Guía para la gestión de incidentes

Información del documento:

Título	Guía para la gestión de incidentes
Identificador	CERTar-RCM-GGI-001
Clasificación	Público
Versión	V 0
Fecha	22/09/2021
Aprobación	RLL

Control de cambios:

Versión	Fecha	Autor	Descripción
V 0	22/09/2021	RLL; SP; FD	Elaboración de documento

Contenido

1. Objetivo

El presente documento lleva como objetivo delinear los aspectos claves y buenas prácticas para la elaboración de una política de clasificación de incidentes que permita la gestión de los mismos.

2. Alcance

Aquellos incidentes identificados o notificados a la organización/equipo de respuesta.

3. Definiciones y abreviaturas

A los efectos prácticos del presente documento se utilizan las siguientes definiciones y/o abreviaturas. Para un mayor detalle o complementación revisar el Glosario de Términos de Ciberseguridad (Anexo II IF-2019-78455467-APN-SGM#JGM) de la Resolución 1523/2019.

Botnets: conjunto de dispositivos que son controlados en forma remota por un atacante. Son utilizadas mayormente para realizar ataques de denegación de servicio distribuidos (dDoS) o bien para exfiltrar información.

Comando y Control (C&C): servidor central utilizado para la administración remota de botnets y efectuar el envío de instrucciones que ejecutarán dichos dispositivos.

Denegación de servicio: conjunto de técnicas que tienen por objetivo dejar un servicio inaccesible o un servidor fuera de operación. Este tipo de ataques puede ser realizado de manera simultánea por n atacantes (Denegación de Servicio distribuido / dDoS)

Incidente de seguridad: evento que tiene un efecto adverso en la seguridad de una red o sistema. Una violación o inminente amenaza de violación de una política de seguridad de la información.

Indicadores de compromiso (IoC): refiere a una estandarización de características para el intercambio de información. Sobre un sistema comprometido se identifican determinados artefactos (servicios, procesos, registros) a fin de identificar otros dispositivos comprometidos por la misma amenaza o implementar medidas de prevención.

Organización: refiere tanto a organismos públicos como a organizaciones del ámbito privado.

RDP (Remote Desktop Protocol): Protocolo propietario de Microsoft utilizado para la administración remota de equipos. RDP permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor.

SQL-i (SQL injection): Una inyección SQL es un tipo de ataque que hace uso de una vulnerabilidad en la validación de los datos introducidos en una aplicación (EJ formulario web), entre otros usos es utilizada para la obtención y/o modificación de datos almacenados en bases de datos.

4. Documentos relacionados

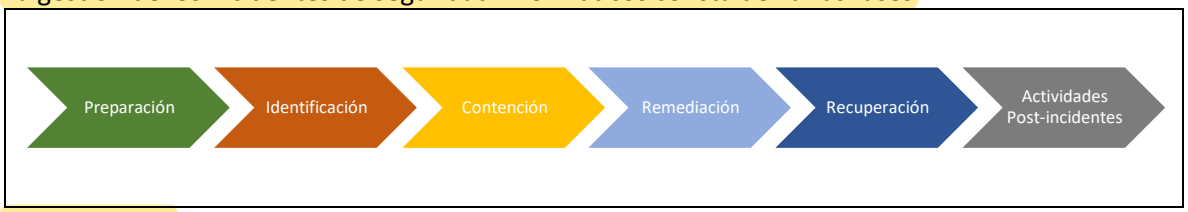
.-

5. Tratamiento de incidentes

A continuación se realiza una descripción de la clasificación de los incidentes, el ciclo de vida, los criterios de evaluación, tipos y formas de comunicar para un correcto tratamiento de incidentes.

5.1. Ciclo de vida de la respuesta a incidentes

La gestión de los incidentes de seguridad informáticos consta de varias fases.



Preparación: Fase de preparación para atender el incidente.
Aquellas actividades proactivas que permitan una mejor atención y respuesta frente a un incidente: entrenamiento, procedimientos actualizados, herramientas, estándares e información útil para cada incidente, entre otras actividades.
Identificación: Detección del incidente.
Refiere a la capacidad de identificar o detectar un incidente, incluye el monitoreo, recolección de información, y toda aquella actividad que permita identificar los hechos, determinar el alcance e involucrar a las partes apropiadas.
En esta etapa también corresponde efectuar la identificación de los indicadores de compromiso (IoC).
Contención: Medidas para limitar y aislar el impacto del incidente sobre los recursos o información de la organización.
Aquellas actividades que permitan evitar la propagación y efectos del incidente. Dependiendo el tipo de incidente se aislará el equipo de la red; se extraerán indicadores de compromiso; se corregirán los fallos; se aplicarán los parches; etc.
Remediación: Medidas para eliminar la vulnerabilidad.
Actividades que permitan determinar las medidas de mitigación más eficaces las cuales dependerán del tipo de incidente.
Recuperación: Procedimientos para volver a una operatoria estable.
Actividades que permitan volver al nivel de operación a su estado normal, publicación de servicios; conexión del equipo a la red; restauración de archivos; reinstalación de sistemas; entre otros.
Actividades Post-incidentes: Identificar e implementar medidas de mejora.
Aquellas tareas que permitan identificar las lecciones aprendidas del incidente, mejorar los procedimientos, técnicas, elaboración de informes, presentaciones, etc.

5.2. Clasificación de incidentes

A fin de facilitar la identificación, gestión y seguimiento de los incidentes es recomendable efectuar una clasificación que permita agrupar por tipo de incidente.

A modo de ejemplo, se podría utilizar la siguiente clasificación:

Clasificación	Tipo	Descripción
Contenido Abusivo	SPAM	Correo electrónico masivo no solicitado.
	Delito de odio	Contenido discriminatorio, acoso, amenazas, incitación a la violencia.
	Abuso sexual infantil, contenido sexual	Material que represente contenido relacionado con el abuso sexual infantil, etc.
Contenido Dañino	Malware	Distribución de malware, equipo infectado, C&C
Obtención de información	Escaneo de redes / análisis de tráfico	Envío de peticiones a un sistema para descubrir vulnerabilidades, obtención del tráfico de red.
	Ingeniería social	Recopilación de información personal sin uso de la tecnología.
Intrusión	Explotación de vulnerabilidades	Intento o compromiso de un sistema a través de vulnerabilidades.
	Ataque de Fuerza Bruta	Múltiples intentos de vulnerar credenciales.
	Ataque desconocido	Aquellos ataques de naturaleza desconocida.
	Compromiso de equipo/sistema	Compromiso de un sistema/aplicación como pueden ser las técnicas de SQLi, keyloggers, web shell, etc.
	Robo	Intrusión física.
Disponibilidad	Denegación de Servicio (DoS/dDoS)	Ataque de denegación de servicio
	Configuración errónea	Configuración débil o errónea de un sistema que permita afectar su disponibilidad.
	Sabotaje	Sabotaje físico.
	Interrupciones	Afectaciones a la disponibilidad por causas ajenas: desastre natural, condiciones climáticas desfavorables, etc.
Compromiso de la información	Acceso no autorizado a la información	Robo de credenciales o acceso a documentos sin autorización.
	Modificación no autorizada de la información	Modificación no autorizada: ataques por Ransomware, modificación de archivos, SQLi, etc.
	Perdida de datos	Perdida de información: fallo de hardware.
Fraude	Uso no autorizado de los recursos	Uso de los recursos para propósitos inadecuados.
	Derechos de autor	Ofrecimiento o instalación de software, utilización o difusión de material protegido por derechos de autor.
	Suplantación	Ataque que suplanta a una entidad.

Clasificación	Tipo	Descripción
	Phishing	Suplantación de identidad para la sustracción de datos
Vulnerable	Sistema vulnerable	Sistema con servicios vulnerables
	Publicación de servicios vulnerables	Servicios activos que puedan ser utilizados para el acceso no autorizado en los sistemas: RDP, Telnet, etc.
	Revelación de información	Servicios que permitan la obtención de información sensible
Otros	APT	Ataques dirigidos a organizaciones
	Otros	Aquellos incidentes que no puedan ser clasificado dentro de los actuales parámetros

5.3. Criterios de evaluación

Los criterios para la adopción del nivel de severidad de un incidente estarán dados por el tipo de incidente y la criticidad del recurso afectado. Se considerará el impacto del incidente, lo cual refiere a la importancia del mismo, en base al impacto potencial o real adverso sobre las infraestructuras tecnológicas, los sistemas de información y los datos que gestionen, especialmente aquellos que comprometan datos personales o críticos de la organización, entidad o jurisdicción, que representen un incumplimiento de la normativa vigente o afecten los servicios vinculados a funciones sustantivas de su competencia; adicionalmente se considera la urgencia, es decir los tiempos máximos aceptables para la gestión del incidente.

Nivel	Detalle
1	Bajo
2	Medio
3	Alto
4	Crítico

Niveles de severidad.

Dependiendo de la prioridad se asignarán los recursos necesarios para su gestión, a su vez es posible que la severidad pueda cambiar durante el ciclo de vida del incidente.
Dependiendo el tipo de incidente, comunidad objetivo, activos, el nivel de severidad asignado al tipo de incidente podrá variar.

Ejemplo

Si el impacto trasciende la organización el nivel será Crítico (4)
Si afecta a toda la organización será Alto (3)
Si afecta a un área crítica será Medio (2)

A modo de ejemplo se presenta el siguiente cruce de nivel de clasificación y tipo de incidente:

Nivel	Clasificación	Tipo
Crítico	Otros	APT
Alto	Contenido Dañino	Malware
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
	Contenido Abusivo	Abuso sexual infantil, contenido sexual
	Intrusión	Explotación de vulnerabilidades
		Ataque de Fuerza Bruta
		Ataque desconocido
		Compromiso de equipo/sistema
	Disponibilidad	Denegación de Servicio (DoS/dDoS)
	Compromiso a la información	Acceso no autorizado a la información
		Modificación no autorizada de la información
		Perdida de datos
	Fraude	Phishing
MEDIO	Contenido Abusivo	Delito de odio
	Obtención de Información	Ingeniería social
	Disponibilidad	Configuración errónea
	Fraude	Uso no autorizado de los recursos
		Derechos de autor
		Suplantación
	Vulnerable	Sistema vulnerable
		Publicación de servicios vulnerables
		Revelación de información
BAJO	Contenido Abusivo	SPAM
	Obtención de Información	Escaneo de redes / Análisis de tráfico
	Otros	Otros

5.4. Estados de un incidente

Es recomendable definir cuáles son los estados que puede tener un incidente. A modo de ejemplo se presentan los siguientes:

Estado	Detalle
Cerrado (Positivo)	El caso se encuentra cerrado. Se identificó actividad maliciosa.
Cerrado (Falso positivo)	El caso se encuentra cerrado. No se identificó actividad maliciosa.
Cerrado (Indeterminado)	El caso se encuentra cerrado. No es posible determinar actividad maliciosa.
Cerrado (Otro)	El caso se encuentra cerrado. No clasifica como incidente, no requiere investigación.
Abierto	El caso se encuentra abierto, en proceso de trabajo o aún sin atender.

En todos los casos se deberá realizar una descripción que motiva el cierre o determinación del estadio.

5.5. Traffic Light Protocol (TLP)

Traffic Light Protocol (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 es un esquema simple e intuitivo que indicar el grado de sensibilidad de la información sobre seguridad que va a ser compartida, 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.

TLP establece cuatro niveles:

Código	Cuándo utilizarlo	Color	Fondo
TLP: RED	Se debe utilizar TLP: RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	#ff0033	#000000
TLP: AMBER	Se debe utilizar TLP: AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	#ffc000	#000000
TLP: GREEN	Se debe utilizar TLP: GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	#33ff00	#000000
TLP: WHITE	Se debe utilizar TLP: WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	#ffffff	#000000

5.6. Comunicaciones, reportes y alertas

Para la notificación de incidentes, por ejemplo con el CERT.ar, se recomienda la adopción de las siguientes buenas prácticas:

- Señalización de la información con TLP (indicado en punto anterior)
- La evidencia relacionada al evento o incidente sean formateados de manera tal que no comprometa a los destinatarios.
    - IP/URL asociadas: <###.###.###[.]###>
    - Links: hxxps://ejemplo[.]com
- Indicadores de compromiso (IoC): se recomienda adjuntar los indicadores identificados durante el incidente. El intercambio de este tipo de información dinamiza la colaboración entre las distintas áreas de seguridad, equipos de respuesta a incidentes, etc.
- Información sensible: En caso de considerar que la información a comunicar puede comprometer a la Organización o a terceros, adoptar el uso de protocolos de cifrado como PGP.

6. Referencias

Argentina 2019. Glosario de Términos de Ciberseguridad. Resolución 1523/2019. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Argentina. 2021. CENTRO NACIONAL DE RESPUESTA A INCIDENTES INFORMÁTICOS (CERT.ar.). Disposición 1/2021. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/241077/20210222

Argentina. 2021. Disposición 7/2021. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/248361/20210819

España. 2020. Esquema Nacional de Ciberseguridad. Gestión de ciberincidentes. Centro Criptológico Nacional. Recuperado de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Estados Unidos. 2012. NIST SP 800-61 - Computer Security Incident Handling Guide. Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

ISO/IEC. 2016. ISO/IEC 27035 - information security (cybersecurity) incident management. Recuperado de https://www.iso.org/standard/60803.html y https://www.iso.org/standard/62071.html

LACNIC. 2012. Manual Básico de: Gestión de incidentes de seguridad informática. Uruguay. Recuperado de https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

7. Anexo

A modo de ejemplo se adjunta formulario de reporte incidentes:

CERTar-FRM-REPIN-001.docx