Guía de Notificación y Gestión de Incidentes de Ciberseguridad

Índice

1. Introducción

El uso de Internet y el de las Tecnologías de la Información y las Comunicaciones (TIC) generaron una gran dependencia para el óptimo funcionamiento de las infraestructuras críticas del Estado argentino, así como también un incremento importante en los servicios que este brinda a la ciudadanía. Por tal motivo, cualquier disrupción parcial o total de los mismos podría causar problemas serios en términos de bienestar social, económico y político.

En ese sentido, se considera central fortalecer las capacidades técnicas, operativas, de gestión de incidentes de ciberseguridad de los organismos del Sector Público Nacional, con el propósito de que sus activos de información esenciales puedan mantener los niveles de riesgo aceptables y sigan funcionando de manera habitual. Tal consideración se encuentra alineada con el objetivo de la Estrategia Nacional de Ciberseguridad que está vinculado al fortalecimiento de la protección de los sistemas de información del Sector Público Nacional.

Para tal fin, el Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar), que depende de la Dirección Nacional de Ciberseguridad de la Subsecretaría de Tecnología de la Información de la Secretaría de Innovación Pública, elaboró esta guía que pretende ser un protocolo de acción para notificar y gestionar aquellos incidentes de ciberseguridad que pudieran afectar a los organismos mencionados, a los CERTs de la Administración Pública Nacional y a todos aquellos que operen en el territorio argentino.

A los fines de la presente guía, se entiende por *incidente de ciberseguridad*[1] *a* la ocurrencia de uno o múltiples eventos relacionados de ciberseguridad identificados que pueden provocar daños a las personas, la sociedad, las organizaciones y las naciones. En tanto, un *evento de ciberseguridad*[2] es un hecho que indica una posible violación de la ciberseguridad o una falla en los controles.

Para la elaboración de este texto, el Equipo, cuyas funciones, acciones y servicios principales se encuentra en el documento RFC-2350- analizó guías y documentos internacionales relacionados con mejores prácticas de ciberseguridad, como los que se mencionan a continuación:

- Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés)
- Organización Internacional de Estandarización (ISO)
- Unión Internacional de Telecomunicaciones (ITU)
- Guía de Mejores Prácticas para la Gestión de Incidentes de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

2. Objetivos

En el marco de las funciones de **CERT coordinador** a nivel nacional, el Equipo de Respuesta ante Emergencias Informáticas de Argentina elaboró esta guía con los siguientes objetivos:

[1] FUENTE: ISO/IEC 27100:2020
[2] FUENTE: ISO/IEC 27100:2020

- Administrar y gestionar toda la información sobre reportes de incidentes de ciberseguridad ocurridos en los organismos del Sector Público Nacional.
- Contribuir a incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de ciberseguridad que puedan afectar activos de información críticos del país.
- Coordinar las acciones a seguir ante incidentes de ciberseguridad, con otros equipos de respuestas a incidentes (CERT/CSIRT) de la República Argentina, particularmente con aquellos que componen la APN.
- Interactuar y cooperar con equipos de similar naturaleza que operen en el país.
- Impulsar la formación de capacidades de prevención, detección, alerta y recuperación para la respuesta ante incidentes de ciberseguridad.
- Proporcionar a los CERTs mencionados y a los Puntos Focales de Ciberseguridad las directrices para notificar y gestionar aquellos incidentes de ciberseguridad que pudieran afectar sus redes, equipos y sistemas informáticos o cualquier otro activo esencial de información.
- Guiar a los organismos públicos alcanzados y a otros equipos de respuesta a incidentes de ciberseguridad para que puedan adoptar e implementar medidas de seguridad, aplicables en sus entornos laborales teniendo en cuenta su tamaño, competencias/modelo de negocio, complejidad y riesgos particulares.
- Proporcionar principalmente a los CERTs/CSIRT y a los Puntos Focales de Ciberseguridad una taxonomía de incifdentes cibernéticos para facilitar el proceso de reporte, el posterior análisis y las fases de contención y erradicación de los mismos.
- Lograr que el personal técnico de los organismos estatales responda de forma rápida, ordenada y eficaz contra aquellos incidentes de ciberseguridad que pudieran afectarlos, para preservar sus activos de información.

3. Alcance

Mediante la implementación de las directrices especificadas en la presente guía, se pretende gestionar de forma coordinada los incidentes de ciberseguridad que afecten a los activos de información. Para tal efecto, se definirán procedimientos y buenas prácticas de ciberseguridad con el fin de contener y mitigar amenazas cibernéticas.

Concretamente, los contenidos de este texto fueron elaborados para cualquier empleado o funcionario que reporte un incidente de ciberseguridad que pueda afectar a los organismos del Sector Público, para los Puntos Focales de Ciberseguridad y para los CERTs de la Administración Pública Nacional. Los lineamientos contenidos en esta guía son recomendados para aquellos CERT/CSIRT que operen en todo el país.

Tales incidentes deberán ser reportados a través de un formulario ubicado en el sitio web CERT.ar, o enviando un correo electrónico a la dirección **reportes@cert.ar**. Las indicaciones de cómo hacerlo se explicarán en el ítem específico del tema. Los Puntos Focales de Ciberseguridad podrán hacerlo también a través de la plataforma que la Dirección Nacional de Ciberseguridad creó específicamente para ellos.

4. Taxonomía y clasificación de un incidente de ciberseguridad

Dado que no todos los incidentes de ciberseguridad tienen las mismas características o implicaciones, resulta necesario disponer de una taxonomía común para la Administración Pública Nacional, con el fin de facilitar el proceso de reporte y el posterior análisis, contención y erradicación.

En consecuencia, se definió la siguiente taxonomía para la clasificación de los incidentes de ciberseguridad que serán reportados al CERT.ar. No obstante, se aclara que en caso de que alguno pueda asociarse con dos o más tipos de incidentes, se clasificará según aquel que mejor se ajuste a la situación acontecida que motiva el reporte.

Clasificación	Tipo	Descripción
Contenido Abusivo	SPAM	Correo electrónico masivo no solicitado.
	Manifestación de odio	Contenido discriminatorio, acoso, amenazas, incitación a la violencia o similar.
	Abuso sexual infantil, contenido sexual.	Material que represente contenido relacionado con el abuso sexual infantil, etc.
Contenido Dañino	Malware	Código malicioso que puede ser distribuido con fines ilegítimos y se instala sin autorización o conocimiento del usuario en equipos que resultan infectados. En este ítem, se encontrarán todos los códigos maliciosos que no estén descritos en otros tipos de la taxonomía.
	Ransomware	Tipo de software malicioso que bloquea el acceso a los datos de la víctima. Quien lo usa puede inclusive publicar y/o difundir la información bloqueada si no se paga el rescate pedido para liberar la información.
	Botnet	Conjunto de hosts conectados a Internet que interactúan con el fin de cumplir una tarea distribuida, que generalmente es maliciosa.
	Command & Control	También llamados C&C o C2, son servidores operados por el/los atacante/s para controlar una botnet.
Obtención de información	Escaneo de redes / análisis de tráfico	Envío de peticiones a un sistema para descubrir vulnerabilidades, obtención del tráfico de red o similar.
	Ingeniería social	Recopilación de información, con el uso o no de la tecnología, en la que el atacante utiliza técnicas de manipulación psicológica o engaños para lograr que la víctima le entregue

		voluntariamente su información.
Intrusión	Explotación de vulnerabilidades	Intento o compromiso de un sistema a través de fallas o ausencia de controles o medidas de seguridad apropiadas.
	Ataque de fuerza bruta	Múltiples intentos de vulnerar credenciales.
	Ataque desconocido	Son aquellos ataques cuya naturaleza no se conoce.
	Compromiso de equipo/sistema	Afectación de la confidencialidad, integridad o disponibilidad de un sistema/aplicación mediante técnicas tales como SQLi, keyloggers, web shell, etc.
	Robo	Intrusión física que concluye con el robo de activos, como pueden ser equipos o información.
	Compromiso de cuenta	Compromiso de un sistema empleando una cuenta con o sin privilegios.
Disponibilidad	Denegación de servicio (DoS/DDoS)	Ciberataque que tiene como objetivo que uno o varios ordenadores, servicios u otros dispositivos no estén disponibles para los usuarios a los que va dirigido, interrumpiendo su funcionamiento normal.
	Configuración errónea	Configuración débil o errónea de un sistema que permita afectar su disponibilidad.
	Sabotaje	Sabotaje físico que puede afectar la disponibilidad de los servicios o de la información. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Afectaciones a la disponibilidad por causas ajenas como desastre natural, condiciones climáticas desfavorables, etc.
Compromiso de la información	Acceso no autorizado a la información	Acceso sin permiso a los activos, como documentos, sistemas, servicios, etc.
	Modificación no autorizada de la información	Alteración no autorizada de la información (creación, modificación o borrado). Esto puede ser causado por ataques de ransomware, queries SQL, etc.
	Pérdida de datos	Pérdida de información sucedida por fallo de hardware.

Indicio de fraude	Uso no autorizado de los recursos	Utilización de los recursos para propósitos inadecuados.
	Derechos de autor	Ofrecimiento o instalación de software, y utilización o difusión de manera ilegítima de material protegido por derechos de autor.
	Suplantación	Ataque mediante el cual una entidad se hace pasar por otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de identidad para la sustracción de datos. Actualmente el phishing se puede clasificar de la siguiente manera: ● **Por correo electrónico:** el phishing por email es el tipo más utilizado y más conocido. ● **Vishing:** este ataque se lleva a cabo a través de una llamada de voz. ● **Whaling:** es un ciberataque dirigido al personal jerárquico de las organizaciones. ● **Smishing:** consiste en mandar un mensaje de texto (SMS) suplantando la identidad del remitente. ● **Basado en malware:** el ciberdelincuente envía un correo electrónico que en sí es el malware. ● **QRishing:** se trata de códigos QR modificados de forma maliciosa.
Activo vulnerable	Sistema vulnerable	Sistema con servicios vulnerables, ya sea por errores de diseño o por no poseer medidas de seguridad o controles apropiados.
	Publicación de servicios vulnerables	Servicios activos expuestos en Internet que pueden ser utilizados para el acceso no autorizado en los sistemas. Ej: RDP, Telnet, etc.
	Revelación de información	Servicios que permiten la obtención de información sensible.
Otros	Amenaza persistente avanzada o APT por sus siglas en inglés	Ataques dirigidos a organizaciones.
	Sectores no críticos	Aquellos incidentes que no puedan ser clasificados dentro de los actuales parámetros.

5. Notificación de incidentes de ciberseguridad

En esta sección se detalla el procedimiento que se deberá realizar cuando se necesite reportar algún incidente al CERT.ar, que funciona en el ámbito de la Dirección Nacional de Ciberseguridad, según lo establece la Disposición N° 1/2021 de esa Dirección. También se incluye el detalle de la información a comunicar, los criterios que se sugieren emplear y una referencia a la forma de asignación de los niveles de impacto y criticidad según cada caso.

Al respecto, cabe aclarar que las entidades y jurisdicciones del Sector Público Nacional deberán reportar a la Dirección Nacional de Ciberseguridad los incidentes de seguridad que se produzcan en el interior de sus ámbitos, dentro de las CUARENTA Y OCHO (48) horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia.

Para viabilizar el mencionado reporte, la Dirección Nacional puso a disposición la cuenta de correo electrónico reportes@cert.ar, que podrá ser utilizada por los CSIRTs pertenecientes a la Administración Pública Nacional, los Puntos Focales de Ciberseguridad y por aquellos funcionarios y empleados de organismos del Sector Público Nacional.

Además, para los Puntos Focales, se ha habilitado también un canal de comunicación dentro de la plataforma de la Dirección Nacional de Ciberseguridad.
Quienes no formen parte de la categoría anterior, podrán reportar sus incidentes a través de un formulario que está disponible en el sitio web cert.ar.

Por otro lado, se explica que en el caso de incidentes de ciberseguridad reportados -que afecten organismos públicos nacionales-, cuando quien informe no sea un Punto Focal de Ciberseguridad, se procederá a validar la información recibida con el representante designado, ni bien esto sea posible.

Es importante destacar que los reportes de incidentes de ciberseguridad serán tratados por la Dirección Nacional de Ciberseguridad, por el CERT.ar y todo su personal como documentación confidencial. Se procederá siempre así, especialmente, cuando se trate de datos que pudieran exponer los del organismo y pongan en riesgo su seguridad y el ejercicio de sus competencias, así como también la información de usuarios en conformidad con la legislación vigente sobre protección de datos personales.

5.1 Criterios para la notificación

Para la notificación inicial de los incidentes de ciberseguridad, se utilizará como criterio de referencia el **Nivel de criticidad** que se asigne a un incidente y su **Nivel de impacto** estimado. Sin embargo, a lo largo del ciclo de vida del incidente, los valores correspondientes a esta evaluación inicial pueden ser modificados para reflejar la situación real según cada caso.

A manera de ejemplo, si se afecta un recurso considerado esencial para el funcionamiento de un servicio que es crítico para la ciudadanía o para la gestión interna del organismo, o si se afecta a otro organismo o a organizaciones cuya actividad es vital para la población, etc. Adicionalmente se considera la urgencia, es decir los tiempos máximos aceptables para la gestión del incidente, determinados por la necesidad de contar con el servicio activo.

A continuación se detallan los lineamientos para determinar estos dos criterios.

5.1.1 Criterios para determinar el nivel de criticidad

Los criterios para la adopción del nivel de criticidad de un incidente estarán dados por el tipo de incidente y el nivel de criticidad que cada organismo le otorgue al activo de información afectado.

A continuación se enumeran los niveles a considerar:

Nivel	Detalle
1	Bajo
2	Medio
3	Alto
4	Crítico

Niveles de criticidad.

Dependiendo de la prioridad, se asignarán los recursos necesarios para su gestión, a su vez es posible que la criticidad pueda cambiar durante el ciclo de vida del incidente.

Nivel	Clasificación	Tipo
Crítico	Otros	Amenaza persistente avanzada - APT
Alto	Contenido dañino	Malware
		Ransomware
		Command & Control
	Disponibilidad	Sabotaje
		Interrupciones
		Denegación de servicio (DoS/dDoS).
	Contenido abusivo	Abuso sexual infantil, contenido sexual.
	Intrusión	Robo
		Explotación de

		vulnerabilidades
		Ataque de fuerza bruta
		Ataque desconocido
		Compromiso de equipo/sistema
	Compromiso a la información	Acceso no autorizado a la información
		Modificación no autorizada de la información
		Pérdida de datos
	Indicio de fraude	Phishing
Medio	Contenido dañino	Botnet
	Intrusión	Compromiso de cuenta
	Contenido abusivo	Manifestación de odio
	Obtención de información	Ingeniería social
	Disponibilidad	Configuración errónea
	Indicio de fraude	Uso no autorizado de los recursos
		Derechos de autor
		Suplantación
	Activo vulnerable	Sistema vulnerable
		Publicación de servicios vulnerables
		Revelación de información
Bajo	Contenido abusivo	SPAM
	Obtención de información	Escaneo de redes / análisis de tráfico
	Otros	Sectores no críticos

5.1.2 Criterios para determinar el nivel de impacto

El impacto que pudiera tener un incidente estará determinado por aspectos tales como el tipo de proceso que afecte, la cantidad y características de usuarios cuyos datos fueron comprometidos y las competencias propias del organismo.

5.2 Alcance de difusión de información mediante el protocolo TLP

Traffic Light Protocol o Protocolo de Semaforización de Tráfico (TLP en adelante) es un esquema de señalización diseñado para el intercambio de información de una manera ágil, delimitando el alcance para su correcta difusión.

TLP está conformado por un esquema simple e intuitivo que menciona el grado de sensibilidad de la información para indicar con quién se puede compartir, facilitando la colaboración con otras organizaciones a nivel nacional e internacional. En el tratamiento de los incidentes, se indicará la señalización de TLP para facilitar dicho intercambio, en los casos que sea necesario.

El siguiente cuadro especifica el protocolo TLP en su versión 2.0.

Código	Cuándo utilizarlo	Cómo compartirlo	Color	Fondo
TLP: RED	Cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones en caso de ser mal utilizada.	Sólo para los ojos y oídos de los destinatarios individuales, fuera de los cuales no está autorizada su divulgación. Los receptores no deben compartir este tipo de información con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff0033	#000000
TLP: AMBER	Cuando la información requiere ser distribuida de forma limitada. Si la divulgación de la misma se realiza por fuera de la organización puede suponer un riesgo para la privacidad, reputación u operaciones del organismo y de	Divulgación limitada. Los receptores sólo pueden difundir esta información dentro de su organización, sobre la base de la necesidad de saber y con sus usuarios, proveedores o asociados que deban estar al tanto para protegerse a sí	#ffc000	#000000

	terceros afectados.	mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.		
TLP: AMBER +STRICT	Cuando la información requiere ser distribuida de forma limitada. Si la divulgación de la misma se realiza por fuera de la organización puede suponer un riesgo para la privacidad, reputación u operaciones del organismo y de terceros afectados.	Divulgación limitada. La fuente restringe el uso compartido sólo a la organización.	#ffc000	#000000
TLP: GREEN	Cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Divulgación limitada. Los receptores pueden difundir esto dentro de su comunidad. Los receptores pueden compartir este tipo de información con organizaciones afiliadas o miembros del mismo sector, pero no a través de canales públicos.	#33ff00	#000000
TLP: CLEAR	Cuando la información es útil para todas las organizaciones que participan, así como terceros de la comunidad o el sector.	Los receptores pueden difundir esto al mundo, no hay límite en la divulgación.	#ffffff	#000000

5.3 Contenido de los reportes

Existen dos tipos de reportes que se deben realizar y ser remitidos al CERT.ar: uno es el inicial y el otro el que se debe hacer al final del proceso de la gestión del incidente.
El primero es aquel que se hará en el marco de las 48 horas de ocurrido el incidente, y se debe informar mediante alguno de los canales habilitados por el CERT.ar para tal fin.
El segundo se elaborará al cerrarse el incidente, es decir, cuando finalice el proceso correspondiente a su gestión y, luego, se genere un informe final que detalle en mayor medida lo acontecido.

5.3.1 Contenido del reporte inicial

Los mensajes de correo electrónico utilizados para el reporte inicial de los incidentes de ciberseguridad deberán contener la siguiente información básica:

1. Breve resumen del incidente de ciberseguridad.
2. Identificación del organismo o institución y la instalación o dependencia afectada.
3. Nombre y datos de contacto (dirección, teléfono, etc.) del Punto Focal de Ciberseguridad o encargado de ciberseguridad del organismo o de quien reporta el incidente.
4. Fecha y hora estimada de detección del incidente de ciberseguridad.
5. Descripción detallada de lo sucedido.
6. Taxonomía, clasificación o tipo de incidente de ciberseguridad, según la sección 4 de esta guía.
7. Nivel de criticidad, de acuerdo a lo establecido en el punto 5.1.1.
8. Nivel de impacto estimado de acuerdo a lo establecido en el punto 5.1.2.
9. Recursos afectados, incluyendo hardware, software, datos, documentos, etc.
10. Indicadores de compromiso: de compromiso de nivel IP, de nivel de dominios y subdominios, de compromiso de correos o a nivel MD5, entre otros similares.
11. Entidades afectadas actuales y potenciales, tanto se trate de organizaciones o personas internas o externas al organismo.
12. Logs generados de forma automática por los sistemas, si corresponde.

Es posible que no se cuente con la información requerida en los puntos 8, 9, 10, 11, 12 y 13 al momento del reporte inicial, pero en caso de poseerla se espera sea informada en el mismo. De lo contrario y de resultar pertinente, podrá ser remitida con posterioridad. Del mismo modo, cualquier otro dato provisto puede ser actualizado mediante las comunicaciones posteriores con el CERT.ar.

5.3.2 Contenido del reporte final

A los efectos del cierre del incidente, se deberá proveer reportes finales detallando lo acontecido en el incidente de ciberseguridad. Deberán contener la siguiente información:

1. Resumen ejecutivo del incidente de ciberseguridad.
2. Identificación del organismo o institución y de la instalación o dependencia afectada.
3. Nombre y datos de contacto (dirección, teléfono, etc.) del Punto Focal de Ciberseguridad o encargado de ciberseguridad del organismo o de quien reporta el incidente. De ser posible, el informe de cierre del incidente de ciberseguridad deberá

ser remitido por el Punto Focal, aunque no fuera éste quien hubiera enviado el reporte inicial.
4. Fecha y hora precisas de ocurrencia del incidente de ciberseguridad, si se conociere.
5. Fecha y hora precisas de detección del incidente de ciberseguridad.
6. Descripción detallada de lo sucedido.
7. Recursos afectados, incluyendo hardware, software, datos, documentos, etc.
8. Origen o causa identificable del incidente de ciberseguridad, si se conociere.
9. Taxonomía, clasificación o tipo de incidente de ciberseguridad, según la sección 4 de esta guía.
10. Nivel de criticidad, de acuerdo a lo establecido en el punto 5.1.1.
11. Nivel de impacto estimado de acuerdo a lo establecido en el punto 5.1.2.
12. Indicadores de compromiso: de compromiso de nivel IP, de nivel de dominios y subdominios, de compromiso de correos o a nivel MD5, entre otros similares.
13. Plan de acción y medidas de resolución y mitigación adoptadas.
14. Entidades afectadas actuales y potenciales, tanto se trate de organizaciones o personas internas o externas al organismo.
15. Medios necesarios para la resolución calculados en horas de trabajo necesarias.
16. Impacto económico estimado, si procede y es conocido.
17. Cantidad de unidades operativas o áreas del organismo afectadas, si se conociere.
18. Posibles daños reputacionales, aun cuando sean eventuales.
19. Logs generados de forma automática por los sistemas, si corresponde y si no fueron enviados previamente.
20. Antecedentes, si procede. Se podrá adjuntar toda la información que se considere pertinente al proceso de gestión del incidente.
21. Clasificación de confidencialidad TLP asignada al incidente y consignada en el asunto (Ver punto 7.4).

Se aclara que durante el proceso de gestión del incidente, el CERT.ar podrá comunicarse con el organismo afectado para solicitar mayor información. Del mismo modo, el organismo podrá remitir cualquier información o documento que a su entender pueda contribuir a mitigar y contener el incidente.

5.3.3 Reporte mediante el formulario online.

Para quienes quieran reportar un incidente o vulnerabilidad de forma anónima o no, se brinda la posibilidad de realizarlo mediante el formulario online disponible en la página del CERT.ar
https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/reportar-un-incidente.

Se deberán consignar los siguientes datos:

1. Tipo de incidente: es un campo obligatorio que contiene las siguientes opciones:
    a. sitio web
    b. compromiso de un activo de información
    c. compromiso de una red informática
    d. phishing

    e. spam
    f. ransomware
    g. malware/virus informático
2. Severidad: es un campo opcional que contiene los siguientes niveles para elegir:
    a. ninguno
    b. bajo
    c. medio
    d. alto
    e. crítico
3. Título del incidente (obligatorio)
4. Descripción (obligatorio)
5. Debilidad (opcional)
6. Impacto (opcional)
7. Correo electrónico (opcional)

5.4 Estados de un incidente

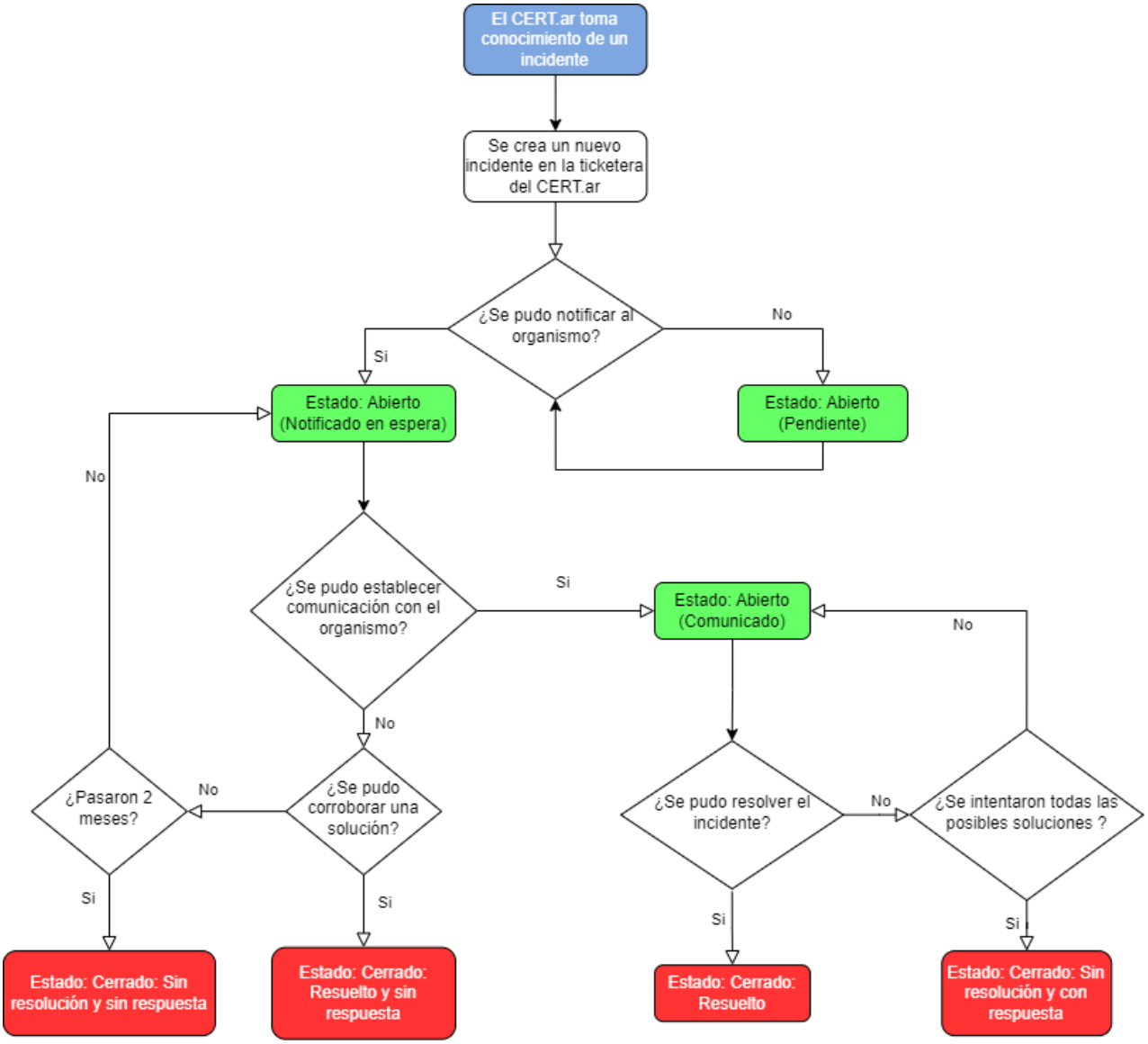
5.4.1 Estados de seguimiento

A continuación, se detallan los diferentes estados de seguimiento para los incidentes gestionados.

Estado	Detalle
Abierto pendiente	El caso se encuentra abierto y pendiente de ser notificado.
Abierto notificado / en espera	El caso fue notificado y se aguarda su respuesta por parte de los destinatarios.
Abierto comunicado	El caso fue notificado y se establecieron comunicaciones para su mitigación.
Cerrado resuelto	El caso se encuentra cerrado porque el organismo afectado pudo solucionar el incidente y notificar la situación.
Cerrado resuelto y sin respuesta	El caso se encuentra cerrado porque no hay respuesta por parte del organismo, sin embargo, se puede corroborar que el incidente fue resuelto.
Cerrado sin resolución y con respuesta	El caso se encuentra cerrado porque el organismo se ha comunicado, pero no se ha podido resolver el incidente, incluso, con las indicaciones proporcionadas.
Cerrado sin resolución y sin respuesta	El caso se encuentra cerrado porque -luego de transcurridos los dos meses de su creación-, el organismo no se ha comunicado y no se puede

	corroborar la resolución del incidente.

El siguiente gráfico es un diagrama de flujo que detalla el ciclo de vida de los estados de un incidente durante su proceso de gestión. Se resaltan en verde los estados de abierto y en rojo los de cerrado.



5.4.2 Estados de cierre

A continuación, se detallan los diferentes estados que puede tener un incidente de ciberseguridad al momento de su cierre.

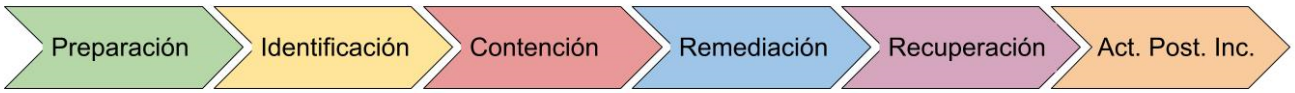
Estado	Detalle
Cerrado positivo	El caso se encuentra cerrado porque se identificó actividad maliciosa.
Cerrado falso positivo	El caso se encuentra cerrado porque no se identificó actividad maliciosa.
Cerrado indeterminado	El caso se encuentra cerrado porque no es posible determinar actividad maliciosa.
Cerrado otro	El caso se encuentra cerrado porque no se clasifica como incidente y no requiere investigación.
Abierto	El caso se encuentra abierto, en proceso de trabajo o aún sin atender.

En todos los casos se deberán documentar los motivos que llevaron al cierre del incidente de ciberseguridad y la determinación del estadio.

6. Gestión de un incidente de ciberseguridad

La gestión de incidentes de ciberseguridad es el conjunto ordenado de acciones tendientes a contener su impacto y restablecer lo antes posible los niveles de operación. Se encuentra fuertemente ligado al concepto de “resiliencia”. El proceso de gestión de incidentes está compuesto por diferentes etapas o fases que suelen realizarse en forma consecutiva. Sin embargo, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea.

El siguiente esquema muestra las etapas antes citadas:



A continuación se describen brevemente cada una de ellas.

6.1 Preparación

La fase de preparación para atender el incidente es una etapa inicial que permite anticipar y entrenar al personal del equipo de respuesta a incidentes de seguridad para atender cualquier evento que pudiera presentarse.
Tiene en cuenta tres pilares fundamentales que son las personas, los procedimientos y la tecnología.

Reúne aquellas actividades proactivas que permiten una mejor atención y respuesta frente a un incidente y comprende, entre otras, las siguientes acciones:

- Entrenamiento y capacitación del personal del equipo con el fin de mejorar las capacidades técnicas y operativas.
- La adopción de estándares y generación y actualización de políticas y procedimientos. Especialmente todos los relativos a gestión de incidentes, recogida de evidencias, análisis forense y recuperación de sistemas.
- La identificación e implementación de herramientas para el tratamiento de los incidentes a utilizar en todas las fases.
- La identificación y establecimiento de canales de comunicación, el escalamiento y el relevamiento de información útil para cada tipo de incidente. Ej: disponer de los datos actualizados de contactos, tanto del personal interno como de los posibles involucrados.
- Realizar un análisis de riesgos que permita disponer de un plan de tratamiento para controlarlos, mitigarlos, transferirlos o aceptarlos.
- Realizar ejercicios que permitan entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación.

6.2 Identificación

La fase de identificación se refiere a la capacidad de identificar o detectar un incidente, incluye el monitoreo, la recolección de información, y toda aquella actividad que permita identificar los hechos, determinar el alcance e involucrar a las partes apropiadas.
Una correcta identificación y detección se basa en:

- Mantener un registro y monitorizar los eventos de redes, sistemas y aplicaciones.
- Recolectar la información y toda aquella actividad que permita identificar los hechos y anomalías.
- Determinar el alcance e involucrar a las partes apropiadas.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir la información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

6.3 Contención

La fase de contención es aquella donde se toman las medidas para limitar y aislar el impacto del incidente, incluye aquellas actividades que permitan evitar la propagación y los efectos del incidente.

En esta etapa se suele realizar el triage que consiste en evaluar toda la información disponible en ese momento, realizar una clasificación y priorizar el incidente en función del tipo y la criticidad de la información y los sistemas afectados.
Dependiendo del tipo de incidente, se aislará el equipo de la red, se extraerán indicadores de compromiso, se corregirán las fallas y se aplicarán parches, etc.

6.4 Mitigación o remediación

La fase de mitigación o remediación agrupa las acciones necesarias para eliminar la amenaza e incluye las actividades que permitan determinar las medidas de mitigación más eficaces, las cuales dependerán del tipo de incidente. En algunos casos podría ser necesario contar con el apoyo de proveedores de servicios, o realizar una recuperación desde una copia de seguridad.
Como recomendaciones generales para esta fase se puede:

- Determinar las causas y síntomas del incidente para establecer las medidas de mitigación más eficaces.
- Identificar y eliminar todo el software utilizado por los atacantes. Dependiendo del incidente, esto puede implicar el formateo de la máquina debido a que es la forma que ofrece mayores garantías.
- Recuperar la última copia de seguridad.
- Identificar servicios utilizados durante el ataque. En algunas ocasiones, los atacantes utilizan servicios legítimos de los sistemas atacados.

6.5 Recuperación

La fase de recuperación involucra la implementación de procedimientos y actividades que permitan volver a una operatoria normal y que las áreas afectadas puedan retomar su actividad.
Dentro de estas actividades, se pueden incluir la publicación de servicios, la conexión de los equipos a la red, la restauración de archivos, la reinstalación o restauración de sistemas, entre otras.
En esta etapa, se aconseja no precipitarse en la puesta en producción de aquellos sistemas que se han visto implicados en ciberincidentes, y se indica buscar en los mismos cualquier signo de actividad sospechosa, definiendo un período de tiempo con medidas adicionales de monitorización.

6.6 Post-incidente

Una vez controlado el incidente y con la operatoria normalizada, se debe reflexionar sobre las lecciones aprendidas. Concretamente, se analizará todo lo sucedido, tanto las causas del incidente y los problemas asociados, como la gestión del mismo, para identificar e implementar medidas de mejora.
Además se debe corroborar la correcta documentación de todo lo sucedido y elaborar el informe correspondiente.

7. Buenas prácticas para la denuncia de incidentes de ciberseguridad

Con el fin de denunciar un incidente de ciberseguridad, se podrán seguir los pasos que están indicados en un documento que habla sobre el tema y se encuentra disponible en https://www.argentina.gob.ar/servicio/denunciar-un-delito-informatico o en el sitio que lo reemplace en el futuro.

7.1 Evidencia digital

En la sección anterior, se mencionó en la fase de Identificación del incidente de ciberseguridad que se sugiere recopilar y almacenar de forma segura todas las evidencias, por lo que en este punto se explicará brevemente el tema y se brindarán buenas prácticas sobre la temática.

7.1.1 Concepto

En el marco de una investigación, la evidencia digital[3] es cualquier información pertinente que fue extraída de un medio tecnológico informático mediante una intervención humana, electrónica y/o informática. Se trata de un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Se caracteriza por ser volátil, frágil, fácil de alterar, dañar o destruir.

A diferencia de otras evidencias físicas, se la puede duplicar de manera exacta sin alterar la versión original y, en algunos casos, su localización puede ser muy dificultosa.
Asimismo, en los procesos judiciales, presenta problemas jurídicos vinculados con el derecho a la intimidad, el secreto de las comunicaciones y las posibles afectaciones de terceras personas, etc.

En su estado natural, este tipo de evidencia no deja ver la información que contiene en su interior, por lo que resulta ineludible examinar a través de instrumentos y procesos forenses específicos.

Por tal motivo, se sugiere tomar precauciones especiales cuando sea necesario recolectar, manipular, documentar y examinar esta información, para evitar que sea invalidada o se muestre imprecisa, ya sea en un proceso administrativo, judicial o en cualquier otro sector donde se la requiera por su valor probatorio.

7.1.2 Principios generales en el manejo de la evidencia digital

La evidencia digital debe poseer cuatro características esenciales denominadas relevancia, suficiencia, validez legal y confiabilidad para el correcto tratamiento de la misma. Se trata de principios generales que se deben cumplir en el manejo y tratamiento de este tipo de información digital. En otras palabras, se puede decir que son elementos que definen la formalidad de cualquier investigación basada en evidencia digital.

Relevancia: la evidencia debe ser útil para las necesidades investigativas y/o los puntos probatorios de cada caso concreto. Este principio opera fundamentalmente como criterio de selección de evidencia, por lo tanto, el experto a cargo debería saber qué lugar ocupa una determinada evidencia en el plan de investigación penal y/o en la actividad de litigación del fiscal.

[3] http://redi.ufasta.edu.ar:8082/jspui/bitstream/123456789/1592/2/PAIF.pdf

Suficiencia: las evidencias obtenidas y eventualmente analizadas deberían ser suficientes para lograr los fines investigativos buscados mediante ellas, y/o para convencer al tribunal acerca de los puntos para los cuales fueron ofrecidas como prueba. Frente a situaciones dudosas, deberá consultarse con el director de la investigación.

Validez legal. Para que la evidencia sea admisible, debe haber sido obtenida respetando las garantías y formas legales, motivo por el cual el experto que la utilice debe cumplir con las disposiciones legales y reglamentarias propias de su actuación.
Asimismo, se deberá constatar la previa autorización judicial o la orden del director de la investigación cuando una acción implique injerencia en derechos fundamentales, como por ejemplo secuestro de dispositivos, análisis de comunicaciones personales, etc.

Confiabilidad: la evidencia debe ser convincente, apta para probar lo que se pretende con ella. Esto se refiere no sólo a las características que una evidencia digital posee en sí misma, sino también a los procedimientos de obtención, preservación, análisis y presentación ante el tribunal. Para asegurar la confiabilidad, el proceso de manejo de evidencia digital debe ser justificable, auditable, repetible y reproducible.

A fin de cumplir con esos principios, se sugiere observar las siguientes pautas:

- Debe minimizarse el manejo de la evidencia digital original con valor investigativo y/o probatorio. Por tal motivo, si es necesario acceder a los datos originales, el especialista debe ser competente para hacerlo y capaz de atestiguar explicando la importancia y las implicaciones de sus acciones.
- Cualquier acción que implique una alteración irreversible de la evidencia debe ser previamente informada al director de la investigación, y debidamente documentada.
- Quien realice cada acción o cambio vinculado con evidencia digital debe responsabilizarse de lo actuado y documentarlo en forma fidedigna.

Para más información, se indica leer el “Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital”, que se incluye en la Resolución 232/2023 del Ministerio de Seguridad de la Nación.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2023-69993929-APN-SSTI#JGM

CIUDAD DE BUENOS AIRES
Viernes 16 de Junio de 2023

Referencia: ANEXO I - Guía de Notificación y Gestión de Incidentes de Ciberseguridad

---

El documento fue importado por el sistema GEDO con un total de 20 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.16 18:13:04 -03:00

Agustina BRIZIO
Subsecretaria
Subsecretaría de Tecnologías de la Información
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2023.06.16 18:13:05 -03:00