CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 817

Esquema Nacional de Seguridad.
Gestión de ciberincidentes

Abril 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.04.22 18:43:34 +02'00'

NIPO: 785-18-022-8

Fecha de Edición: abril de 2020
El Sr. Carlos Galán, el Sr. José Antonio Mañas e Innotec System han participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

Entre los elementos más significativos del actual escenario nacional e internacional se encuentran el incesante desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) y, correlativamente, el incremento de los riesgos derivados de su utilización. Esta realidad exige al Sector Público garantizar el uso adecuado de las herramientas tecnológicas para satisfacer los principios de eficacia, eficiencia y seguridad que los servicios públicos demandan, en beneficio último de los ciudadanos y los intereses nacionales.

Partiendo del conocimiento y la experiencia previa en materia de amenazas y vulnerabilidades, la Ley 11/2002, reguladora del Centro Nacional de Inteligencia, encomendó al Centro Criptológico Nacional (CCN) el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y la protección de la información clasificada, a la vez que confería a su Secretario de Estado Director la responsabilidad de dirigir el CCN, incluyéndose entre tales competencias la elaboración y difusión de normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de información de las entidades del Sector Público, como así prescribe el Real Decreto 412/2204, por el que se regula el CCN.

El Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad (ENS), trayendo causa de lo dispuesto en la Ley 40/2015, de Régimen Jurídico del sector Público, vino a establecer la política de seguridad en la utilización de medios electrónicos en el ámbito público, constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada y los servicios prestados por medios electrónicos.

En paralelo, la Unión Europea ha venido desarrollando importantes medidas legislativas culminando, por la parte que ahora nos interesa, en primer lugar, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, adaptada a nuestro ordenamiento por Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, que prescribe la aplicación del ENS en los tratamientos de datos personales de su ámbito competencial.

En segundo lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, relativa la seguridad de las redes y sistemas de información en la Unión (Directiva NIS), transpuesta por Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información, señalando de nuevo al ENS como la normativa singular en materia de seguridad de los sistemas de información del Sector Público, confiere asimismo al CCN-CERT, en los supuestos de especial gravedad, la responsabilidad de la coordinación nacional de la respuesta técnica de los CSIRT (*Computer Security Incident Response Team*) concernidos por la norma.

Todas estas responsabilidades nos impulsan y animan a seguir participando, como hasta ahora, en la construcción de la Seguridad Nacional.

Abril 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El Centro Criptológico Nacional (CCN) desarrolla y publica el presente documento como respuesta al mandato recogido en el artículo 36 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, que señala: "*El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Response Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN"* y el RD 951/2015, de 23 de octubre, que modifica al RD 3/2010.
2. El **Real Decreto-ley 12/2018**, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información, quedan fijados los Equipos de respuesta a incidentes de seguridad informática de referencia en lo concerniente a las relaciones con los Operadores de Servicios Esenciales: El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre (Sector Publico, en adelante). Además, **en los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinaria**s, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.
3. Es al amparo de estas funciones, misiones y responsabilidades, que confiere al CCN la responsabilidad de elaborar y difundir las correspondientes **guías de seguridad** de las tecnologías de la información y las comunicaciones para el mejor cumplimiento de lo establecido en el ENS, por lo que se desarrolla y publica la presente **Guía CCN-STIC 817 Gestión de Ciberincidentes en el ENS.**

Nota importante:

El contenido de esta Guía se encuentra alineado con la Guía Nacional de Notificación y Gestión de Ciberincidentes, aprobada por el Consejo Nacional de Ciberseguridad.

2. OBJETO

4. El propósito de esta Guía es ayudar al Sector Público al establecimiento de las **capacidades de respuesta a ciberincidentes** y su adecuado tratamiento, eficaz y eficiente, dirigiéndose especialmente a:
    - Equipos de Respuesta a Ciberincidentes internos a las organizaciones.
    - Responsables de Seguridad de la Información (de obligada nominación para los Operadores de Servicios Esenciales, de conformidad con lo previsto en el artículo 16.3 del Real Decreto-ley 12/2018, de 7 de septiembre) y Responsables Delegados.
    - Responsables de Sistemas de Información (CIO Chief Information Officer) y, en general,
        - Gestores de programas de Ciberseguridad.
        - Administradores de Red y de Sistemas,

- Personal de Seguridad.

5. En concreto, esta Guía proporcionará a los Responsables de Seguridad de dichas entidades públicas:

   - Un acercamiento a la tipificación de los ciberincidentes.
   - Unas recomendaciones para determinar la peligrosidad de los ciberincidentes. Una metodología de notificación al CCN-CERT, atendiendo al momento y a la tipología del ciberincidente.

Nota importante:

El contenido de esta Guía se encuentra alineado con la herramienta LUCIA, desarrollada por el CCN-CERT, para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad, tal y como se detalla en el Anexo C de este documento.

Con la herramienta LUCIA, el organismo podrá gestionar diversos tipos de ciberincidentes:

- **Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).**
- **Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).**
- **Los provenientes del Sistema de Alerta Temprana para Sistemas de Control Industrial (SAT-ICS).**
- **Cualesquiera otro tipo de ciberincidentes generales.**

3. ALCANCE

6. El artículo 11 del ENS señala la obligación de que las entidades públicas de su ámbito de aplicación dispongan de una **Política de Seguridad de la Información** que articule una serie de **Requisitos Mínimos de Seguridad.** Entre tales requisitos, y por lo que compete al presente documento, se contempla la **Gestión de Incidentes de Seguridad**, exigencia que se concreta en el artículo 24 del mismo cuerpo legal, que señala que:

   - Se establecerá un sistema de detección y reacción frente a código dañino.
   - Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

7. Siguiendo la línea terminológica iniciada por la Estrategia de Ciberseguridad Nacional, a lo largo del presente documento se utilizará el término **ciberincidente** como sinónimo de **incidente de seguridad** en el ámbito de los Sistemas de Información y las Comunicaciones.

4. LA GESTIÓN DE LOS CIBERINCIDENTES

8. La gestión de ciberincidentes consta de varias fases.

9. La fase inicial contempla la creación y formación de un **Equipo de Respuesta a Ciberincidentes (ERC)**, y la utilización de las herramientas y recursos necesarios[1]. Durante esta fase de **PREPARACIÓN**, el organismo público, atendiendo a lo dispuesto en

[1] Por ejemplo, la adhesión a los servicios del Sistema de Alerta Temprana (SAT) del CCN-CERT, tanto en la red SARA (Sistemas de Aplicaciones y Redes para las Administraciones (SAT-SARA) como en internet (SAT-INET) o en los Sistemas de Control Industrial (SAT-ICS).

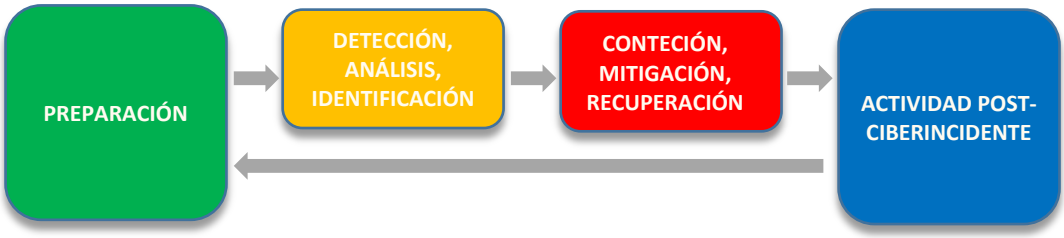
los Anexos I y II del ENS, y previo el correspondiente análisis de riesgos, habrá identificado y desplegado un determinado conjunto de medidas de seguridad.

10. La adecuada implantación de las antedichas medidas ayudará a detectar las posibles brechas de seguridad de los Sistemas de Información de la organización y su análisis, en la fase de **DETECCIÓN, ANÁLISIS E IDENTIFICACIÓN**, desencadenando los procesos de notificación a los que hubiere lugar.

11. La **DETECCIÓN** de la amenaza, una vez que ha penetrado en el organismo, puede ser realizada por el propio organismo y/o por las sondas desplegadas por el CCN-CERT, que generarán el correspondiente aviso.

12. La organización, en la fase de **CONTENCIÓN, MITIGACIÓN Y RECUPERACIÓN** del ciberincidente –y atendiendo a su peligrosidad- deberá intentar, en primera instancia, mitigar su impacto, procediendo después a su eliminación de los sistemas afectados y tratando finalmente de recuperar el sistema al modo de funcionamiento normal. Durante esta fase será necesario, cíclicamente, persistir en el análisis de la amenaza, de cuyos resultados se desprenderán, paulatinamente, nuevos mecanismos de contención y erradicación.

13. Tras el incidente, en la fase de **ACTIVIDAD POST-CIBERINCIDENTE**, los responsables del organismo emitirán un Informe del Ciberincidente que detallará su causa originaria y su coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados) y las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.



Ciclo de vida de la Respuesta a Ciberincidentes

4.1 CLASIFICACIÓN DE LOS CIBERINCIDENTES

14. Puesto que no todos los ciberincidentes poseen las mismas características ni la misma peligrosidad, es necesario disponer de una taxonomía de los ciberincidentes, lo que ayudará posteriormente a su análisis, contención y erradicación.

15. Los factores que podemos considerar a la hora de establecer criterios de clasificación son, entre otros:

- **Tipo de amenaza:** código dañino, intrusiones, fraude, etc.
- **Origen de la amenaza:** Interna o externa.
- La **categoría**[2] de seguridad de los sistemas afectados.

[2] Atendiendo a los criterios señalados en el Anexo I del ENS para categorizar los Sistemas de Información.

- El **perfil de los usuarios afectados**, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El **número y tipología de los sistemas afectados**.
- El impacto que el incidente puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
- Los **requerimientos legales y regulatorios**.

16. La combinación de uno o varios de estos factores es determinante a la hora de tomar la decisión de crear un ciberincidente o determinar su peligrosidad y prioridad de actuación.

17. La tabla siguiente muestra una **clasificación de los ciberincidentes**, (Mas detalle en Glosario en Anexo D)

CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES		
Clasificación	**Tipo de incidente**	**Descripción y ejemplos prácticos**
Contenido abusivo	**Spam**	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	**Sistema infectado**	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
Obtención de información	**Escaneo de redes (scanning)**	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	**Explotación de vulnerabilidades conocidas**	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).

	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	**Compromiso de cuenta con privilegios**	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad	**DoS (Denegación de servicio)**	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	**Acceso no autorizado a información**	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	**Uso no autorizado de recursos**	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	**Criptografía débil**	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para

		la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	**Otros**	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Tabla 1.- Clasificación de los Ciberincidentes

4.2 LA DETECCIÓN DE LOS CIBERINCIDENTES

18. No es fácil en todos los casos determinar con precisión si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad.

19. Básicamente, los indicios de que nos encontramos ante un ciberincidente pueden provenir de dos tipos de fuentes: los *precursores* y los *indicadores*. Un **precursor** es un indicio de que *puede ocurrir* un incidente en el futuro. Un **indicador** es un indicio de que un incidente *puede haber ocurrido o puede estar ocurriendo ahora*.

20. Algunos ejemplos de precursores son:

    – Las entradas de log del servidor Web, con los resultados de un escáner de vulnerabilidades.
    – El anuncio de un nuevo exploit, dirigido a una atacar una vulnerabilidad que podría estar presente en los sistemas de la organización.
    – Amenazas explícitas provenientes de grupos o entidades concretos, anunciado ataques a organizaciones objetivo[3].

21. Los indicadores son muy comunes, tales como:

    – el sensor de intrusión de una red emitiendo una alerta cuando ha habido un intento de desbordamiento de búfer contra de un servidor de base de datos;
    – las alertas generadas por software antivirus;
    – la presencia de un nombre de archivo con caracteres inusuales;
    – un registro de log sobre un cambio no previsto en la configuración de un host;
    – los logs de una aplicación, advirtiendo de reiterados intentos fallidos de login desde un sistema externo desconocido;
    – la detección de un número importante de correos electrónicos rebotados con contenido sospechoso;
    – desviación inusual del tráfico de la red interna,

[3] Es el caso del anuncio de ataques por grupos hacktivistas, por ejemplo.

22. La gestión y coordinación de incidentes desarrollada por el CCN-CERT para los organismos del sector público español, a través del Sistema de **Alerta Temprana de Red SARA (SAT-SARA)**[4], del **Sistema de Alerta Temprana de Internet (SAT-INET)**[5] y del **Sistema de Alerta Temprana para Sistemas de Control Industrial (SAT-ICS)**[6] da adecuada respuesta a todas estas necesidades.

4.3 LA PELIGROSIDAD DE LOS CIBERINCIDENTES

23. Además de tipificar los ciberincidentes dentro de un determinado grupo o tipo, la gestión de los mismos (asignación de prioridades y recursos, etc.) exige determinar la peligrosidad[7] potencial que el ciberincidente posee. Para ello, es necesario fijar ciertos **Criterios de Determinación de la Peligrosidad** con los que comparar las evidencias que se disponen del ciberincidente, en sus estadios iniciales.

24. A efectos de la presente Guía, la peligrosidad de un ciberincidente dado se asignará a uno de una escala de cinco valores. Esta escala, de menor a mayor peligrosidad, es la mostrada seguidamente.

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	MUY ALTO
5	CRÍTICO

Tabla 2 - Niveles de Peligrosidad

El cuadro siguiente muestra el **Nivel de Peligrosidad de los Ciberincidentes**, atendiendo a la repercusión que la materialización de la amenaza de que se trate podría tener en los sistemas de información de las entidades del ámbito de aplicación del ENS

Este Nivel de Peligrosidad será el utilizado por el CCN-CERT en sus comunicaciones a las entidades afectadas, adheridas a los Sistemas de Alerta Temprana de Red SARA (SAT-SARA), de Internet (SAT-INET) o de los Sistemas de Control Industrial (SAT-ICS).

[4] Servicio desarrollado por el CCN-CERT en colaboración con el Ministerio de Hacienda y Administraciones Públicas (Organismo responsable de la red SARA. Sistema de Aplicaciones y Redes para las Administraciones). Su objetivo es la detección en tiempo real de ataques y amenazas, llevando a cabo a través del análisis del tráfico de red que circula entre las redes de los Organismos de las Administraciones Públicas conectados a la red SARA.

[5] Servicio desarrollado e implantado por el CCN-CERT para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito e Internet.

[6] Servicio desarrollado e implantado por el CCN-CERT para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico de las redes de control industrial del Organismo adscrito.

[7] *Peligrosidad*: Cualidad de peligroso. (DRAE, edición 22ª). En otros textos puede denominarse como criticidad.

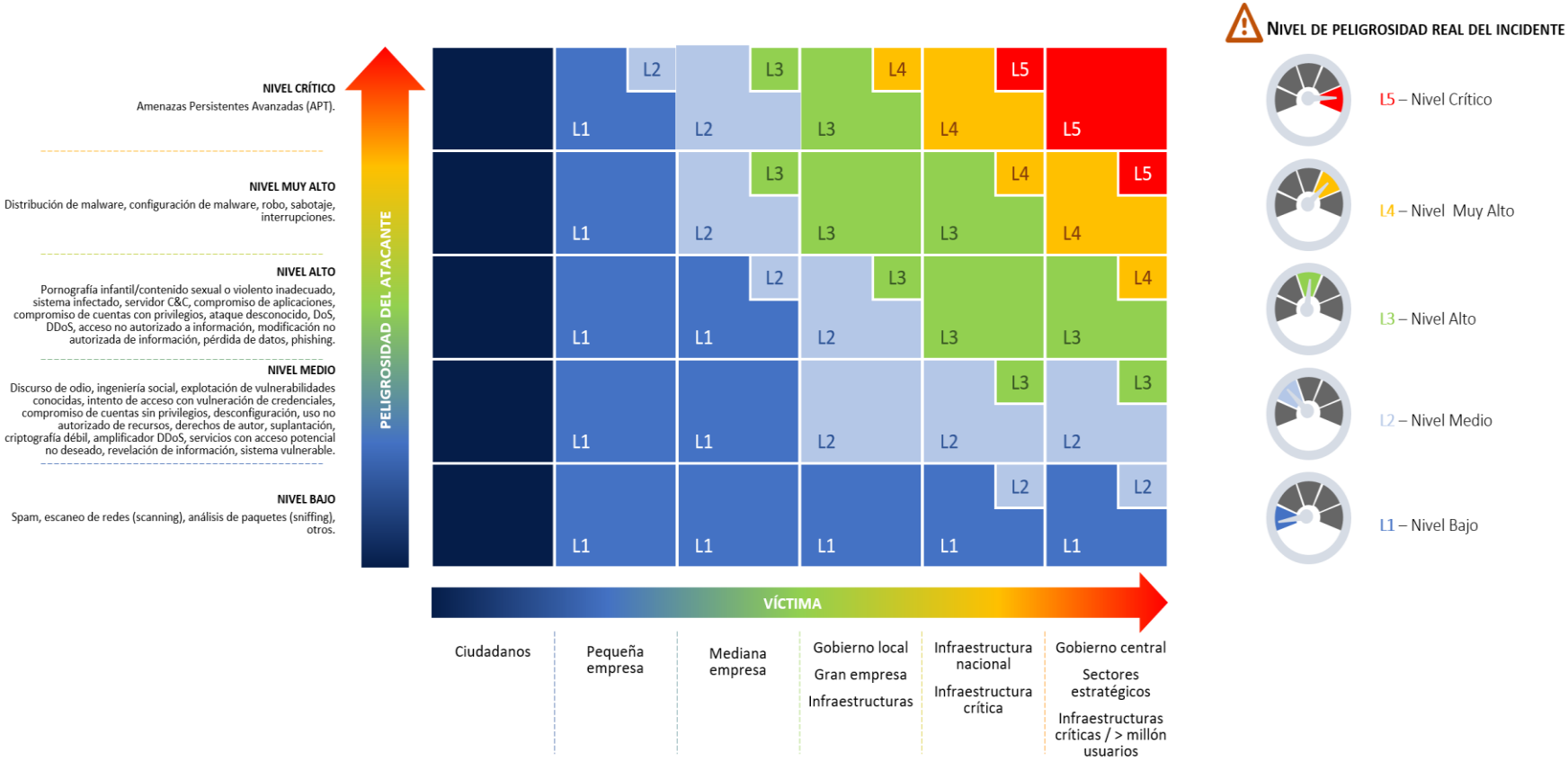


Tabla 3 - Niveles de Peligrosidad

4.4 NIVEL DE IMPACTO DEL CIBERINCIDENTE EN LA ORGANIZACIÓN

25. El ENS señala que el impacto de un ciberincidente en un organismo público se determina evaluando las consecuencias que tal ciberincidente ha tenido en las funciones de la organización, en sus activos o en los individuos afectados.

26. El cuadro siguiente muestra cómo debe determinar el organismo afectado **el Nivel de Impacto Potencial**[8] de los Ciberincidentes en la organización.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
CRÍTICO	Afecta apreciablemente a la Seguridad Nacional.
	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a una Infraestructura Crítica.
	Afecta a sistemas clasificados SECRETO.
	Afecta a más del 90% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios.
	El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
	Impacto económico superior al 0,1% del P.I.B. actual.
	Extensión geográfica supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
MUY ALTO	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
	Afecta a un servicio esencial.
	Afecta a sistemas clasificados RESERVADO.
	Afecta a más del 75% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios.
	El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
	Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.

[8] Se define **impacto potencial** como una estimación del daño que podría causar un incidente de seguridad.

	Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
	Daños reputacionales a la imagen del país (marca España).
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
ALTO	Afecta a más del 50% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona.
	Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual.
	Extensión geográfica superior a 3 CC.AA.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
MEDIO	Afecta a más del 20% de los sistemas de la organización.
	Interrupción en la presentación del servicio superior al 5% de usuarios.
	El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
	Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual.
	Extensión geográfica superior a 2 CC.AA.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
BAJO	Afecta a los sistemas de la organización.
	Interrupción de la prestación de un servicio.
	El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona.
	Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual.
	Extensión geográfica superior a 1 CC.AA.
	Daños reputacionales puntuales, sin eco mediático

Tabla 4 – Criterios de determinación del Nivel de Impacto

4.5 SEGUIMIENTO POR PARTE DEL CCN-CERT

27. La herramienta LUCIA, a disposición de los organismos del ámbito de aplicación del ENS, y tal y como se detalla en el Anexo C de esta Guía, utiliza un sistema de seguimiento de tickets que puede usarse para documentar el desarrollo del ciberincidente y las acciones que se han llevado a cabo en cada momento, correspondientes a las fases de detección, contención, erradicación y recuperación.

28. Una vez notificado el incidente al organismo afectado por parte del Sistema de Alerta Temprana de Red SARA (SAT-SARA), de Internet (SAT-INET) o para los Sistemas de Control Industrial (SAT-ICS) del CCN-CERT, se realizará un seguimiento del mismo, asignándole un determinado Estado.

29. La tabla siguiente muestra los diferentes estados que puede tener un ciberincidente, en un instante dado.

Estado	Descripción
Cerrado (Resuelto y sin respuesta)	No hay respuesta por parte del organismo afectado en un periodo determinado. No obstante, el incidente parece estar resuelto.
Cerrado (Resuelto y con respuesta)	El organismo afectado ha solventado la amenaza y notifica a su CSIRT de referencia el cierre del ciberincidente.
Cerrado (Sin impacto)	La detección ha resultado positiva pero el organismo no es vulnerable o no se ve afectado por el ciberincidente.
Cerrado (Falso positivo)	La detección ha sido errónea.
Cerrado (Sin resolución y sin respuesta)	Si el ciberincidente no ha sido resuelto por el organismo afectado y este no ha comunicado con el CSIRT de referencia, es cerrado con este estado.
Cerrado (Sin resolución y con respuesta)	No se ha alcanzado una solución al problema o el afectado indica que no sabe solventarlo incluso con las indicaciones proporcionadas por el CSIRT.
Abierto	Estado que va desde que el organismo afectado notifica la amenaza al CSIRT de referencia, o bien este último lo comunica al afectado, hasta que se produce el cierre del mismo por alguna de las causas anteriormente descritas.

Tabla 5 – Estados de los ciberincidentes notificados por los Sistemas de Alerta Temprana del CCN-CERT

30. Dicho seguimiento se realizará en función del nivel de peligrosidad o impacto del ciberincidente, en base a la siguiente tabla en la que se muestra los días tras los que se cerrará un ciberincidente sin respuesta:

Nivel de peligrosidad o impacto	Obligación de notificar al CCN-CERT	Cierre del ciberincidente (días naturales)	Precisiones
CRÍTICO	Sí	120	- Se cierran automáticamente por los Sistemas de Alerta Temprana trascurrido el número de días especificado en la columna anterior desde la última actualización del incidente en LUCIA. - El Sistema de Alerta Temprana envía recordatorios del aviso al organismo.
MUY ALTO	Sí	90	
ALTO	Sí	45	
MEDIO	No	30	
BAJO	No	21	

Anualmente, la organización remitirá al CCN-CERT un resumen con los datos esenciales de <u>todos</u> los ciberincidentes ocurridos en el periodo considerado. El Anexo B de esta Guía contiene un listado de aquellas informaciones más relevantes que deben incluirse en tal Informe Anual.

4.6 MÉTRICAS E INDICADORES

31. El Anexo A de esta Guía contiene un conjunto de Métricas e Indicadores que los organismos del ámbito de aplicación del ENS pueden usar para evaluar la **implantación, eficacia y eficiencia** del proceso de Gestión de Ciberincidentes.

4.7 RECOLECCIÓN Y CUSTODIA DE EVIDENCIAS

32. Aunque el motivo principal para la recolección de las evidencias de un ciberincidente es ayudar a su resolución, también puede ser necesaria para iniciar procesos de naturaleza legal. En tales casos, es importante documentar claramente cómo se han obtenido y custodiado las evidencias, y siempre conforme a lo dispuesto en la legislación vigente[9].

33. Debe mantenerse un registro detallado de todas las evidencias, incluyendo:

- La identificación de la información (por ejemplo, la localización, el número de serie, número de modelo, el nombre de host, dirección MAC y direcciones IP de los ordenadores afectados.
- Nombre, cargo y el teléfono de cada persona que ha recogido o gestionado evidencias durante la investigación del ciberincidente.
- Fecha y hora de cada ocasión en la que ha sido tratada cada evidencia.
- Ubicaciones donde se custodiaron las evidencias.

34. No obstante, acopiar datos de evidencias no es una tarea sencilla. En general, siempre es conveniente empezar el acopio de evidencias tan pronto como se detecta un ciberincidente. Por otro lado, desde un punto de vista probatorio, es conveniente obtener inmediatamente una instantánea del sistema atacado, dejándolo inaccesible y garantizando su integridad[10], antes de tratar las copias hechas del sistema atacado con diferentes tipos de herramientas que, de otro modo, podrían alterar parte de la información o el estado de los sistemas comprometidos[11].

35. Los organismos del ámbito de aplicación del ENS deberán redactar y aprobar normas sobre la custodia de las evidencias de un ciberincidente. Se muestran seguidamente algunos de los factores más significativos a la hora de determinar aquella normativa:

- Persecución del delito: Si, como consecuencia del ciberincidente, pudiera procesarse al atacante, será necesario custodiar adecuadamente las pruebas del delito hasta que se hayan completado todas las acciones legales.
- Retención de datos: Todos los organismos deben poseer políticas de retención de datos que señalen durante cuánto tiempo pueden conservarse ciertos tipos de datos, respetando en todo caso lo dispuesto en la legislación vigente para cada tipo de información.

[9] Sobre este particular, el ERC hará bien en discutir el asunto de la obtención y custodia de pruebas con la Asesoría Jurídica del organismo, con el CCN-CERT o con terceras partes especializadas, incluyendo, si ello es necesario, Fuerzas y Cuerpos de Seguridad y Fiscalía para la Criminalidad Informática.
[10] Y trabajar, a partir de entonces, con copias del sistema.
[11] Para obtener información adicional sobre la preservación de evidencias, puede consultarse la Guía NIST SP 800-86, Guía para la Integración de Técnicas Forenses en Respuesta a Incidentes, para obtener información adicional sobre la preservación de evidencias.

– Coste de la custodia: Custodiar los elementos físicos que pueden contener evidencias (por ejemplo, discos duros, sistemas comprometidos, etc.) comporta un coste que conviene tener en cuenta.

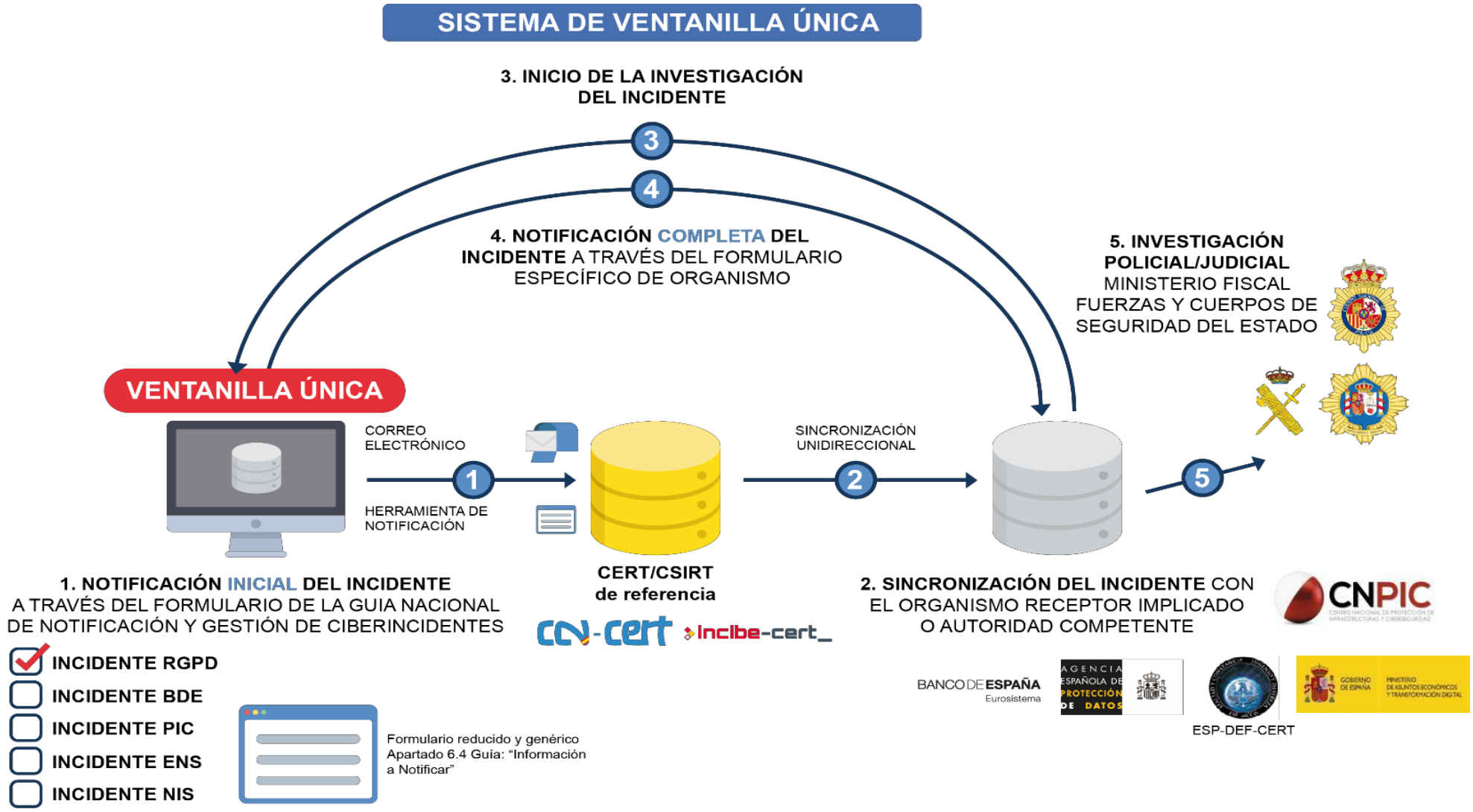
4.8 INTERCAMBIO DE INFORMACIÓN Y COMUNICACIÓN DE CIBERINCIDENTES

36. Además de la preceptiva notificación de los ciberincidentes al CCN-CERT, en ocasiones los organismos públicos necesitarán comunicarse con terceros (Fuerzas y Cuerpos de Seguridad y medios de comunicación social, específicamente). El resto de las comunicaciones con otros actores (ISPs, CSIRTs, CNPIC, otras autoridades competentes, etc.) se desarrollarán a través del CCN-CERT, según la *Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes*.

37. La coordinación y el intercambio de información con los organismos adecuados puede fortalecer la capacidad de la organización para responder con eficacia a los ciberincidentes. Por ejemplo, si un organismo identifica algún comportamiento sospechoso en su red y remite información sobre el evento al CCN-CERT, es muy probable que se hayan tenido referencias de comportamientos similares en otras organizaciones y se sea capaz de responder adecuadamente a la actividad sospechosa.

38. Otro incentivo para el intercambio de información es el hecho de que la capacidad de responder a ciertos ciberincidentes podría requerir el uso de herramientas que pueden no estar disponibles para un solo organismo, sobre todo si se trata de un organismo pequeño o mediano. En estos casos, el organismo en cuestión puede aprovechar su red de intercambio de información de confianza para externalizar de manera eficaz el análisis del ciberincidente a los recursos de terceros que sí tienen las capacidades técnicas adecuadas para gestionar adecuadamente el ciberincidente.

39. En este sentido, y de acuerdo con la Guía Nacional de Notificación y Gestión de Ciberincidentes, se define el sistema de ventanilla única mediante el cual la comunicación del ciberincidente por parte de la víctima se realizará siempre a través del CERT de referencia, según el cuadro adjunto:


SISTEMA DE VENTANILLA ÚNICA
3. INICIO DE LA INVESTIGACIÓN DEL INCIDENTE
4. NOTIFICACIÓN COMPLETA DEL INCIDENTE A TRAVÉS DEL FORMULARIO ESPECÍFICO DE ORGANISMO
5. INVESTIGACIÓN POLICIAL/JUDICIAL
MINISTERIO FISCAL
FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO
VENTANILLA ÚNICA
CORREO ELECTRÓNICO
HERRAMIENTA DE NOTIFICACIÓN
SINCRONIZACIÓN UNIDIRECCIONAL
CERT/CSIRT de referencia
1. NOTIFICACIÓN INICIAL DEL INCIDENTE
A TRAVÉS DEL FORMULARIO DE LA GUIA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES
INCIDENTE RGPD
INCIDENTE BDE
INCIDENTE PIC
INCIDENTE ENS
INCIDENTE NIS
Formulario reducido y genérico
Apartado 6.4 Guía: "Información a Notificar"
2. SINCRONIZACIÓN DEL INCIDENTE CON EL ORGANISMO RECEPTOR IMPLICADO O AUTORIDAD COMPETENTE
CNPIC
BANCO DE ESPAÑA
Eurosistema
ESP-DEF-CERT

5. ANEXO A. MÉTRICAS E INDICADORES

7.1MÉTRICAS DE IMPLANTACIÓN

M1	**Indicador**	Alcance del sistema de gestión de ciberincidentes	
	Objetivo	Saber si todos los sistemas de información están adscritos al servicio	
	Método	Se cuentan cuántos servicios están bajo control. (Si se conociera cuántos servicios hay en total, se podría calcular un porcentaje). • #servicios de categoría ALTA (ENS Anexo I) • #servicios de categoría MEDIA (ENS Anexo I)	
	Caracterización	Objetivo	100%
		Umbral amarillo	ALTA: 4/5 (80%) MEDIA: 2/3 (67%)
		Umbral rojo	ALTA: 2/3 (67%) MEDIA: ½ (50%)
		Frecuencia medición	trimestral
		Frecuencia reporte	anual

5.2MÉTRICAS DE RESOLUCIÓN DE INCIDENTES

M2	**Indicador**	Resolución de ciberincidentes de nivel de impacto ALTO (ENS Anexo I – afectando a sistemas de categoría ALTA)	
	Objetivo	Ser capaces de resolver prontamente incidentes de alto impacto	
	Método	Se mide el tiempo que se tarda en resolver un incidente con un impacto en sistemas de categoría ALTA: desde que se notifica hasta que se resuelve • T(50) tiempo que se tarda en cerrar el 50% de los incidentes • T(90) tiempo que se tarda en cerrar el 90% de los incidentes	
	Caracterización	Objetivo	T(50) = 0 && T(90) = 0
		Umbral amarillo	T(50) > 5d || T(90) > 10d
		Umbral rojo	T(50) > 10d || T(90) > 20d
		Frecuencia medición	anual
		Frecuencia reporte	anual

M3	**Indicador**	Resolución de ciberincidentes de nivel de impacto MEDIO (ENS Anexo I – afectando a sistemas de categoría MEDIA)	
	Objetivo	Ser capaces de resolver prontamente incidentes de impacto medio	
	Método	Se mide el tiempo que se tarda en resolver un incidente con un impacto en sistemas de categoría MEDIA: desde que se notifica hasta que se resuelve: • T(50) tiempo que se tarda en cerrar el 50% de los incidentes • T(90) tiempo que se tarda en cerrar el 90% de los incidentes	
	Caracterización	Objetivo	T(50) = 0 && T(90) = 0
		Umbral amarillo	T(50) > 10d || T(90) > 30d
		Umbral rojo	T(50) > 15d || T(90) > 45d
		Frecuencia medición	anual
		Frecuencia reporte	anual

5.3 MÉTRICAS DE RECURSOS

M4	**Indicador**	Recursos consumidos	
	Objetivo	Conocer si es necesario aumentar la fuerza de trabajo	
	Método	Estimación del número de horas-hombre dedicadas a resolver incidentes de seguridad fórmula: #horas dedicadas a incidentes / #horas formalmente contratadas para seguridad TIC	
	Caracterización	Objetivo	< 20%
		Umbral amarillo	20%
		Umbral rojo	50%
		Frecuencia medición	trimestral
		Frecuencia reporte	anual

5.4 MÉTRICAS DE GESTIÓN DE INCIDENTES

M5	**Indicador**	Estado de cierre los incidentes	
	Objetivo	Ser capaces de gestionar incidentes de seguridad	
	Método	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin	
	Caracterización	Objeto	<10%
		Umbral amarillo	20%
		Umbral rojo	50%
		Frecuencia mediación	Trimestral
		Frecuencia reporte	Anual

M6	**Indicador**	Estado de cierre los incidentes de peligrosidad MUY ALTA/ CRÍTICA	
	Objetivo	Ser capaces de gestionar incidentes de seguridad de alta peligrosidad	
	Método	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin respuesta / # total de incidentes notificados	
	Caracterización	Objeto	0%
		Umbral amarillo	5%
		Umbral rojo	20%
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

6. ANEXO B. ELEMENTOS PARA EL INFORME DE CIERRE DEL CIBERINCIDENTE[12]

- **Nivel de Peligrosidad (final) del ciberincidente.**
- **Resumen de las acciones realizadas para:**
  - Contención del ciberincidente.
  - Erradicación del ciberincidente.
  - Recuperación de los sistemas afectados.
- **Impacto del ciberincidente, medido en:**
  - Tipología de la información o sistemas afectados.
  - Grado de afectación a las instalaciones de la organización.
  - Posible interrupción en la prestación del servicio normal de la organización.
  - Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
  - Pérdidas económicas.
  - Extensión geográfica afectada.
  - Daños reputacionales asociados.

[12] Para ciberincidentes con un nivel de peligrosidad ALTO, MUY ALTO ó CRÍTICO.

7. ANEXO C. INTRODUCCIÓN A LA HERRAMIENTA LUCIA

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta de **gestión de tickets** que permite al organismo del ámbito de aplicación del ENS gestionar cada uno de sus ciberincidentes, al tiempo que posibilita la integración de todas las instancias de la herramienta instaladas en los diferentes organismos con la instancia instalada en el CCN-CERT, posibilitando de este modo la consolidación y sincronización de los ciberincidentes registrados por cada organismo en el Nodo de Coordinación del CCN-CERT.

7.1 OBJETIVOS

La plataforma LUCIA persigue los siguientes objetivos:

- Dotar a los organismos del ámbito de aplicación del ENS de una plataforma única y distribuida de tratamiento de ciberincidentes, para la gestión independizada de incidentes de seguridad en todos los organismos adscritos.
- Ser conforme con los requisitos del Esquema Nacional de Seguridad (ENS).
- Federar los sistemas LUCIA desplegados.
- Reportar al CCN-CERT la información de contexto (metadatos) de los ciberincidentes identificados en los organismos.
- Comunicar y sincronizar ciberincidentes entre el CCN-CERT y su comunidad de organismos, mejorando los procedimientos con aquellos adscritos a los Sistemas de Alerta Temprana de Internet (SAT-INET), Sistemas de Control Industrial (SAT-ICS) y Red SARA (SAT-SARA).

7.2 CARACTERÍSTICAS

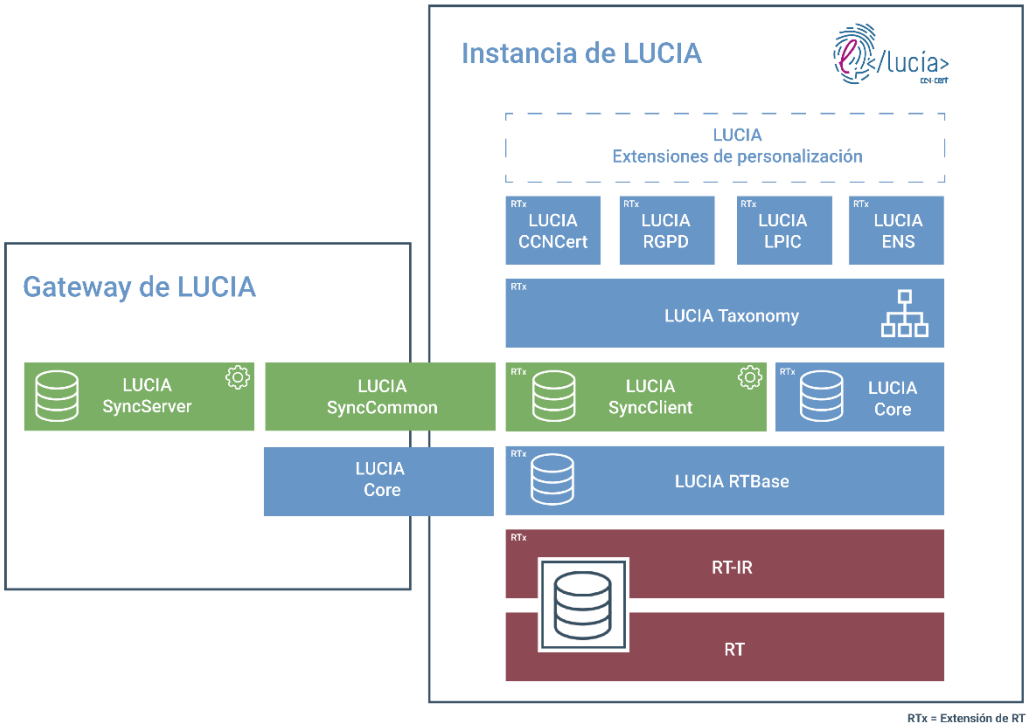
LUCIA se basa en la implementación del sistema abierto para la Gestión de Incidencias Request Tracker (RT), en el que se incluye la extensión para equipos de respuesta a incidentes Request Tracker for Incident Response (RT-IR).

Entre sus características principales destacan las siguientes:

- Modelo personalizado, al objeto de cumplir los requerimientos y procedimientos del CCN-CERT y las exigencias derivadas de la conformidad con el ENS.
- Información sincronizada y compartida entre los diferentes organismos adscritos.

- Basada en la utilización de servicios REST, lo que permite una mayor flexibilidad y mejora de la integración y rendimiento en RT.
- Comunicación segura, basada en un modelo transaccional, de cara a garantizar la correcta recepción y evitando la pérdida de incidentes notificados.
- Plataforma única disponible para todos los organismos adscritos:
    - Distribución de una máquina virtual, previamente paquetizada.
    - Adaptable a la arquitectura de almacenamiento de cada organismo.
- Trazabilidad de incidentes entre organismos y el CCN-CERT.
- Clasificación de incidentes unificada, proporcionando un "lenguaje común" de gestión y tratamiento.
- Registro de tiempos de respuesta entre diferentes estados del incidente.

7.3 ARQUITECTURA

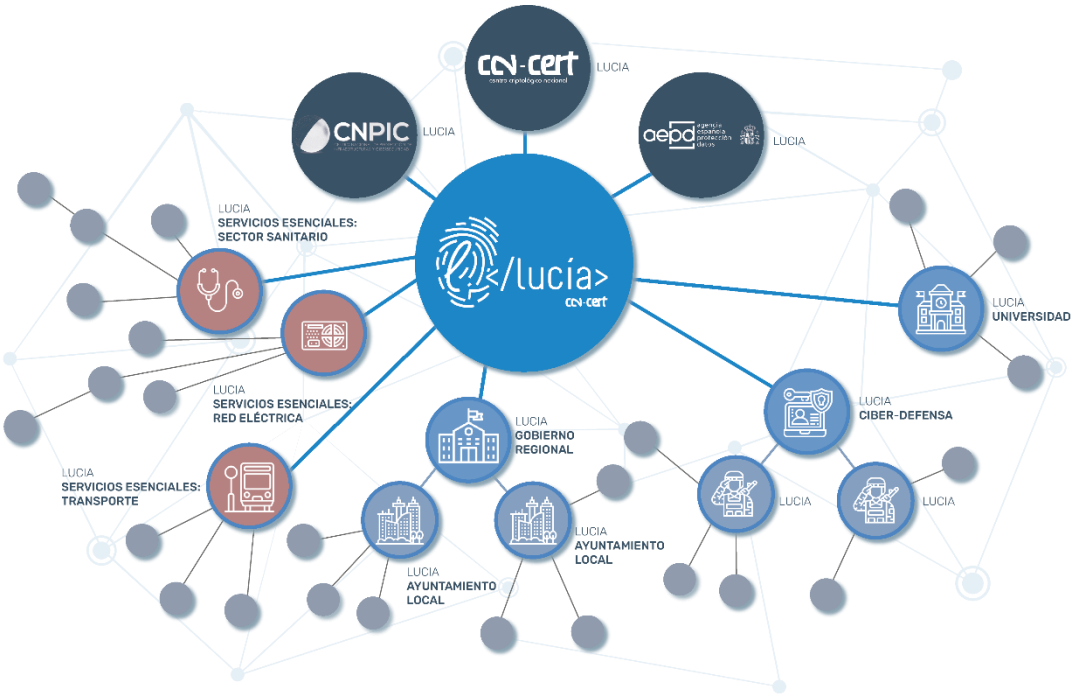


En el gráfico a continuación se pueden ver los componentes internos que conforman LUCIA:

Esta arquitectura modular permite personalizar las instancias de una forma mucho más flexible, especialmente con componentes de personalización que se apoyan sobre los componentes principales de LUCIA.

Cabe destacar el componente principal LUCIA ENS, para adecuar la instancia a los requisitos específicos del Esquema Nacional de Seguridad (ENS).

El siguiente gráfico muestra el diagrama conceptual del despliegue y comunicaciones del



sistema LUCIA:

La sincronización entre las diferentes instancias de LUCIA desplegadas y el sistema central del CCN-CERT se realiza de la siguiente forma:

- Sincronización Unidireccional: La política de Sincronización Unidireccional permite que cualquier organismo adherido realice las llamadas de creación, creación extendida, modificación, actualización de información, añadido de comentarios y cambio de estado de los tickets que reporta al servidor central de LUCIA.

  Esta política permitirá que cualquier incidente recogido localmente en una instancia de LUCIA se replique de forma automática en el servidor central, garantizando que sólo se comparte la información de contexto del incidente, sin datos adicionales.

- Sincronización Bidireccional: La política de Sincronización Bidireccional permitirá dotar al sistema de la funcionalidad implementada en la política de Sincronización Unidireccional desde el propio servidor central de LUCIA hacia instancias de LUCIA desplegadas en ciertos organismos en los que el CCN-CERT dispone de sondas. Es la política por defecto utilizada en los incidentes notificados por los Sistemas de Alerta Temprana (SAT).

  Este mecanismo opera en ambos sentidos, posibilitando la sincronización de los incidentes creados en el sistema central con aquellos otros creados desde los organismos adscritos.

7.4 NOTIFICACIÓN A TERCEROS

LUCIA implementa además un mecanismo de notificación a determinados organismos, como al propio CCN-CERT de aquellos ciberincidentes de los que se requiere una intervención más profunda.

Este mecanismo, conocido como “notificación a terceros”, se inicia para tickets individuales a través de una edición en la que se indica que el incidente debe ser notificado a dicho organismo.

Esto permite que un organismo pueda notificar a otro por diversas razones (e.g., solicitar soporte adicional para tratar el incidente, requisitos normativos, etc.)

8. ANEXO D. GLOSARIO

Término	Definición
Ataque por fuerza bruta o ataque exhaustivo	STIC 401 GLOSARIO 2.97.1 ATAQUE EXHAUSTIVO 1. Caso particular de ataque sólo al texto cifrado en el que el criptoanalista, conociendo el algoritmo de cifra, intenta su descifrado probando con cada clave del espacio de claves. Si el cardinal de este último es un número muy grande, el tiempo invertido en recorrer el citado espacio es fabuloso, y las probabilidades de éxito escasísimas. [Ribagorda:1997] 2.97.2 (EN) BRUTE FORCE (I) A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries a large number of possible solutions to the problem. (See: impossible, strength, work factor.) [RFC4949:2007]
APT (*Advanced Persistent Threat*) **Amenaza Avanzada Persistente**	STIC 401 GLOSARIO 2.47.1 AMENAZAS AVANZADAS PERSISTENTES (APT) Un ataque selectivo de ciberespionaje o cibersabotaje, llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. McAfee. Predicciones de amenazas para 2011.
Ciberincidente	Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta. STIC 401 GLOSARIO 2.210.1 CIBERINCIDENTE Incidente relacionado con la seguridad de las Tecnologías de la Información y las Comunicaciones que se produce en el Ciberespacio. Este término engloba aspectos como los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc. [ISDEFE-6:2009]
CCN-CERT	Centro Criptológico Nacional-Computer Emergency Response Team STIC 401 GLOSARIO 2.185.1 CERT - EQUIPO DE REACCIÓN RÁPIDA ANTE INCIDENTES INFORMÁTICOS Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.
CIO	Chief Information Officer
CISO	Chief Information Security Officer STIC 401 GLOSARIO 2.850.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN Persona encargada de velar por la seguridad de la información de la

	organización. Su labor consiste en estar al día de la evolución tecnológica en la medida en que afecta a la seguridad de la información, estableciendo puentes entre el responsable de seguridad corporativa y los responsables de tecnología. No suele incluir entre sus responsabilidades la seguridad física, ni la gestión de riesgos, ni la continuidad de las operaciones.
Cross Site Scripting (XSS). Secuencia de comandos en sitios cruzados	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada. Suele utilizarse junto con CSRF (Cross-Site Request Forguery falsificación de petición en sitios cruzados) o inyección SQL (Structured Query Language). STIC 401 GLOSARIO 2.353.2 XSS Secuencias de comandos en sitios cruzados (Cross-site Scripting) es una brecha de seguridad que se produce en páginas Web generadas dinámicamente. En un ataque por XSS, una aplicación Web se envía con un script que se activa cuando lo lee el navegador de un usuario o una aplicación vulnerable. Dado que los sitios dinámicos dependen de la interacción del usuario, es posible ingresar un script malicioso en la página, ocultándolo entre solicitudes legítimas. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios en línea en general. Una vez iniciado el XSS, el atacante puede cambiar configuraciones de usuarios, secuestrar cuentas, envenenar cookies, exponer conexiones SSL, acceder sitios restringidos y hasta instalar publicidad en el sitio víctima. http://www.inteco.es/glossary/Formacion/Glosario/ 2.353.3 XSS (CROSS-SITE SCRIPTING) Es una brecha de seguridad que se produce en páginas Web generadas dinámicamente. En un ataque por XSS, una aplicación Web se envía con un "script" que se activa cuando lo lee el navegador de un usuario o una aplicación vulnerable. Dado que los sitios dinámicos dependen de la interacción del usuario, es posible ingresar un "script" malicioso en la página, ocultándolo entre solicitudes legítimas. Los puntos de entrada comunes incluyen buscadores, foros, "blogs" y todo tipo de formularios "online" en general. Una vez iniciado el XSS, el atacante puede cambiar configuraciones de usuarios, secuestrar cuentas, envenenar "cookies", exponer conexiones SSL, acceder sitios restringidos y hasta instalar publicidad en el sitio víctima. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S 2.353.4 VULNERABILIDAD CROSS-SITE-SCRIPTING Esta falla permite a un atacante introducir en el campo de un formulario o código embebido en una página, un "script" (perl, php, javascript, asp) que tanto al almacenarse como al mostrarse en el navegador, puede provocar la ejecución de un código no deseado. http://www.vsantivirus.com/vul-webcamxp.htm
CSIRT	Computer Security Incident Response Team equipo similar a un CERT.
CSRF /XSRF Falsificación de petición entre sitios cruzados	STIC 401 GLOSARIO 2.358 CROSS-SITE REQUEST FORGERY Acrónimos: CSRF, XSRF 2.358.2 CROSS SITE REQUEST FORGERY El CSRF (del inglés Cross-site request forgery o falsificación de petición en sitios cruzados) es un tipo de exploit malicioso de un sitio web en el

	que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, cabalgamiento de sesión, y ataque automático. http://es.wikipedia.org/wiki/Cross_Site_Request_Forgery 2.358.1 FALSIFICACIÓN DE SOLICITUDES ENTRE DISTINTOS SITIOS (CSRF) Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que permiten que se ejecuten acciones no deseadas mediante una sesión que ha sido autenticada. Suele utilizarse junto con XSS o inyección SQL. http://es.pcisecuritystandards.org
Defacement o Deface **Desfiguración o desfigurar**	STIC 401 GLOSARIO 2.377 DEFACEMENT 2.377.1 DESFIGURAR. Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia. El cambio de imagen puede ser a beneficio del atacante, o por mera propaganda (a beneficio del atacante o para causar una situación embarazosa al propietario de las páginas). CCN-CERT IA_09-15 Informe de Amenazas. Deface o Defacement (desfigurar o desfiguración) deformación o cambio producido de manera intencionada en una página web legítima a través de algún tipo de acceso de código malicioso.
DoS / DDoS **(*Denial of Service / Distributed Denial of Service*)** **Denegación [Distribuida] del Servicio**	STIC 401 GLOSARIO 2.381.1 DENEGACIÓN DE SERVICIO. Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso. Un método más sofisticado es el Ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños. Esto puede ser así mediante el uso de programas malware que permitan la toma de control del equipo de forma remota, como puede ser en los casos de ciertos tipos de gusano o bien porque el atacante se ha encargado de entrar directamente en el equipo de la víctima. http://www.inteco.es/glossary/Formacion/Glosario/ 2.382.1 DENEGACIÓN DE SERVICIO DISTRIBUIDA. Ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultáneamente. 2.382.2 DENEGACIÓN DE SERVICIO DISTRIBUIDA Ataque DoS en el que participan gran cantidad de máquinas atacantes. [CCN-STIC-612:2006]
Evento	STIC 401 GLOSARIO 2.476.3 EVENTO (Operación del Servicio) Un cambio de estado significativo para la cuestión de un Elemento de Configuración o un Servicio de TI. El término Evento también se usa como Alerta o notificación creada por un Servicio de TI, Elemento de Configuración o herramienta de Monitorización. Los Eventos requieren normalmente que el personal de

	Operaciones de TI tome acciones, y a menudo conllevan el registro de Incidentes.[ITIL:2007]
Evento de seguridad	STIC 401 GLOSARIO 2.476.2 SUCESO DE SEGURIDAD DE LA INFORMACIÓN Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.[UNE-ISO/IEC 27000:2014]
Gusano	STIC 401 GLOSARIO 2.553.1 GUSANO Programa que está diseñado para copiarse y propagarse por sí mismo mediante mecanismos de red. No realizan infecciones a otros programas o ficheros. [CCN-STIC-430:2006] 2.553.3 GUSANO Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S
IDS/IPS	Intrusion Detection System/Intrusion Prevention System Sistema de Detección de Intrusiones / Sistema de Prevención de Intrusiones
Incidente	Una ocurrencia que, real o potencialmente, pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información; o la información que el sistema procesa, almacena o transmite; o que constituye una violación o amenaza inminente de violación de las políticas, normas o procedimientos de seguridad de la organización. STIC 401 GLOSARIO 2.574.2 INCIDENTE (Operación del Servicio) Interrupción no planificada de un Servicio de TI o reducción en la Cali-dad de un Servicio de TI. También lo es el Fallo de un Elemento de Configuración que no ha impactado todavía en el Servicio. Por ejemplo el Fallo de uno de los discos de un "mirror". [ITIL:2007] 2.574.3 INCIDENTE Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL). [COBIT:2006] 2.574.4 INCIDENCIA Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos. Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
Incidente de seguridad	*Véase Ciberincidente*
Ingeniería social	2.601 INGENIERÍA SOCIAL (PICARESCA) 2.601.2 INGENIERÍA SOCIAL Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es

	inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S 2.601.4 INGENIERÍA SOCIAL Eufemismo empleado para referirse a medios no técnicos o de baja complejidad tecnológica utilizados para atacar a sistemas de información, tales como mentiras, suplantaciones, engaños, sobornos y chantajes. [CCN-STIC-403:2006]
Inyección de ficheros remota	STIC 401 GLOSARIO 2.622.1 ERRORES DE INYECCIÓN Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web. En esta clase de vulnerabilidades se incluye la inyección SQL, la inyección LDAP (Ligthweight Directory Access Protocol) y la inyección XPath. http://es.pcisecuritystandards.org
Inyección SQL	STIC 401 GLOSARIO 2.623.1 INYECCIÓN SQL Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos. http://es.pcisecuritystandards.org
JP Jornada- persona	Estimación del esfuerzo necesario para realizar una tarea cuya unidad equivale a una jornada de trabajo ininterrumpido de un trabajador medio.
Pharming (“farm” granja)	Deriva del término en inglés "farm" (granja) STIC 401 GLOSARIO 2.747.1 PHARMING Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP (Internet Protocol) donde se aloja una web(página) falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad. http://www.inteco.es/glossary/Formacion/Glosario/
Phising (similar a “fishing” pescando). Spear phishing ("lanza")	STIC 401 GLOSARIO Ver: • http://en.wikipedia.org/wiki/Phishing 2.761.1 PHISHING. Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio. 2.761.2 PHISHING. Phishing es la denominación que recibe la 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. El estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador. http://www.inteco.es/glossary/Formacion/Glosario 2.761.3 PHISHING. Los ataques de "phishing" usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura ("spam") para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S 2.983.1 SPEAR PHISHING. Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima) CCN-CERT IA_09-15 Informe de Amenazas. Suplantación de identidad. Consiste en el envío de correos electrónicos que aparentan ser fiables y que suelen derivar a páginas web falsas recabando datos confidenciales de las víctimas. Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
Plan de Respuesta a Ciberincidentes	Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un ciberincidente.
Ransomware. ("Secuestro" informático).	STIC 401 GLOSARIO 2.821.1 RANSOMWARE. El ransomware es un código malicioso para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado. El ransomware se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos. Un programa de malware ransomware también puede ser llamado criptovirus, criptotroyano o criptogusano. Consiste en el secuestro del ordenador (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate. CCN-CERT IA_09-15 Informe de Amenazas. Consiste en el secuestro del ordenador (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.
RAT	Pieza de software que permite a un "operador" controlar a distancia un

(Remote Acces Tool) Herramienta para Acceso Remoto	sistema como si se tuviera acceso físico al mismo. Aunque tiene usos perfectamente legales, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.
Rootkit	STIC 401 GLOSARIO 2.870.1 ROOTKIT Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos. http://www.alerta-antivirus.es /seguridad/ ver_pag.html?tema=S 2.870.2 ROOTKIT Tipo de software malicioso que, al instalarse sin autorización, es capaz de pasar desapercibido y tomar el control administrativo de un sistema informático. http://es.pcisecuritystandards.org
Scanner (Scanning) Escáner de vulnerabilidades / Análisis de seguridad de la red	STIC 401 GLOSARIO 2.461.1 ESCÁNER DE VULNERABILIDADES Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no. 2.461.2 ANÁLISIS DE SEGURIDAD DE LA RED Proceso mediante el cual se buscan vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas. http://es.pcisecuritystandards.org
Sniffer/*Sniffing* ("husmeador", monitor de red)	2.977.1 MONITOR DE RED Programas que monitorizan la información que circula por la red con el objeto de capturar información. Las placas de red tienen un sistema de verificación de direcciones mediante el cual saben si la información que pasa por ella está dirigida o no a su sistema. Si no es así, la rechaza. Un Sniffer consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer). Existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo contraseñas de acceso a cuentas, aprovechándose de que generalmente no son cifradas por el usuario. También son utilizados para capturar números de tarjetas de crédito o direcciones de correo. El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). Los buenos Sniffers no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S Programa de captura de paquetes de red. Literalmente, "husmeador".

	[CCN-STIC-435:2006]
SOAP	Simple Object Access Protocol. Es un protocolo para acceso a servicios web que define como dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML (eXtensible Markup Language).
Spam (correo basura)	STIC 401 GLOSARIO 2.969.2 CORREO BASURA Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S
Spear Phising	STIC 401 GLOSARIO 2.983.1 SPEAR PHISHING. Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima)
Spyware "spy software" (programas espía)	STIC 401 GLOSARIO 2.972.1 SPYWARE Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último. http://es.pcisecuritystandards.org 2.972.3 SPYWARE Código malicioso diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario. [CCN-STIC-400:2006] 2.972.4 SOFTWARE ESPÍA Cualquier forma de tecnología que se usa para recoger información sobre una persona o empresa, o información referente a equipos o a redes, sin su conocimiento o consentimiento. También puede venir implementado en su hardware. Puede capturar hábitos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet. Al igual que los virus puede ser instalado al abrir un adjunto de correo infectado, pulsando en una ventana de publicidad o camuflado junto a otros programas que instalemos. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S
SQL	Structured Query Language
Suplantación (Spoofing)	STIC 401 GLOSARIO 2.992.2 SUPLANTACIÓN (En inglés Spoofing) Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previa-mente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S 2.992.3 SPOOFING En materia de seguridad de redes, el término spoofing es una técnica de

	suplantación de identidad a través de la Red, llevada a cabo por un intruso generalmente con usos de malware o de investigación. Los ataques de seguridad en las redes a través de técnicas de spoofing ponen en riesgo la privacidad de los usuarios que navegan por Internet, así como la integridad de sus datos. De acuerdo a la tecnología utilizada se pueden diferenciar varios tipos de spoofing: • IP spoofing: Consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. • ARP spoofing: Es la suplantación de identidad por falsificación de tabla ARP. Las tablas ARP (Address Resolution Protocol) son un protocolo de nivel de red que relaciona una dirección de hardware con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que ésta envíe, será direccionado al ata-cante. • DNS spoofing: Es una suplantación de identidad por nombre de dominio, la cual con-siste en una relación falsa entre IP y nombre de dominio. • Web spoofing: Con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc. • Mail spoofing: Suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de phising o spam. http://www.inteco.es/glossary/Formacion/Glosario/Spoofing
Troyano	STIC 401 GLOSARIO 2.155.1 CABALLO DE TROYA. Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo. DRAE. Diccionario de la Lengua Española. 2.155.2 TROYANO También denominado “caballo de Troya”. Una clase de software malicioso que al instalarse permite al usuario ejecutar funciones normalmente, mientras los troyanos ejecutan funciones maliciosas sin que este lo sepa. http://es.pcisecuritystandards.org 2.155.3 TROYANO Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. [CCN-STIC-430:2006] 2.155.4 CABALLO DE TROYA Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa. Por ejemplo, un programa que reordene de una manera conveniente un fichero y, prevaliéndose de los derechos de escritura que debe concedérsele, copie el mismo en otro fichero accesible sólo por el creador de dicho programa .[Ribagorda:1997] CCN-CERT IA_09-15 Informe de Amenazas .Caballo de Troya o troyano, es un código dañino con apariencia de un programa inofensivo que al

	ejecutarlo brinda al atacante acceso remoto al equipo infectado, normalmente instalando una puerta trasera (backdoor).
Virus	STIC 401 GLOSARIO 2.1049.1 VIRUS Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros. [CCN-STIC-430:2006]

9. ANEXO E. REFERENCIAS

- RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.
- RD 951/2015, de 23 de octubre, de modificación del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- RD Ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Guía Nacional de Notificación y Gestión de Ciberincidentes.