PRESIDENCIA DE LA
REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA

Guía de Identificación & Reporte de Incidentes Cibernéticos

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD

Guía de Identificación &
Reporte de Incidentes Cibernéticos

Edición: 01

Centro Nacional de Ciberseguridad (CNCS)
Centro Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD)
Fecha de Publicación: 04 de Enero 2023
Diagramación: Henry González

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

PRÓLOGO 01

INTRODUCCIÓN 02

OBJETIVO 05

ALCANCE 05

MARCO REGULATORIO 06

ALCANCE DE AUTORIDAD 08

COMUNIDAD ATENDIDA 09

¿QUÉ ES UN INCIDENTE CIBERNÉTICO? 09

CLASIFICACION DE LOS INCIDENTES 10

VECTORES DE ATAQUE 12

¿QUÉ HACER ANTE UN INCIDENTE CIBERNÉTICO? 13

REPORTE DE INCIDENTE CIBERNÉTICO 20

CRITERIO DE NOTIFICACIÓN DE INCIDENTES 24

GLOSARIO 32

REFERENCIAS 36

PRÓLOGO

El presidente Luis Rodolfo Abinader Corona, mediante decreto No. 313-22, de fecha 14 de junio del 2022 dispuso la Estrategia Nacional de Ciberseguridad 2030, la cual establece las líneas de acción a ejecutar por el país para adaptar el ecosistema nacional a los nuevos retos de las amenazas cibernéticas. La directriz presidencial también establece los lineamientos del Centro Nacional de Ciberseguridad para el cumplimiento de los objetivos estratégicos considerados.

En adición, de cara a fortalecer la seguridad cibernética de las entidades de la Administración Pública, el presidente de la República Dominicana emitió el decreto 685-22 de fecha 18 de noviembre del 2022, con el objeto de establecer los principios y lineamientos generales que servirán de base a los entes y órganos de la Administración Pública para la adopción de controles, políticas y estándares para incrementar los niveles de madurez cibernética en el sector público, la notificación obligatoria de eventos e incidentes de ciberseguridad, así como el intercambio de información sobre amenazas cibernéticas, conforme lo establece la Estrategia Nacional de Ciberseguridad 2030.

A fin de avanzar en el cumplimiento mandato Presidencial, el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) del Centro Nacional de Ciberseguridad (CNCS), ha formulado la segunda edición de la Guía Identificación y Reporte de Incidentes Cibernéticos, de conformidad con el artículo 12 y 17 de dicha norma del Ejecutivo.

Juan Gabriel Gautreaux
Director Ejecutivo
Centro Nacional de Ciberseguridad

Carlos Leonardo
Director CSIRT-RD
Centro Nacional de Ciberseguridad

INTRODUCCIÓN

La adopción de las tecnologías de la información en el mundo ha aumentado significativamente en los últimos años. Las tecnologías de la información, como el internet, han revolucionado la forma en que las personas se comunican, acceden a la información y realizan sus actividades diarias. Esto ha tenido un gran impacto en la sociedad y ha cambiado la forma en que las empresas y los individuos operan a nivel global.

Este aumento ha traído consigo un aumento en los riesgos cibernéticos. A medida que más personas y empresas dependen de las tecnologías de la información, también aumentan las oportunidades para los ciberdelincuentes. Estos pueden aprovechar vulnerabilidades en sistemas informáticos para acceder a información confidencial, robar dinero o realizar otros delitos informáticos. Por lo tanto, es importante que las personas y las empresas tomen medidas para protegerse contra estos riesgos y estén conscientes de las posibles amenazas cibernéticas.

La protección de las redes y sistemas de información públicos y privados debe ser prioridad de los gobiernos para garantizar la prestación continua de servicios a sus respectivas naciones.

La presente guía establece los mecanismos de comunicación y de interacción con los responsables de gestionar los sistemas de información con atención especial a las de la Administración Pública para reportar incidentes cibernéticos al CSIRT-RD y buscar las soluciones que correspondan en cada caso, para asegurar su continuo funcionamiento y la protección de la información almacenada en las mismas, de conformidad con lo establecido en el art. 12 del Decreto 685-22.

Contempla las acciones a realizar para la identificación y gestión de incidentes de seguridad, que comprende las actuaciones para la identificación, contención y mitigación, preservación de evidencia y consideraciones legales, recuperación y documentación, como apoyo a los procesos internos de las organizaciones relacionados con la respuesta a incidentes cibernéticos.

Detalla el proceso a seguir para reportar al CSIRT-RD los incidentes cibernéticos ocurridos en sus infrae.structuras tecnológicas para fines de seguimiento

Esta guía está alineada con los siguientes:

Agenda Digital 2030, carta de ruta que busca garantizar el acceso de los dominicanos a las tecnologías de la información y comunicación, con el objetivo de reducir la brecha digital y brindar mejores servicios a la ciudadanía. La ciberseguridad es un eje transversal de la Agenda Digital 2030 del país, el que tiene como cuarto riesgo a la desigualdad digital y las fallas de las medidas de ciberseguridad.

Decreto 313-22 que emite la Estrategia Nacional de Ciberseguridad 2030 que establece las líneas de acción en materia de ciberseguridad para la protección del Estado, sus habitantes y, en general, del desarrollo y la seguridad nacional para crear en República Dominicana un ciberespacio más seguro y confiable.

Se hace especial énfasis en el Art. 5 del Decreto referente al Objetivo Estratégico 2 de la Estrategia sobre Protección y resiliencia de infraestructuras tecnológicas.

El Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) desarrolla y publica el presente documento como ordena el artículo 20 del Decreto 685-22, del 18 de noviembre 2022, y el Decreto 230-18 de fecha 19 de junio 2018, por el que se regula el Centro Nacional de Ciberseguridad, que señala las funciones del CSIRT-RD:

Literal (a) “Asistir en la respuesta a incidentes de seguridad cibernética a los organismos de su comunidad objetivo”.

Literal (b) “Coordinar con los responsables de la seguridad de la información de los organismos de su comunidad objetivo para la prevención, detección, manejo y recopilación de información sobre incidentes cibernéticos”

Literal (h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad cibernética ocurridos en sistemas informáticos de los organismos de su comunidad objetivo.

Plan de Acción de la Estrategia Nacional de Ciberseguridad, elaborado por el Consejo Nacional de Ciberseguridad elaborado, el 11 marzo del 2019.

La guía es producto de lo establecido en la línea de acción 2.1.3 de la Estrategia Nacional de Ciberseguridad 2030: “Desarrollar y establecer los protocolos de activación y acción para los organismos de respuesta, y todo el ciclo de gestión de los incidentes.”, la línea de acción 2.1.4 “Elaborar y establecer un plan nacional de comunicación e intercambio de información

ante crisis de incidentes de seguridad cibernética" y la línea de acción 2.3.3 "Elaborar y establecer los protocolos de intercambio de información entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT), las instituciones del Estado, las infraestructuras críticas y el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), para la gestión de los incidentes de ciberseguridad".

El Art. 19 del decreto 685-22 "Atribuciones del Centro Nacional de Ciberseguridad", confieren al Centro Nacional de Ciberseguridad a responsabilidad de elaborar y difundir los protocolos, guías y pautas para la prevención, detección, notificación, respuesta y recuperación a incidentes de ciberseguridad para el mejor cumplimiento de lo establecido en la Estrategia Nacional de Ciberseguridad.

El gobierno de la República Dominicana asume el compromiso de seguir avanzando en materia de ciberseguridad y esta guía es un aporte en esa línea de acción.

OBJETIVO

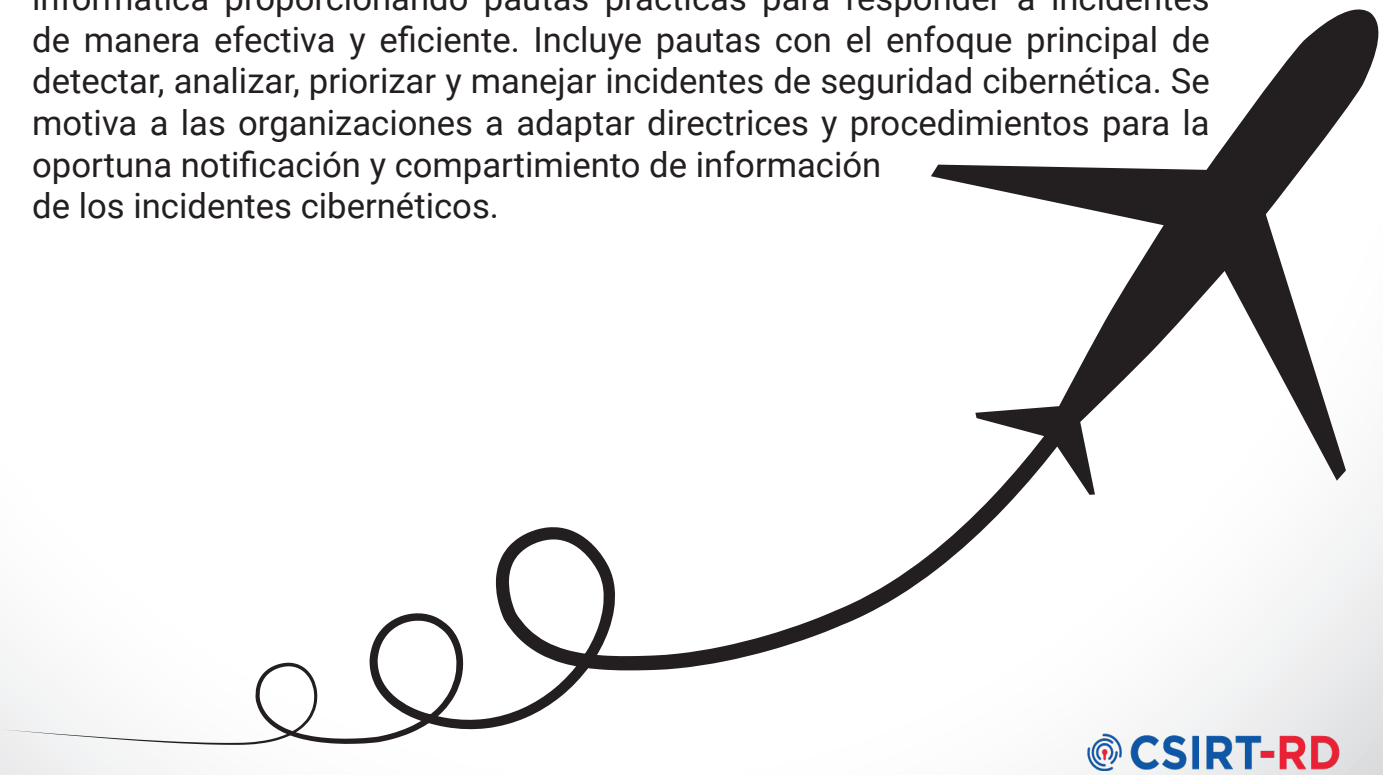
- Proporcionar los pasos a seguir ante la ocurrencia de un incidente cibernético.
- Servir de apoyo a las entidades públicas y privadas en el fortalecimiento de las capacidades de identificación y respuesta a incidentes cibernéticos.
- Concientizar a los responsables de administrar las infraestructuras tecnológicas y sistemas de información sobre las buenas prácticas de gestión de incidentes cibernéticos.
- Proveerles los mecanismos y protocolos adecuados para la notificación oportuna al CSIRT-RD de los incidentes cibernéticos, en especial los relacionados a la infraestructura crítica nacional.

También, proporcionar a la comunidad objetivo:

- Entendimiento de la taxonomía de los incidentes cibernéticos.
- Recomendaciones para determinar la peligrosidad de los incidentes.

ALCANCE

Ayudar a las organizaciones a mitigar los riesgos de los incidentes de seguridad informática proporcionando pautas prácticas para responder a incidentes de manera efectiva y eficiente. Incluye pautas con el enfoque principal de detectar, analizar, priorizar y manejar incidentes de seguridad cibernética. Se motiva a las organizaciones a adaptar directrices y procedimientos para la oportuna notificación y compartimiento de información de los incidentes cibernéticos.



MARCO REGULATORIO

Decreto 230-18	Crea el Centro Nacional de Ciberseguridad y el Equipo Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana, con la misión establecer los mecanismos de ciberseguridad adecuados para la protección del Estado sus habitantes y, en general, del desarrollo y la seguridad cibernética nacional.
Decreto 313-22	Establece la Estrategia Nacional de Ciberseguridad 2030 y los planes complementarios de Ciberdelincuencia, Ciberdefensa y Ciberterrorismo
Decreto 685-22	Establece los principios y lineamientos generales que sirven de base a los entes y órganos de la Administración Pública para la adopción de controles, políticas y estándares para incrementar los niveles de madurez cibernética en el sector público, la notificación obligatoria de eventos e incidentes de ciberseguridad, así como el intercambio de información sobre amenazas cibernéticas, conforme lo dispuesto en el decreto núm. 313-22, que establece la Estrategia Nacional de Ciberseguridad 2030, del 14 de junio de 2022.
Decreto 71-21	Establece el Gabinete de Transformación Digital.
Decreto 527-21	Adopta la Agenda Digital 2030 de la República Dominicana conteniendo la ciberseguridad como uno de sus ejes transversales.
Ley 53-07	Sobre Crímenes y Delitos de Alta Tecnología: Tiene como objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en prejuicio de personas físicas o morales en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

Autoridades Legales

Una razón por la cual muchos incidentes relacionados con la ciberseguridad no resultan en condenas es que algunas organizaciones no contactan adecuadamente a la policía cibernética. Varios organismos de aplicación de la ley están disponibles para investigar incidentes relacionados a ciberdelitos:

- Comisión Interinstitucional Contra Crímenes y Delitos de Alta Tecnología (CICDAT).
- **División de Investigación de Delitos Informáticos (DIDI).**
- Departamento de Investigación de Delitos de Alta Tecnología (DICAT).
- **Procuraduría Especializada contra Crímenes y Delitos de Alta Tecnología**
- **(PEDATEC).**

ALCANCE DE AUTORIDAD

La vinculación del Equipo de respuesta a Incidentes Cibernéticos (CSIRT-RD) y la comunidad atendida está basada en cuatro (4) modelos de autoridad, que a su vez definen las atribuciones y las obligaciones que debe asumir los involucrados frente a un incidente cibernético que ocurra en una entidad de la comunidad.

A continuación, se definen los modelos de autoridad que son aplicados a las comunidades atendidas por el CSIRT-RD:

1. Autoridad Completa
Consiste en la completa autoridad que tiene el CSIRT-RD para establecer las acciones necesarias inherentes a la gestión de un incidente cibernético y las medidas de prevención que los miembros de la comunidad están obligados a implementar. El CSIRT-RD tiene la potestad de implementar mecanismos preventivos como el monitoreo de redes y servicios para identificar intentos de ataques cibernéticos para evitar incidentes a tiempo y apoyar en minimizar el impacto de estos.

2. Autoridad Compartida
Ante un incidente cibernético el CSIRT-RD recomendará a la entidad afectada las acciones a tomar y apoyará con experticia y equipos de acuerdo con cada caso. Sin embargo, las decisiones se tomarán en conjunto.

3. Autoridad Nula
Frente a incidentes cibernéticos el CSIRT-RD no tiene autoridad sobre la toma de decisiones en la entidad afectada. Simplemente provee asesoramiento, información y experiencia sin tomar acciones o decisiones por su cuenta.

4. Autoridad Indirecta
El CSIRT-RD no tiene autoridad sobre la comunidad afectada por un incidente cibernético. No obstante, puede ejercer una presión indirecta mediante el impulso de acciones por parte de un organismo con autoridad sobre la misma.

COMUNIDAD ATENDIDA

EL CSIRT-RD ofrece servicios de respuesta a incidentes cibernéticos a las siguientes entidades agrupadas por categorías y modelo de autoridad aplicable.

Comunidad	Autoridad Aplicada
Entidades Públicas del Estado	Autoridad Completa
Fuerzas Armadas e Instituciones de Fuerza del Orden	Autoridad Indirecta
Infraestructuras Críticas Nacionales – **Públicas**	Autoridad Completa
Infraestructuras Críticas Nacionales – **Privadas**	Autoridad Compartida
Sector Privado	Autoridad Nula
Sociedad Civil en General	Autoridad Nula

¿QUÉ ES UN INCIDENTE CIBERNÉTICO?

Es un evento que pone en peligro la confidencialidad, integridad y disponibilidad de un sistema de información o la información que es procesada, almacenada o transmitida por el mismo, constituye una violación a las políticas de seguridad o prácticas de seguridad estándar implementadas en la institución

Un evento es cualquier ocurrencia observable en un sistema o red. Los eventos incluyen un usuario que se conecta a un recurso compartido de archivos, un servidor que recibe una solicitud desde un portal web y un firewall que bloquea un intento de conexión, entre otros. Existen eventos desfavorables que provocan una consecuencia negativa, como el bloqueo del sistema, inundaciones de paquetes, uso de privilegios en los sistemas, acceso no autorizado a datos confidenciales y la destrucción de datos.

Tipos de Incidentes

Las características del incidente van a determinar cuáles son las acciones que se deben llevar a cabo para resolverlo, el CSIRT-RD cuenta con un catálogo de incidentes que les permite categorizar y tipificar de una manera adecuada.

Estas no serán las únicas topologías que se podrían considerar, la evolución de la tecnología de la información y la complejidad de los ataques abre la posibilidad de contemplar otros nuevos tipos de incidentes.

CLASIFICACION DE LOS INCIDENTES

Debido a que todos los incidentes no poseen las mismas características e implicaciones, es necesario disponer de una clasificación común de los posibles incidentes que puedan ser registrados, lo que servirá de referencia para el proceso de gestión e investigación.

Esta clasificación ha sido creada con referencia de las mejores prácticas a nivel internacional (NIST 800-12 , ISO 27000) y la taxonomía aprobada por el TF-CSIRT como una referencia fija para todos los CSIRT a nivel internacional.

Catálogo de Incidentes		
Tipo de Incidente	**Descripción**	**Categoría**
Virus	Cadena de código con objetivo de infiltrar o dañar sistemas informáticos u otros dispositivos sin el consentimiento del usuario.	Código malicioso
Malware		
Rootkit		
Ransomware		
Herramientas de Acceso Remoto (RAT)		
Denegación de Servicios (DoS)	Ataques con objetivo de colocar fuera de servicio temporal o definitivo sistemas o dispositivos que soportan la operatividad de las infraestructuras de TI.	Disponibilidad
Denegación Distribuida de Servicios (DDoS)		
Interrupción		
Sabotaje		
Error de Configuración		
Error Humano		
Sniffing	Ataques dirigidos a colectar información fundamental y confidencial que permita ejecutar ataques más avanzados en contra de la infraestructura tecnológica.	Robo de información
Ingeniería Social (Phishing/Spear Phishing)		
Escaneo de vulnerabilidades		

Catálogo de Incidentes		
Tipo de Incidente	**Descripción**	**Categoría**
Defacemente (Alteración sitio web)	Ataques dirigidos a la explotación de portales web tanto en diseño, operación o configuración.	Intrusión
Inyección SQL		
Ataque de Fuerza bruta		
Explotación de vulnerabilidades (Hardware/Software)		
Acceso no autorizado	Incidentes relativos a acceso, fuga, extracción, eliminación o alteración de información confidencial.	Compromiso de Información
Modificación/Publicación/ Eliminación de información no autorizado		
Suplantación/Spoofing	Incidentes relacionados a la suplantación de identidad/credenciales	Fraude
Spam (Correo No deseado)	Ataques relacionados a la publicación/envío de publicidad no deseada y de abuso sexual en línea a través de redes de información de infraestructura de TI del Estado	Contenido abusivo
Publicación/almacenamiento de contenido de abuso sexual infantil en línea		

VECTORES DE ATAQUE

Los incidentes pueden ocurrir de distintas maneras, por lo que la organización debe estar generalmente preparada para manejar cualquier tipo de incidente, más aún en los que utilizan vectores de ataque comunes. Diferentes tipos de incidentes merecen diferentes estrategias de respuesta.

Los vectores de ataque enumerados a continuación no están destinados a proporcionar clasificación por incidente; más bien, se enumeran los métodos comunes de ataque, que pueden usarse como base para definir procedimientos de manejo más específicos:

- **Almacenamiento externo/extraíble:** Ataque ejecutado desde un medio extraíble o un dispositivo periférico, por ejemplo, código malicioso que se propaga a un sistema desde una unidad flash USB infectada.
- **Degradación de servicios:** Ataque que emplea métodos de fuerza bruta para comprometer, degradar o destruir sistemas, redes o servicios (por ejemplo, un DDoS destinado a perjudicar o denegar el acceso a un servicio o aplicación; un ataque de fuerza bruta contra un mecanismo de autenticación, como contraseñas, CAPTCHAS o digital firmas).
- **Web:** Ataque ejecutado desde un sitio web o una aplicación basada en la web, por ejemplo, un sitio con XSS (cross-site scripting) utilizado para robar credenciales o una redirección a un sitio que explota una vulnerabilidad del navegador e instala malware.
- **Correo electrónico:** Ataque ejecutado a través de un mensaje de correo electrónico o un archivo adjunto; por ejemplo, explotar código disfrazado como un documento adjunto o un enlace a un sitio web malicioso en el cuerpo de un mensaje de correo electrónico.
- **Suplantación de identidad:** Ataque que implica el reemplazo de algo benigno y auténtico con algo malicioso, por ejemplo, suplantación de identidad, ataques de hombre en el medio (man in the middle), puntos de acceso inalámbricos falsos y ataques de inyección SQL.
- **Uso inapropiado:** Cualquier incidente que resulte de la violación de las políticas de uso aceptable de una organización por un usuario autorizado, excluyendo las categorías anteriores; por ejemplo, usuario que instala software para compartir archivos, lo que lleva a la pérdida de datos confidenciales; o un usuario realiza actividades ilegales en un sistema.
- **Pérdida o robo de equipo:** La pérdida o robo de un medio o dispositivo informático utilizado por la organización, como una computadora portátil, teléfono inteligente o token de autenticación.
- **Otro:** Cualquier ataque que no encaja en ninguna de las categorías anteriores.

¿QUÉ HACER ANTE UN INCIDENTE CIBERNÉTICO?

El objetivo principal de la gestión de incidentes cibernéticos es recuperar el nivel habitual de funcionamiento de los sistemas o servicios minimizando las pérdidas en el menor tiempo posible.

El proceso de recuperar el nivel habitual y las acciones a tomar para mitigar el impacto de las posibles consecuencias del incidente, en adición al proceso de análisis y levantamiento de evidencia son las principales acciones a realizar para enfrentar un incidente cibernético.

La antesala a la gestión de incidentes es la preparación.Toda entidad debe estar preparada para cualquier suceso que pueda ocurrir, tomando en cuenta los tres pilares fundamentales: las personas, los procedimientos y la tecnología.

Entre los puntos a tomar en cuenta de la fase de **preparación** se deben considerar:

- Disponer de información de contacto actualizada.
- **Mantener las políticas y procedimientos actualizados.**
- Tener identificadas las herramientas a utilizar en todas las fases de gestión de incidentes.
- **Capacitación para el equipo humano responsable para mejorar sus capacidades técnicas y operativas.**
- Realizar un análisis de riesgos para disponer de un plan de tratamiento que permita controlar los riesgos.
- **Ejecución de ciberejercicios para entrenar las capacidades.**

RESPUESTA AL INCIDENTE

El proceso de respuesta a incidentes cibernéticos posee las siguientes fases:

- Identificación.
- **Contención y Mitigación.**
- Preservación de evidencia.
- Consideraciones legales.
- **Recuperación.**
- Documentación.

Identificación de un Incidente Cibernético

Para identificar un incidente cibernético, determinar su alcance y los sistemas afectados, se puede obtener información de diferentes fuentes en función de la naturaleza y tipo de incidente. Uno de los principales mecanismos para la adquisición de información es la revisión de logs para detectar anomalías, de igual forma existen otras fuentes de información como son:

- Sistemas de Detección/ Sistemas de Prevención.
- **Alertas de Sistemas de Correlación de eventos (SIEM).**
- Registro de conexiones realizadas mediante el proxy corporativo.
- **Consumo excesivo de recursos.**
- Anomalía en el tráfico con pico de consumo en horas no habituales.
- **Compartir información con otros equipos internos y externos de forma bidimensional para mejorar las capacidades de detección.**

El análisis de esta información permite identificar un posible incidente de seguridad, en caso de que alguno de estos registros presente un comportamiento fuera de lo común será necesaria la realización de un análisis detallado para identificar si realmente existe un incidente.

A nivel de sistemas existen varias formas de detectar o identificar si un sistema está siendo afectado, entre las cuales podemos destacar los siguientes ejemplos:

- Procesos y servicios inusuales o host extraños, poco habituales o incluidos en lista negra de servidores de comando y control utilizados en botnets.
- **Entradas sospechosas en el registro, principalmente en el caso de infecciones de malware en sistemas Windows, siendo esta una de las principales técnicas que utiliza el malware para mantener la persistencia en el sistema infectado.**
- Carga excesiva de disco o memoria pueden estar producidas por un incidente de seguridad como denegación de servicio o intrusiones.
- **Sesiones abiertas en la maquina desde otros equipos, anomalías en las tablas ARP, carpeta compartidas inusuales.**
- Tareas programadas o actividades sospechosas en los registros de auditoria y logs que indique algún funcionamiento anormal del sistema o intentos de intrusión en algún servicio.
- **Cuentas de usuarios inusuales en el sistema o especialmente privilegiadas.**

La identificación del incidente se puede producir mediante fuentes de información externa.

Contención y Mitigación

Luego de identificar el incidente cibernético, la siguiente acción es contenerlo y mitigar sus efectos utilizando toda la información obtenida en la fase del reconocimiento y para lograrlo es necesario definir la extensión, el tipo de equipos afectados y buscar las características comunes para determinar la extensión de la infección y así tomar las medidas de aislamiento en función de los patrones identificados.

Las recomendaciones principales para la contención y mitigación que pueden aplicarse son las siguientes:

- Desconectar el equipo o segmento de red del resto de la organización. Esto puede hacerse si se ha identificado el equipo o equipos infectados.
- **En caso de ser un equipo critico debe aislarse y realizar los filtros para que solo se transmita el tráfico necesario para el funcionamiento del sistema.**

- En caso de conocer los detalles técnicos, vectores de propagación, patrón de comportamiento de una denegación de servicio o las características de un intento de intrusión mediante fuerza bruta.
- **En caso de identificar una vulnerabilidad como la fuente de generación del incidente, se deben aplicar todas las recomendaciones de mitigación proporcionadas por el fabricante.**

Fuga de información y Adquisición de Evidencia

Identificar el vector de fuga de información es vital para reducir o contener la cantidad de información que puede verse comprometida aplicando los controles y medidas técnicas adecuadas que limiten la exposición. Es importante cuantificar las repercusiones que pueden causar la fuga de información y en caso de que sea necesario incluir otras áreas para la gestión del incidente y trazar una estrategia para enfrentar la fuga de información.

Una vez identificados y aislados los equipos que forman parte del incidente, se debe tener en cuenta dentro de la estrategia de contención la preservación de la evidencia para el posterior análisis forense del incidente y se deben extraer los datos volátiles de la memoria antes de proceder al apagado del sistema en caso de que sea necesario o requerido por el proceso de retención. Esta información puede resultar importante para el proceso de investigación.

Para el proceso de análisis forense son utilizadas herramientas destinadas a este fin, procurando no alterar el sistema ni los datos de los mismos ya que puede corromperse información importante como fechas, registro de tiempo, entre otros.

El proceso de adquisición de información es importante contar con mecanismos para la preservación de su integridad, mediante la aplicación de funciones hash criptográficas apropiadas, para esto es importante tener en cuenta varios criterios.

La mayoría de las herramientas de análisis forense soportan funciones MD5 y SHA1. Estas funciones conllevan procesamiento menor, de igual forma conlleva a una seguridad menor. Por otro lado, SHA2 requiere un procesamiento mayor ya que ofrece mayor robustez.

Entre las principales herramientas para la adquisición de datos volátiles:

- En sistemas Unix/Linux, la herramienta LIME desde un USB conectado al sistema comprometido. La herramienta Volatility, de igual forma puede ser utilizada desde un dispositivo USB.
- **En sistemas Windows existen herramientas tales como; FTK Imager, DumpIT, Memory DD para la realización de volcado de memoria.**
- En sistemas virtuales se puede encontrar la memoria RAM en extensiones .sav (virtualbox) y en extensiones .vmen (vmware).

Recuperación

Luego de identificar, contener, preservar la evidencia y reportar el incidente, procede la recuperación de los sistemas afectados.

Para aquellos sistemas que no son críticos, una vez que es detectado el vector de infección e implementadas las medidas correctivas oportunas para reducir el riesgo de reproducción del incidente, se pueden restaurar los sistemas desde una copia de respaldo que haya sido realizada antes del incidente.

En caso de que el sistema sea crítico que no exista alta disponibilidad, se tendrá que valorar añadir controles al plan de continuidad del negocio y a su vez realizar copias periódicas en todo el sistema. En cualquier caso, en sistemas críticos siempre se deben seguir las instrucciones del fabricante para su restauración o reinstalación al momento de llevar acabo la recuperación.

Documentación

Dentro del proceso de gestión de incidentes cibernéticos es importante la documentación de todo lo aprendido durante el proceso. Estas lecciones pueden ser parte vital para identificar de manera proactiva futuros incidentes de seguridad con características similares. Es importante tener información precisa de la linea de tiempo de cuando sucedió, qué sucedió, y el periodo de tiempo se extendió hasta su resolución.

La documentación de los incidentes debe ser detallada indicando las herramientas utilizadas, como fueron utilizadas y sus resultados, así como indicar la documentación utilizada para resolver el incidente y las colaboraciones que fueron necesarias.

Estas informaciones se utilizan para conocer con exactitud las características, naturaleza y tipo de incidente y los vectores de infección e indicadores de compromiso, así alimentar la parametrización de los sistemas de seguridad y realizar campañas de concientización adaptada a la situación de la organización. Todas las acciones técnicas y procedimientos siempre deben velar por cumplir con las consideraciones legales que apliquen a la organización y de igual forma tomar en cuenta la clasificación de la información establecida.

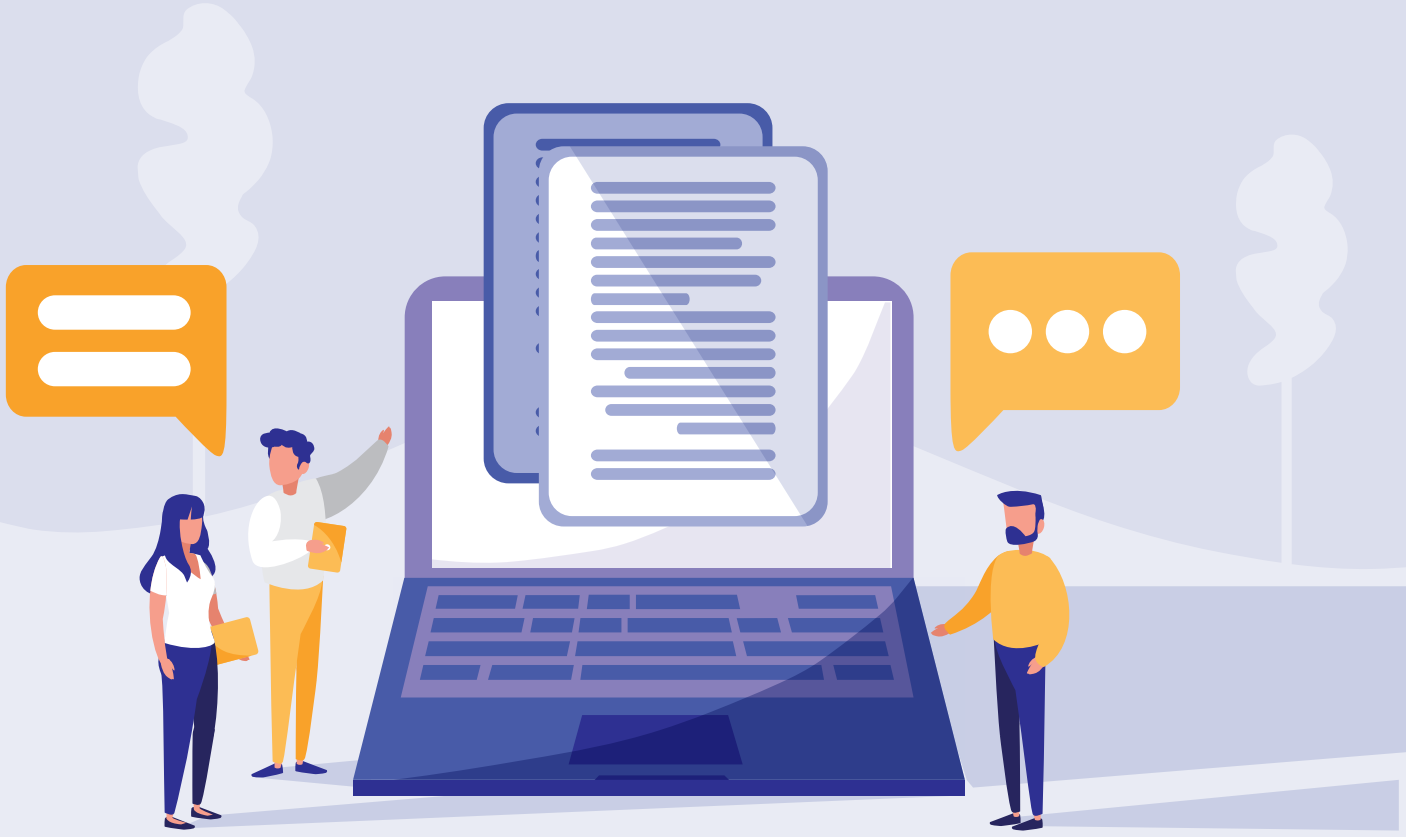
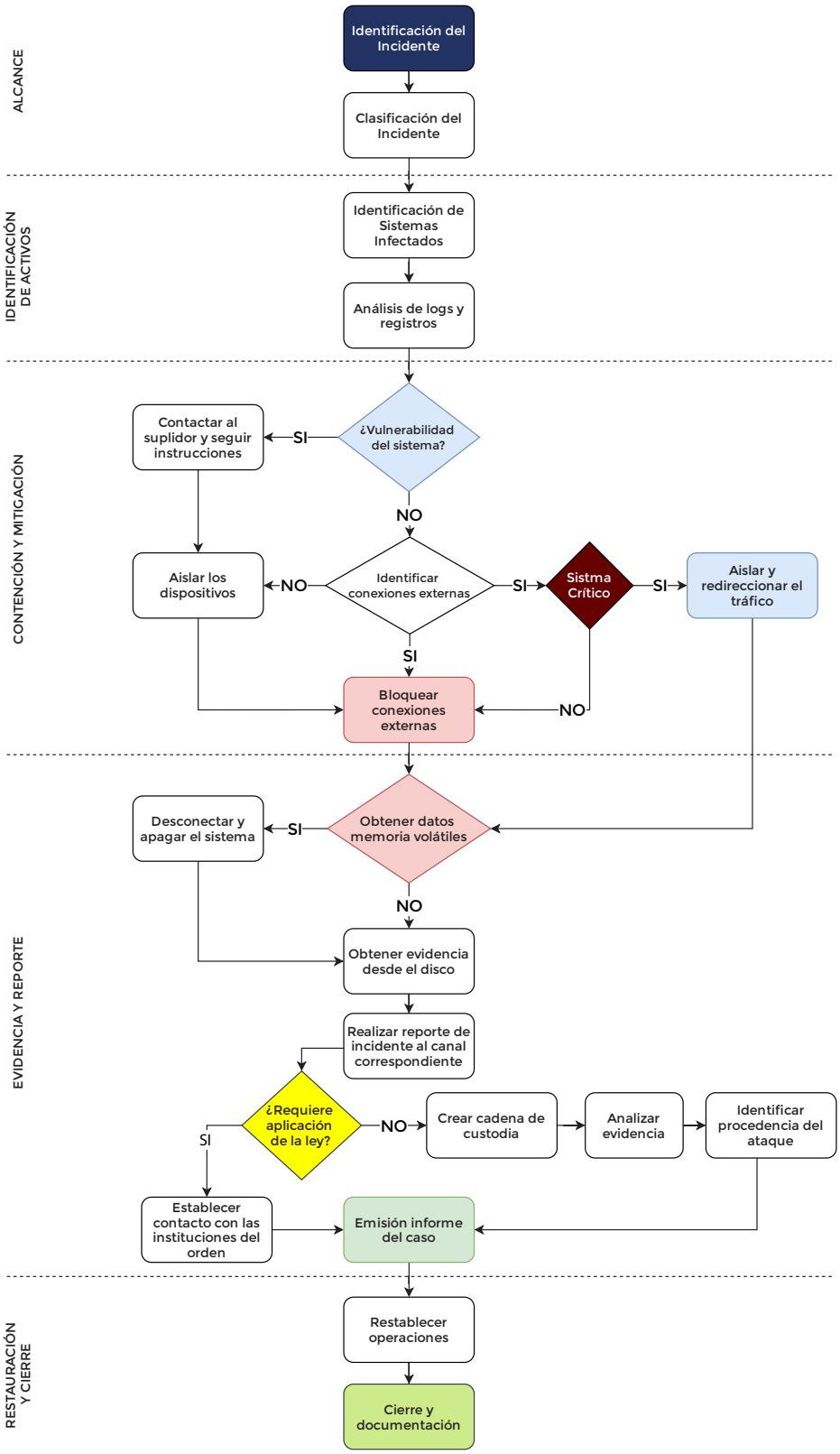


Diagrama de Flujo de las Fases de Respuesta a Incidentes



REPORTE DE INCIDENTE CIBERNÉTICO

El rol principal del Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) es brindar respuesta oportuna a los incidentes de seguridad cibernética reportados por las instituciones de su comunidad atendida.

Para llevar a cabo una eficiente gestión de respuesta es necesario contar con informaciones claves que permitan la correcta atención, es por lo que en los siguientes puntos se indican las informaciones necesarias a presentar al momento de realizar un reporte.

¿Cómo Reportar?

El reporte de incidentes cibernéticos se realizará a través de la persona registrada como punto de contacto de la organización mediante el correo incidentes@csirt.gob.do. Se recomienda la utilización de correo cifrado utilizando la llave pública PGP de incidentes@csirt.gob.do que se encuentra publicada en el formulario RFC-2350. Esto iniciará la comunicación entre las partes y generará un código único de identificación del incidente dentro del sistema de gestión de incidentes del CSIRT-RD.

Como segunda opción de contacto se podrán realizar a través del formulario de reporte de incidentes en el portal de Centro Nacional de Ciberseguridad: https://cncs.gob.do/reportar-incidentes/

En caso de alguna urgencia podrá contactarse con el analista de servicio, los datos para la comunicación se encuentran en el siguiente enlace. https://cncs.gob.do/sobre-nosotros/rfc-2350/

El intercambio de información se realiza mediante correo eléctrico institucional y siempre llevará en el “asunto” el código único del incidente generado por el sistema de gestión.

Información Necesaria

Para que la gestión de incidente por parte del CSIRT-RD sea eficiente y oportuna, la comunicación del reporte debe incluir todo lo que el usuario entienda necesario para la resolución de este. Con esta información el administrador de la cola de incidentes realizará el registro correspondiente en el sistema de gestión de incidentes.

Dentro de las informaciones mínimas requeridas o necesarias para el registro se encuentran las siguientes, pero no se limita a estas:

Formulario de Reporte de Incidente	
Asunto:	Título que describe de forma general el incidente.
Descripción:	Descripción breve sobre el incidente.
Función u objetivo:	Identificar si es una consulta o es el reporte de incidente. Por defecto será considerado un reporte de incidente.
Afectado:	Indicar la entidad o persona afectada
Tipo de incidente (según la taxonomía del acápite de Clasificación de Incidente):	Indicar el tipo de incidente según la categoría definida en este documento.
Recursos afectados:	Indicar la información técnica sobre el número y tipos de activos afectados.
Impacto:	Indicar un aproximado de impacto en la entidad, tomando en cuenta los recursos afectados.
Nivel (peligrosidad):	Indica el nivel de criticidad del incidente.
Mensaje:	Este apartado va a contener toda la información adicional por el emisor del informe y la información levantada por el personal del CSIRT-RD al momento de la identificación del incidente.
Origen del incidente:	Indicar con la mayor precisión posible el origen, en caso de tener conocimiento.
Fecha y hora del incidente:	Indicar con la mayor precisión posible la fecha y hora del incidente.
Fecha y hora de detección:	Indicar con la mayor precisión posible la fecha y hora de detección.
Acciones realizadas:	Indicar las actividades realizadas en contramedida al incidente.
Adjunto:	Colocar todos los documentos que puedan aportar información al análisis.

Estados y Valores de Cierre

Durante el proceso de las distintas fases de gestión de incidente, el CSIRT-RD mantendrá el incidente en estado "abierto", realizando las actividades necesarias con el punto de contacto y los seguimientos correspondientes.

No siempre la solución de un caso será de manera satisfactoria, es por lo que se cuenta con diferentes estados que puede tener un incidente reportado en un instante dado.

Estado	Descripción
Abierto:	Estado que va desde el registro del caso hasta que se produce el cierre del mismo.
Resuelto:	La institución ha realizado las labores de corrección y el CSIRT-RD ha notificado la solución de los mismos.
Cerrado falso positivo:	La detección ha sido errónea.
Cerrado (Sin solución y sin respuesta):	Pasado un periodo de 30 días si el incidente no ha sido cerrado es cerrado con este estado.
Cerrado (sin solución y con respuesta):	La institución no ha alcanzado una solución al problema a pesar de contar con las recomendaciones del CSIRT-RD.

Clasificación y Priorización

La correcta clasificación y priorización de los incidentes le permite al equipo nacional de respuesta a incidentes CSIRT-RD brindar soluciones oportunas y consistentes al usuario, así como también asegurar el manejo de información según la sensibilidad de la información. El CSIRT-RD puede modificar la clasificación y prioridades durante la resolución del incidente, esto quedará registrado dentro del sistemas de gestión de incidentes.

Según la prioridad de los incidentes, el CSIRT-RD contempla los siguientes niveles:

- **CRÍTICO: El incidente de seguridad** que afecta a alguna de las dimensiones de seguridad y supone un perjuicio muy grave o total para los objetivos de la organización, sus activos críticos o los individuos afectados.

- **ALTO:** El incidente de seguridad que afecta a alguna de las dimensiones de seguridad y supone un perjuicio grave para los objetivos del ente u órgano, sus activos críticos o los individuos afectados.
- **MEDIO:** El incidente de seguridad que afecta a alguna de las dimensiones de seguridad supone un perjuicio parcial sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- **BAJO:** El incidente de seguridad que afecta a alguna de las dimensiones de seguridad supongan un perjuicio mínimo o incluso nulo sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Escalado de Incidentes

El CSIRT-RD posee una metodología para el escalado de soporte al momento de atender un incidente:

NIVEL 1 – Los analistas de este nivel realizan las actividades de atención primaria a los reportes de incidentes y consultas. Además, realizan el seguimiento a todos los reportes e incidentes abiertos y generan toda la documentación necesaria.

Entre las incidencias a responder se encuentran:

- Respuestas a solicitudes de información.
- **Ataques o incidentes conocidos.**
- Monitorización y respuesta antes vulnerabilidades públicas.
- **Identificación de oportunidades de mejoras en la infraestructura o sistemas de seguridad.**
- Identificación de oportunidades de mejoras a los procedimientos y políticas de seguridad internas.

NIVEL 2 – Los analistas de este nivel tienen un conocimiento elevado en seguridad, es un equipo de expertos que siempre responderá los incidentes escalados desde el equipo de primer nivel.

Entre las incidencias a responder se encuentran:

- Ataques no conocidos o de difícil identificación.
- **Análisis de vulnerabilidades sospechosas.**
- Soporte para consultas relacionadas a infraestructura de seguridad o configuración adecuada de los equipos.
- **Realizar pruebas de intrusión.**
- Análisis de impacto y riesgo real de vulnerabilidades.

CRITERIO DE NOTIFICACIÓN DE INCIDENTES

Al momento de recibir la notificación de un incidente se utilizará como criterio de referencia el nivel de peligrosidad que se le asigne al incidente, tomando en cuenta que en la medida del proceso de desarrollo, investigación, mitigación o resolución del mismo puede variar.

En caso de que un incidente se asocie a más de un tipo de incidente se le asociará el nivel más alto de peligrosidad según los criterios expuestos.
Los incidentes serán asociados en alguno de los siguientes niveles de peligrosidad: CRITICO, ALTO, MEDIO, BAJO.

NIVEL DE PELIGROSIDAD			
NIVEL	**AMENAZA**	**VECTOR DE ATAQUE**	**CARACTERISTICAS DEL INCIDENTE**
CRITICO	Ciberespionaje, Interrupción de los Servicios IT / Filtración de datos / Compromiso de los servicios	APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, códigos dañinos confirmados de “Alto Impacto” (RAT, troyanos enviando datos, rootkit, etc.).	• Capacidad para filtrar información valiosa o confidencial, en cantidad considerable y en poco tiempo. • Capacidad para tomar el control de los sistemas sensibles.
ALTO	Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Suplantación	Códigos dañinos de Medio Impacto (virus, gusanos, troyanos), ataques externos, compromiso de servicios no esenciales (DoS / DDoS), tráfico DNS con dominios relacionados con APTs o campañas de malware, accesos no autorizados, suplantación, sabotaje, inyección SQL, spear phising, pharming.	• Capacidad para filtrar información valiosa. • Capacidad para tomar el control de ciertos sistemas.

NIVEL DE PELIGROSIDAD			
NIVEL	**AMENAZA**	**VECTOR DE ATAQUE**	**CARACTERISTICAS DEL INCIDENTE**
MEDIO	Logro o incremento significativo de capacidades ofensivas	Envío y descarga de archivos sospechosos, remitentes con dominios o direcciones IP sospechosas, escaneo de activos y vulnerabilidades, códigos dañinos de "Bajo Impacto" (adware, spyware, etc.), sniffing, ingeniería social.	• Capacidad para filtrar un volumen apreciable de información. • Capacidad para tomar el control de algún sistema de bajo impacto en las operaciones de TI.
BAJO	Ataques a la imagen / menosprecio / errores y fallos	Spam sin adjuntos, identificación de software desactualizado, publicación, almacenamiento de contenido de abuso sexual infantil en línea, error humano, fallo de hardware y software.	• Escasa capacidad para filtrar un volumen apreciable de información. • Nula o escasa capacidad para tomar el control de sistemas.

El impacto se evaluará con respecto a tres características principales:

- Alcance o distribución territorial: el área geográfica que podría verse afectada por la pérdida o indisponibilidad de una infraestructura crítica.
- **Gravedad, intensidad o magnitud: las consecuencias de la interrupción o destrucción de una infraestructura crítica.**
- Efectos del tiempo o distribución temporal: el punto en el que la pérdida de un servicio podría tener un impacto grave (inmediato, uno o dos días, una semana).

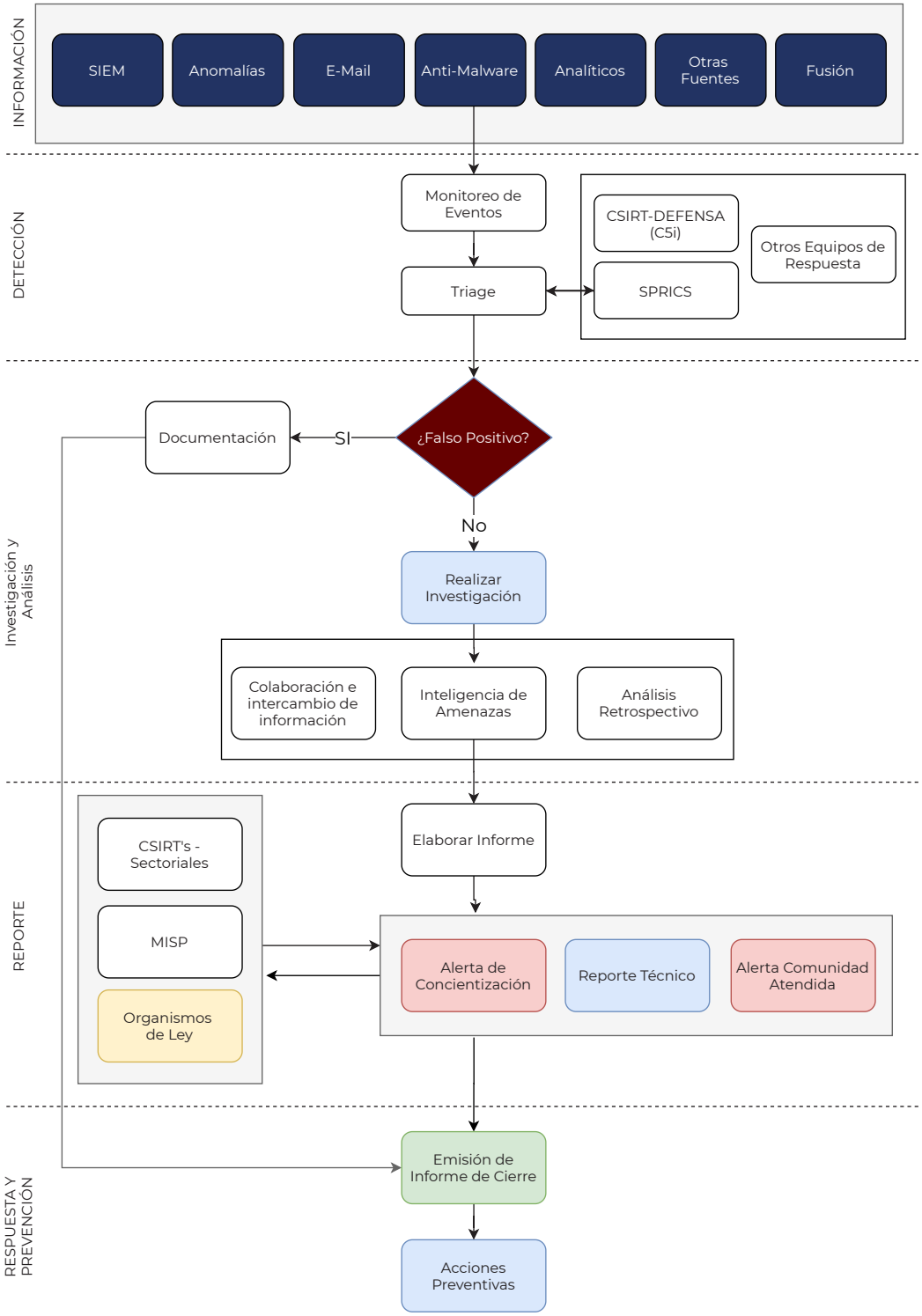
Para esto se utilizarán criterios de impacto indicativo como se muestra a continuación:

Criterio	Detalle
Instituciones involucradas	El activo, sistema o aplicación es utilizada por más de una infraestructura crítica o institución del Estado.
Impacto económico	La afectación del servicio genera una pérdida económica importante en la producción o recaudación.
Orden Público	La afectación del servicio afecta el correcto funcionamiento del orden público y procesos judiciales.
Confianza Pública	Refiere al impacto mediático negativo que causa la falla, interrupción o pérdida del servicio.
Relaciones Internacionales	Afectación de las relaciones o contratos con empresas extranjeras u otros países.
% de impacto	Refiere al porcentaje de espacio territorial o personas afectadas.

A continuación, se presenta la tabla de criterios para determinar el impacto de un incidente cibernético, mediante la cual las entidades notificantes podrán asignar un determinado nivel de impacto a un incidente:

Nivel	Descripción
Critico	• Anulación en más de un 90% de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales. • **Los activos, sistemas o aplicaciones afectadas son utilizadas por más de un servicio esencial o institución del Estado.** • Interrupción de la prestación del servicio superior a 8 horas. • **Daño muy grave, e incluso irreparable, de los activos de la organización, sean estos financieros, de información, de imagen o de otra naturaleza.** • Daños reputacionales de la imagen del país muy elevados y cobertura en medios de comunicaciones internacionales. • **Afecta la seguridad nacional y ciudadana.** • El incumplimiento de alguna ley o regulación sobre la materia.
Alto	• **Anulación en más de un 70% de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales.** • Interrupción de la prestación del servicio superior a 1 hora. • **Daño grave de los activos de la organización, sean estos financieros, de información, de imagen o de otra naturaleza.** • Daños reputacionales muy elevados y cobertura en medios de comunicaciones internacionales. • **Perjuicio grave a individuos, de difícil o imposible reparación.** • El incumplimiento de alguna ley o regulación.
Medio	• **Reducción parcial a más de un 30% de la capacidad del ente u órgano para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.** • Daño parcial de los activos del ente u órgano, así sean estos financieros, de información, de imagen u otra naturaleza. • **Daño reputacional comprobable.** • Perjuicio moderado a algún individuo. • **Otros de naturaleza análoga.**
Bajo	• No hay reducción de la capacidad del ente u órgano para atender eficazmente con sus obligaciones corrientes, las cuales se siguen desempeñando normalmente. • **No hay daño o con daño mínimo de activos del ente u órgano, así sean estos financieros, de información, de imagen u otra naturaleza.** • No hay perjuicio a individuos.
Sin impacto	**No hay ningún impacto apreciable.**

Ciclo de Gestión de los Incidentes



Otros Organismos de Respuesta

De igual forma las redes financieras y de defensa de Republica Dominicana, tienen a su disposición una serie de organismos de referencia, en los cuales se fundamenta la capacidad de respuesta a incidentes de ciberseguridad de cada sector:

- **CSIRT-Defensa del Centro de Mando y Control, Comunicaciones, Computo, Ciberseguridad e Inteligencia (C5i) del Ministerio de Defensa**, con un marco de competencia en las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional, apoyando a los operadores de servicios que tengan incidencia en la Defensa Nacional.
- **SPRICS – Administración Monetaria y Financiera**, con un ámbito de competencia en el sistema financiero y de pagos, incluyendo asimismo las empresas y operadores de apoyo a los mismos, y otras entidades que la Junta Monetaria autorice, como el ente de respuesta a incidentes de ciberseguridad que afecten o pudieran afectar a los sistemas y la operatividad de las entidades citadas, interconectadas con el SPRICS.

Intercambio de Información y Comunicación de Incidentes Cibernéticos

Además de la notificación de los incidentes cibernéticos al CSIRT-RD, en ocasiones las entidades de la Administración Pública necesitarán comunicarse con terceros, como los organismos de seguridad del Estado y los medios de comunicación para la divulgación del incidente a sus clientes. En cambio, el resto de las comunicaciones con otros actores como CSIRT's Sectoriales, organismos internacionales, proveedores de plataforma de inteligencia de amenazas, entre otros, se realizarán a través del CSIRT-RD, en su rol de organismo de Intercambio de Información sobre los Indicadores de Compromiso (IoC) de incidentes cibernéticos.

Los esfuerzos de coordinación para el compartimiento de información con organizaciones externas se consultarán con el departamento legal antes de iniciar el intercambio. Puede haber contratos u otros acuerdos establecidos previamente, por ejemplo, Acuerdo de Confidencialidad (NDA) para proteger la confidencialidad de la información más confidencial de la organización.

TLP (Traffic Light Protocol)

Traffic Light Protocol (TLP): es el esquema creado para el intercambio de información sensible en el ámbito de seguridad de la información para que el autor pueda indicar las consideraciones que deben ser tomadas al momento de poner en circulación la información y que el receptor tenga conocimiento de las acciones a tomar en caso de distribución.

Signo	Utilización	Distribución	Código de Color
TLP-RED	Para la información que es limitada a personas seleccionadas y su divulgación podría tener un impacto negativo en las operaciones.	Puede ser distribuida únicamente a las personas designadas.	**RGB** R230 G44 B0
TLP-AMBER **TLP-AMBER+STRICT**	Para la información interna que con su mal uso o distribución causaría riesgos de privacidad afectando la reputación y las operaciones.	Para TLP:AMBER la información puede ser distribuida con la condición de tener la necesidad de conocimiento sobre la misma a la organización y su comunidad autorizada. En el caso de AMBER+STRICT restringe el uso compartido solo a la organización.	**RGB** R247 G182 B53
TLP-GREEN	Para todas las informaciones que pueden ser compartidas en la organización y con terceros.	Puede ser distribuida a las organizaciones asociadas, pero no por medios públicos.	**RGB** R119 G210 B8
TLP-CLEAR	Para la información que pueda ser utilizada sin ocasionar ningún riesgo en caso de que sea mal utilizada.	Puede ser distribuida a las organizaciones asociadas, pero no por medios públicos.	**RGB** R255 G255 B255

Ministerio Publico y Policía Nacional

En cuanto un incidente reportado al CSIRT-RD tenga características delictivas, criminales o infracciones legales, y sea solicitado a través de Ministerio Publico, el CSIRT-RD por medio a los mecanismos legales establecidos, compartirá información relativa a la evidencia recolectada durante el proceso de gestión de incidentes.

Los órganos de investigación serán contactados a través de un punto de contacto designado de manera consistente con el requisito de la ley y los procedimientos de la organización. Este recurso estará familiarizado con los procedimientos de presentación de informes para todas las agencias de investigación relevantes.

Notifiación de Incidentes a Equipos de Respuesta Sectoriales

El CSIRT-RD cooperará con el CSIRT-Defensa y SPRICS en todas aquellas situaciones en que requieran apoyo de los operadores de servicios que soportan su comunidad atendida y en todos los incidentes detectados que tengan impacto con la Defensa Nacional y el sector financiero respectivamente.

GLOSARIO

Activo de Información: Cualquier información o sistema relacionado que tenga valor para la organización.

Amenaza: Situación nociva que puede suceder y cuando sucede tiene consecuencias negativas sobre los activos de información afectando su funcionamiento.

Acceso Remoto: Es una característica que permite conectarse a una PC desde cualquier lugar mediante internet y software especializados para utilizar las características.

Análisis de riesgos: proceso que comprende la identificación de activos de información, sus amenazas y vulnerabilidades a los que se encuentra expuestos, así como la probabilidad de ocurrencia y el impacto con el fin de determinar los controles adecuados.

Ataque fuerza bruta: Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar mediante el empleo de combinaciones alfanuméricas, con el fin de acceder al sistema.

Cifrado: Método que permite aumentar la seguridad de un mensaje mediante la codificación del contenido de manera que solo pueda tener acceso la persona autorizada.

Criptografía: Técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca la clave mediante la cual ha sido cifrado.

Ciberincidente: Todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

Confidencialidad: Propiedad de la información por la que se garantiza que esta accesible a personas autorizadas.

Disponibilidad: Capacidad de un servicio, sistema o información de ser accesible y utilizable por los usuarios o procesos autorizados cuando sea requerido.

Delito: Cualquier acción tipificada como delito según lo establecido en ley 53-07.

Denegación de servicio (DoS): Consiste en una seria de técnicas que provocan la inoperatividad de un servicio o un recurso. Consiste en la implementación masiva de peticiones a un servidor, lo que genera una sobre carga del servicio y el posterior colapso.

Denegación distribuida de servicio (DDoS): Es una variable de DoS, en el cual las peticiones se llevan a cabo de forma ordenada desde varios puntos hasta el mismo objetivo.

Defacement: Tipo de ataque a sitio web en el que se implementa un cambio en la apariencia visual de la web.

Explotación: Cualquier práctica mediante la cual un atacante cibernético vulnera un sistema de información y/o comunicación, con fines ilícitos o para los cuales no está debidamente autorizado.

Escaneo de puertos: Análisis local o remoto mediante software, del estado del puerto de una maquina conectada a la red, con la finalidad de obtener información relativa a la indicación de los servicios activos y las posibles vulnerabilidades.

Escaneo de red: Análisis mediante el cual es posible tener un escaneo del estado de la red, con la finalidad de obtener información relativa a la identificación de los servicios activos y sus posibles vulnerabilidades.

Incidente de Seguridad: Suceso que afecta los pilares de la ciberseguridad que son confidencialidad, integridad y disponibilidad de los activos de información.

Incidente cibernético: Evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la contienen.

Ingeniería social: Técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

Infraestructura crítica de la información: Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

Inyección SQL: Tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

Integridad: Es la propiedad de la información que garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, perdida o destrucción.

Malware: Programa malicioso que tiene como objetivo dañar, robar o introducirse al sistema sin ser detectado por el usuario. Existen varios tipos de programas maliciosos; virus, troyanos, spyware, entre otros.

Phishing: Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social.

Ransomware: El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

Rootkit: Conjunto de software dañino que permite el acceso privilegiado a un equipo mientras oculta su presencia en el sistema.

Sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Sabotaje: Daño o deterioro que se hace en instalaciones, productos, etc., como procedimiento de lucha contra los patronos, contra el Estado o contra las fuerzas de ocupación en conflictos sociales o políticos.

Spear Phishing: Variante de phishing mediante la cual el atacante focaliza su actuación sobre un objetivo concreto.

Suplantación/Spoofing: Técnica de suplantación de identidad en la red, llevada a cabo por un ciberdelincuente gracias a un proceso de investigación o con el uso de malware.

SPAM (Correo masivo): Correo no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.

Spyware (Malware espía): Es un tipo de malware que espia las actividades del usuario sin su consentimiento o consentimiento, se pueden difundir por un troyano o mediante explotación de software.

Taxonomía: Clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.

Virus: Tipo de malware cuyo principal objetivo es modificar o alterar el comportamiento de un sistema sin el consentimiento del usuario.

Vulnerabilidad: Deficiencias de un programa que pueden permitirle a un ciberatacante acceder a información no permitidas.

REFERENCIAS

- Guía Nacional de Notificación y gestión de incidentes, https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf, (Consultada Abril 2020).
- Glosario de Terminos del Equipo de Respuesta a Incidentes Cibernéticos CSIRT-RD.
- Glosario de Términos de Ciberseguridad , INCIBE https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf (Consultada Abril 2020)
- https://dle.rae.es/ , Consultada 11 de Mayo 2020.
- https://www.pandasecurity.com/homeusers/downloads/docs/product/help/gl/2014/sp/177.htm , consultada 11 de mayo 2020.

PRESIDENCIA DE LA
REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

Agenda Digital 2030

República Dominicana