad de las mismas.

En el **"Anexo 11"** se establecen las etapas que componen el Procedimiento de Cadena de Custodia para la preservación, procesamiento, traslado, análisis y almacenamiento; el cual es responsabilidad de quienes en cumplimiento de las funciones propias de su encargo o actividad en términos de la ley, tenga contacto con ellos, esto será a cargo de personal especializado ya que por la naturaleza de las evidencias relacionadas con un incidente de seguridad de la información, requiere de un manejo y control especial para llevarlas a cabo.

## 12. Recomendaciones para la presentación de denuncias y reserva de la información

### Recomendaciones para la presentación de denuncias

1. **Datos Generales**:
   - Identificación de la organización afectada.
   - Acreditación de la personalidad, documento que acredite la personalidad jurídica del representante o apoderado legal de la organización afectada; y en su caso la persona autorizada para recibir notificaciones y/o contar con la calidad de asesor jurídico ante el Ministerio Público.

2. **Relatoría de hechos:**
   - Día, hora, lugar.

- Persona que tuvo conocimiento e intervino primero ante el hecho, preferentemente el RSI o responsable del ERISC.
- Descripción de la situación en particular, qué detectó y cómo, se deben mencionar los procedimientos aplicados a la seguridad de la información que son necesarios ejecutar para la respuesta y recuperación en torno al incidente cibernético.
- Servicios afectados, qué servicios afectó describiendo de forma cuantitativa y cualitativa, si existió pérdida, modificación o destrucción de información u otra información relevante como datos sensibles, financieros y/o personales.
- Notificación, indicar a quién se notificó, y qué acciones se realizaron para la respuesta y recuperación ante el incidente.
- Acciones realizadas para el resguardo físico y lógico de la información y del dispositivo afectado.
- Acciones generadas para la preservación de los dispositivos afectados a través del resguardo físico y lógico de la información, con el fin de evitar cualquier circunstancia que pueda causar la pérdida, destrucción, alteración o contaminación de los elementos materiales probatorios.
- Presentación de denuncia, debido a la volatilidad de la información digital, se deberá presentar la denuncia ante el Agente del Ministerio Público en el menor tiempo posible, para que se pueda iniciar la investigación correspondiente y se canalice a las instituciones especializadas para su debida atención y contención.

3. **Medios probatorios:**
   - Aportación de indicios ante el Agente del Ministerio Público de conformidad con lo establecido en el numeral 11 del presente Protocolo.
   - La entrega de indicios deberá acordarse con el Agente del Ministerio Público para que se garantice la integridad de los indicios y se pueda contar con todas las condiciones necesarias para su traslado y almacenamiento.

4. **Petitorios a la autoridad:**
    - Dependiendo el caso, la institución afectada podrá solicitar peritos al Agente del Ministerio Público para que ejecute las actividades del procesamiento de los elementos materiales probatorios, debido a que se requiere la intervención de un manejo y control especializado para su preservación y recolección, así como también emita las recomendaciones para su traslado.

    - En este caso, se podrá requerir, a solicitud del Agente del Ministerio Público la intervención de la Dirección General Científica de la Guardia Nacional una vez que se tenga por recibida la denuncia correspondiente ante dicha autoridad y esta inicie la investigación correspondiente.

## 13. Reserva de la información

Es compromiso y obligación de las dependencias, entidades, instituciones y organismos que participan en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, establecer con base en su operación y criticidad, los niveles de divulgación de la información que se origine a partir de la implementación de este Protocolo, solicitando su reserva legal al tratarse de información que constituya un riesgo a la seguridad pública y seguridad nacional, así como a la identificación y operación de los activos esenciales de información de los *Múltiples Involucrados*, de conformidad con lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública.

## 14. Seguimiento del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos

El seguimiento de acciones del Protocolo se realizará a través del CERT-MX de la Dirección General Científica de la Guardia Nacional, instancia que considerará al menos los siguientes rubros:

a. Número de sectores y subsectores identificados, fuente de información "**Anexo 2**".
b. Número de activos esenciales de información por sector y subsector, fuente de información "**Anexo 3**".
c. Avances en la implementación por sector y subsector conforme al Cuestionario de Autoevaluación del Nivel de Implementación del Marco de Referencia de Ciberseguridad del NIST, fuente de información "**Anexo 4**".
d. Número de *Múltiples Involucrados* que forman parte del protocolo, fuente de información "**Anexo 2**".
e. Número de incidentes cibernéticos identificados y atendidos, fuente de información "**Anexo 6**" y **https://www.gob.mx/gncertmx**.
f. Avances en el nivel de implementación de los *Múltiples Involucrados* que forman parte del Protocolo, fuente de información "**Anexo 4**".
g. Reporte trimestral, semestral y anual de Incidentes Cibernéticos identificados y notificados a los Múltiples Involucrados, fuente de información CERT-MX.
h. Reporte trimestral, semestral y anual de incidentes Cibernéticos notificados al CERT-MX de la Dirección General Científica de la Guardia Nacional "**Anexo 6**" y **https://www.gob.mx/gncertmx**.
i. Reporte anual de cumplimiento de niveles de servicio a cargo del CERT-MX de la Dirección General Científica de la Guardia Nacional, "**Anexo 6**" y **https://www.gob.mx/gncertmx**.

# 15.Glosario

**Ad hoc:** Expresión en latín que refiere a que es apropiado, adecuado o especialmente dispuesto para un determinado fin.

**Amenaza:** Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales.

**Activo Esencial de información:** El activo de información cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura de TIC o en los servicios que soporta.

**Activo de Información Clave:** Todo activo de información estratégico que está relacionado con la provisión de bienes y prestación de servicios públicos, cuya afectación impida de manera parcial o total su ejecución.

**Activo Crítico de información:** Todo activo de información que está relacionado con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.

**Acuerdo de Nivel Operacional (OLA):** Es un documento que define los tiempos de atención para las actividades de respuesta a incidentes cibernéticos a cargo del CERT-MX en apoyo al cumplimiento de objetivos de ciberseguridad de los Múltiples Involucrados, los cuales están definidos en el **"Anexo 10"** del Protocolo.

**Aviso de privacidad:** Es un documento físico, electrónico o sonoro, a través del cual, el responsable informa al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

**Ciberseguridad:** Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de información de la organización y los usuarios en el ciberentorno.

**Código abierto:** Es el software con una licencia Open Source.

**Comisión Intersecretarial:** La que con fines de aprovechamiento de las Tecnologías de la Información y Comunicación y de la Seguridad de la Información, presida la Coordinación de Estrategia Digital Nacional.

**Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC):** Es un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas con la finalidad de mitigar sus acciones y efectos, y restaurar las condiciones normales de operación.

**Gestión de Incidentes Cibernéticos:** Procedimientos específicos para detectar, clasificar, analizar, responder y mitigar incidentes que atentan la seguridad de la información de redes y sistemas de cómputo.

**Gestión de riesgos:** Empleo de técnicas y procedimientos para el seguimiento continuo del estado de ciberseguridad del sistema de información.

**Gestión integrada de riesgos:** Se refiere a un proceso general de diagnóstico del riesgo y sus componentes (identificación del riesgo, análisis del riesgo y evaluación del riesgo), así como al tratamiento del riesgo (mitigar, transferir, asumir, evitar).

**Instancias del sector privado:** Son parte de la economía reguladas por el Estado, están dirigidas por individuos como personas físicas o morales y operan con fines de lucro.

**Instituciones de la Administración Pública Federal:** Las dependencias y entidades integrantes de la Administración Pública Federal;

**Infraestructura de Servicios Críticos de Información:** Son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado).

**Marco de Gestión de Seguridad de la Información:** el conjunto de políticas, procedimientos y recursos que adoptan las Instituciones de la APF para fortalecer la seguridad de la información; incluye la clasificación de activos de información institucionales, el análisis de riesgos, gestión de vulnerabilidades, respuesta a incidentes, planes de continuidad y supervisión de la seguridad; bajo un proceso de planeación, implementación, supervisión y mejora continua;

**Gestión de Incidentes de Seguridad en Cómputo:** Es el conjunto de actividades encaminadas a detectar, analizar y reportar los incidentes de seguridad de la información, así como responder para minimizar su impacto en la organización.

**Malware Information Sharing Plattform o MISP:** Herramienta utilizada para compartir indicadores de compromiso (IoC), desarrollada por CIRCL, el equipo de defensa de Bélgica y la OTAN (NIRC). Esta herramienta, ha conseguido a su alrededor una inmensa comunidad de empresas y organismos que colaboran con un objetivo común: compartir indicadores para permitir ampliar las capacidades de protección, así como, mejorar y establecer mejores acciones preventivas y de detección frente a ciberataques.

**Múltiples Involucrados:** A las Instituciones de la Administración Pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado, que cuentan con Infraestructuras esenciales de Información en el país.

**Órgano interinstitucional encabezado por la CEDN**: Consejo Ejecutivo de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, o aquellos que éste establezca.

**Plan de Continuidad de Tecnologías de la Información y Comunicación:** Documento que propicia una apropiada gestión de incidentes de seguridad, buscando disminuir la probabilidad de ocurrencia o el impacto que produciría la materialización de fallas en los sistemas y servicios informáticos ante la presencia de ataques o desastres.

**Plan de Tratamiento de Riesgos:** Documento que establece el tratamiento de los riesgos de seguridad y privacidad de la información, define las acciones a realizar para reducir las pérdidas y

brindar protección a la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio y garantizar la continuidad del negocio.

**Resguardo lógico:** Se refiere al resguardo de información contenida de forma digital, que puede realizarse de varias formas: una opción es la carga de archivos en sistemas de almacenamiento masivo (NAS o SAN), a través de almacenamiento en Internet o almacenamiento en la nube, o realizar copias de seguridad (backup) en otro medio físico, como un CD-R o un DVD-R.

**Responsable de Seguridad de la Información:** la persona titular de la UTIC, a excepción de las Instituciones de la APF que por su legislación específica o estructura organizacional cuenten con un área de Seguridad de la Información que no dependa de la UTIC, en dichos casos el rol de responsable recaerá en la persona titular del área de Seguridad de la Información.

**Seguridad de la información:** La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

**Seguridad Nacional:** Son las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo al artículo 3 de la Ley en la materia.

**Sistema de Gestión de Seguridad de la Información o SGSI:** Es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de los activos de información en las organizaciones. Un SGSI es, por tanto, el conjunto de prácticas orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información.

**Triage:** Fase donde se analiza la información disponible sobre el potencial incidente de seguridad y, si efectivamente es un incidente, se determina la severidad de este y se asignan los recursos necesarios (clasificación, priorización y asignación de incidentes).

**UTIC:** Unidad de Tecnologías de Información y Comunicaciones o área responsable de las TIC en cada Institución de la APF.

**Vulnerabilidades:** Debilidad presente en un activo de información que potencialmente permitirá que una amenaza lo impacte de manera negativa, con posibles afectaciones para la seguridad de la información dentro de la Institución.