GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 817

ESQUEMA NACIONAL DE SEGURIDAD
GESTIÓN DE CIBERINCIDENTES

Junio 2018

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.06.26 14:48:55 +02'00'

NIPO: 785-18-022-8

Fecha de Edición: junio de 2018
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.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010, de 8 de enero, desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Junio 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

TABLA DE CONTENIDOS

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. De acuerdo con el artículo 37 del RD 3/2010, el CCN tiene por misiones, entre otras:

   - El soporte y coordinación para el **tratamiento de vulnerabilidades y la resolución de incidentes de seguridad** que tengan la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.
   - La investigación y divulgación de **las mejores prácticas sobre seguridad de la información** entre todos los miembros de las Administraciones públicas. Con esta finalidad, las **series de documentos CCN-STIC** (*Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones*), elaboradas por el Centro Criptológico Nacional, ofrecerán **normas, instrucciones, guías y recomendaciones** para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.
   - La **formación** destinada al personal de la Administración especialista en el campo de la ciberseguridad, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.
   - La información sobre **vulnerabilidades, alertas y avisos** de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

3. Por su parte, la **Estrategia de Ciberseguridad Nacional** confiere al CCN-CERT un papel central en el desarrollo de su **Línea de Acción 2: Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas**, como actor imprescindible en la garantía de la plena implantación del ENS, mediante el refuerzo de las **capacidades de inteligencia, detección, análisis y respuesta del CCN-CERT y de sus Sistemas de Detección y Alerta Temprana**.

4. Es al amparo de estas funciones, misiones y responsabilidades, y de lo expresado en el artículo 29 del ENS, 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**[1].

[1] Consúltese la Guía CCN-STIC 403 Gestión de Incidentes de Seguridad, para una descripción más general de los Incidentes de Seguridad y su Gestión.

2. OBJETO

5. El propósito de esta Guía es ayudar a las entidades públicas del ámbito de aplicación del ENS 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.
   - CSIRTs (Computer Security Incident Response Team).
   - Administradores de Red y de Sistemas,
   - Personal de Seguridad,
   - Personal de apoyo técnico,
   - Responsables de Seguridad IT (CISO Chief Information Security Officer) y Responsables Delegados.
   - Responsables de Sistemas de Información (CIO Chief Information Officer) y, en general,
   - Gestores de programas de Ciberseguridad.

6. 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 tres 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).**
- **Cualesquiera otro tipo de ciberincidentes generales.**

3. ALCANCE

7. 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:

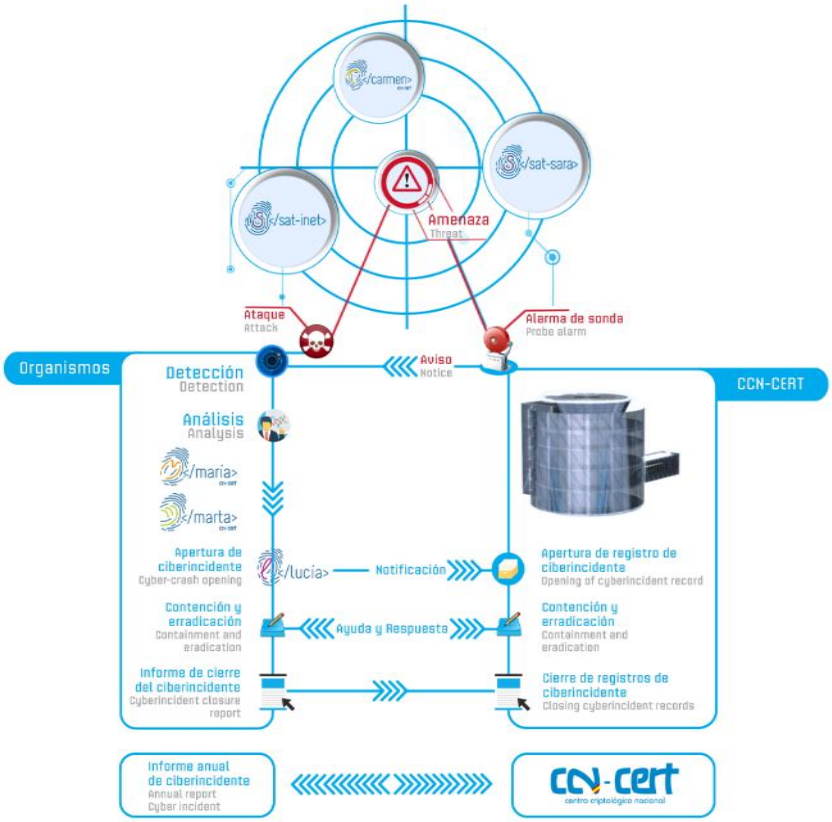
   - Se establecerá un sistema de detección y reacción frente a código dañino.

- 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.

8. 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. DIAGRAMA DE GESTIÓN DE LOS CIBERINCIDENTES

9. El gráfico siguiente muestra un esquema básico de actuación frente a un ciberincidente.
10. Obsérvese que 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.
11. En ambos situaciones, caso de confirmarse el ciberincidente, el organismo arrancará en paralelo la Notificación formal al CCN-CERT (usando la herramienta LUCIA) y las acciones de la fase de CONTENCIÓN, que comprenderá entre otras, las señaladas en el gráfico.
12. Una vez ERRADICADA la amenaza, el organismo, usando la misma herramienta, notificará al CCN-CERT el cierre del ciberincidente.



5. LA CAPACIDAD DE RESPUESTA A CIBERINCIDENTES

5.1EVENTOS Y CIBERINCIDENTES

13. Los ataques contra los Sistemas de Información son, cada día, no sólo más numerosos y diversos, sino también más peligrosos o potencialmente dañinos. Aunque las acciones y medidas preventivas, adoptadas en base a los resultados obtenidos de los preceptivos análisis de riesgos a los que deben someterse todos los sistemas públicos, contribuyen sin lugar a dudas a reducir el número de ciberincidentes, la realidad nos muestra que, desafortunadamente, no todos los ciberincidentes pueden prevenirse.

14. Por tanto, se hace necesario disponer de la adecuada **capacidad de respuesta a ciberincidentes**, que detectando rápidamente ataques y amenazas, minimice la pérdida o la destrucción de activos tecnológicos o de información, mitigue la explotación dañina de los puntos débiles de las infraestructuras y alcance la recuperación de los servicios a la mayor brevedad posible. Esta Guía ofrece pautas para el manejo de ciberincidentes y la determinación de la respuesta más adecuada a cada tipo, independientemente de la plataforma tecnológica subyacente, el hardware, los sistemas operativos o las aplicaciones.

15. Puesto que gestionar adecuadamente los ciberincidentes constituye una actividad compleja –que contempla la adopción de métodos para recopilar y analizar datos y eventos, metodologías de seguimiento, procedimientos de tipificación de su peligrosidad y priorización, así como la determinación de canales de comunicación con otras unidades o entidades, propias o ajenas a la organización-, la consecución de una capacidad de respuesta eficaz a ciberincidentes exige una **planificación escrupulosa** y la correspondiente **asignación de recursos**, adecuados y suficientes.

16. A efectos de utilizar un vocabulario común, se incluye en el Anexo D de esta Guía un Glosario con las definiciones terminológicas usadas en el texto.

5.2LA RESPUESTA A LOS CIBERINCIDENTES

17. Para los organismos públicos, el beneficio más significativo de poseer una adecuada capacidad de respuesta a ciberincidentes es abordar su gestión de forma sistemática (es decir, siguiendo una metodología consistente y consolidada), lo que facilita la adopción de las medidas adecuadas. Así, una correcta Capacidad de Respuesta a Ciberincidentes ayuda a los equipos de seguridad responsables a minimizar la pérdida o exfiltración de información o la interrupción de los servicios. Otro de sus beneficios es la posibilidad de utilizar la información obtenida durante la gestión del ciberincidente para preparar mejor la respuesta a incidentes de seguridad futuros y, en su consecuencia, proporcionar una mayor y mejor protección a los sistemas.

18. Además de pretender una mejor prestación de servicios de Administración Electrónica, los órganos y organismos del ámbito de aplicación del ENS deben acomodar su capacidad de respuesta a los ciberincidentes a la normativa legal que resulte de aplicación en cada caso y para cada Administración territorial o sectorial involucrada. Entre tal regulación cabe destacar la debida observancia a lo dispuesto en la Estrategia de Ciberseguridad Nacional, la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (y su normativa de desarrollo), la Ley 11/2007, de 22 de junio, de Acceso de los Ciudadanos a los Servicios Públicos, el Esquema Nacional de

Interoperabilidad (y su normativa derivada), el Esquema Nacional de Seguridad (y su normativa derivada), la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, entre otras.

5.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE CIBERINCIDENTES

19. Política de Seguridad

El artículo 11 del ENS señala los requisitos mínimos que debe contemplar toda Política de Seguridad, entre ellos, los **Incidentes de seguridad**, para los que debe especificarse:

- La posición del Equipo de Respuesta a Ciberincidentes (ERC), sus competencias y autoridad, dentro de la estructura de la organización y la definición de los roles y responsabilidades de cada unidad.
- Responsabilidades departamentales y personales.

20. Normativa de seguridad

- Definición de los ciberincidentes considerados a tenor del análisis de riesgos y los términos de referencia usados.
- Criterios para la comunicación de ciberincidentes y, en su caso, el intercambio de información, interna y externamente.
- Nivel de peligrosidad de los ciberincidentes

21. Procedimientos operativos de seguridad

- Mecanismos para la notificación de Informes de Ciberincidentes.
- Formularios de notificación, comunicación e intercambio de información.

22. Elementos del Plan de Respuesta a Ciberincidentes

Los organismos del ámbito de aplicación del ENS deben poseer un **Plan de Respuesta a Ciberincidentes** que dé adecuada respuesta a sus requisititos específicos, atendiendo a la misión, el tamaño, la estructura y las funciones de la organización. El Plan debe, asimismo, determinar y asegurar que se disponen de los recursos humanos y materiales necesarios y debe contar con el imprescindible apoyo por parte de la Dirección.

Una vez que el organismo ha redactado –y aprobado por su Dirección- el Plan de Respuesta a Ciberincidentes, se iniciará su implantación. El Plan deberá ser revisado, al menos, anualmente, para asegurar que el organismo está siguiendo adecuadamente la Hoja de Ruta para la mejora continua.

23. Procedimientos de Respuesta a Ciberincidentes

Cada organismo del ámbito de aplicación del ENS debe redactar y aprobar los **Procedimientos de Respuesta a Ciberincidentes**, que deberán estar fundamentados en la Política de Seguridad de la Información y el antedicho Plan de Respuesta a Ciberincidentes, y que comprenderán el desarrollo de aspectos técnicos, listas de control y formularios específicos, utilizados por el Equipo de Respuesta a Ciberincidentes (ERC).

6. LA GESTIÓN DE LOS CIBERINCIDENTES

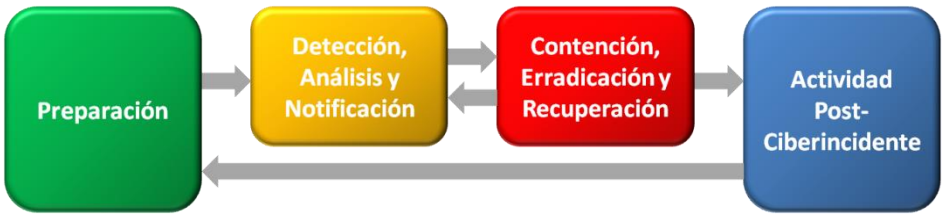
24. La gestión de ciberincidentes consta de varias fases.

25. 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[2]. Durante esta fase de **PREPARACIÓN**, el organismo público, atendiendo a lo dispuesto en 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. Sin embargo, como es sabido, incluso tras la implantación de tales medidas, persistirá un riesgo residual, que deberá ser asumido por la Alta Dirección del organismo.

26. 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 Y NOTIFICACIÓN**, desencadenando los procesos de notificación a los que hubiere lugar.

27. La organización, en la fase de **CONTENCIÓN, ERRADICACIÓN 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.

28. 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

29. *La Guía CCN-STIC 403 Gestión de Incidentes de Seguridad* desarrolla pormenorizadamente estas fases.

6.1 CLASIFICACIÓN DE LOS CIBERINCIDENTES

30. 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.

[2] 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).

31. 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**[3] de seguridad de los sistemas afectados.
    - 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**.

32. 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.

33. La tabla siguiente muestra una **clasificación de los ciberincidentes**, atendiendo al vector de ataque utilizado. (Ver Glosario en Anexo D)

CLASIFICACIÓN DE LOS CIBERINCIDENTES		
Clase de Ciberincidente	**Descripción**	**Tipo de ciberincidente**
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus
		Gusanos
		Troyanos
		Spyware
		Rootkit
		Ransomware (secuestro informático)
		Herramienta para Acceso Remoto Remote Access Tools (RAT)

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

Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	Denegación [Distribuida] del Servicio DoS / DDoS
		Fallo (Hardware/Software)
		Error humano
		Sabotaje
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	Identificación de activos y vulnerabilidades (escaneo)
		Sniffing
		Ingeniería social
		Phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	Compromiso de cuenta de usuario
		Defacement (desfiguración)
		Cross-Site Scripting (XSS)
		Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados
		Inyección SQL
		Spear Phishing
		Pharming
		Ataque de fuerza bruta
		Inyección de Ficheros Remota
		Explotación de vulnerabilidad software
		Explotación de vulnerabilidad hardware
		Acceso no autorizado a red
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información
		Modificación y borrado no autorizada de información.
		Publicación no autorizada de

		información
		Exfiltración de información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Suplantación / Spoofing
		Uso de recursos no autorizado
		Uso ilegítimo de credenciales
		Violaciones de derechos de propiedad intelectual o industrial.
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura)
		Acoso/extorsión/ mensajes ofensivos
		Pederastia/ racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	Abuso de privilegios por usuarios
		Acceso a servicios no autorizados
		Sistema desactualizado
		Otros
Otros	Otros incidentes no incluidos en los apartados anteriores	

Tabla 1.- Clasificación de los Ciberincidentes

6.2 LA DETECCIÓN DE LOS CIBERINCIDENTES

34. 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. Esta dificultad estriba en tres factores esenciales:

    – Los ciberincidentes pueden detectarse usando distintas herramientas, con diferentes niveles de detalle y fidelidad: **sistemas automatizados** de detección (incluyendo la utilización de IDS/IPS[4] de red o de servidor, software antivirus y analizadores de logs, entre otros) o **medios manuales** (como la notificación de problemas por parte de los propios usuarios). Además, algunos ciberincidentes se

[4] Intrusion Detection Systems e Intrusion Prevention Systems (Sistemas de Detección de Intrusiones y Sistemas de Prevención de Intrusiones)

manifiestan con signos de anomalías muy evidentes, mientras que otros, por el contrario, son muy complicados de detectar[5].

- El volumen de indicios de potenciales ciberincidentes es, normalmente, considerable. No es raro, por ejemplo, que una organización se encuentre con la necesidad de tratar miles o incluso millones de alertas diarias de sensores de intrusión.
- Es necesario disponer de un profundo conocimiento técnico especializado y una experiencia dilatada, que avalen un análisis adecuado y eficiente de los datos relacionados con los ciberincidentes.

35. 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*.

36. La mayoría de los ataques no tienen precursores identificables o detectables, desde la perspectiva del objetivo. Si la organización detecta la presencia de precursores, puede tener una oportunidad para evitar que el ciberincidente se materialice, acondicionando adecuadamente sus medidas de seguridad. 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[6].

37. Mientras que los precursores son relativamente escasos, 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, etc.

38. Incluso si un indicador es exacto, esto no significa necesariamente que se haya producido un ciberincidente. Algunos indicadores -tales como la caída de un servidor o la modificación de archivos críticos, por ejemplo- podrían tener lugar por distintas razones y muy alejadas de un ciberataque, incluyendo el error humano. Sin embargo, cuando un indicador da muestras de actividad es razonable sospechar que un incidente podría estar ocurriendo, debiéndose actuar en consecuencia. La determinación de si un evento en particular es en realidad un ciberincidente constituye, en ocasiones, una cuestión de apreciación y juicio, siendo necesario intercambiar la información del

[5] Como es el caso de los ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia: los conocidos como APTs (Advanced Persistant Threat Amenazas Avanzadas Persistentes)
[6] Es el caso del anuncio de ataques por grupos hacktivistas, por ejemplo.

supuesto ciberincidente con diferentes miembros del ERC y, en su caso, de otra unidad (interna o externa), para poder tomar una decisión razonablemente adecuada[7].

39. Aunque algunos ciberincidentes son fáciles de detectar (por ejemplo, la desfiguración de una página web), muchos de ellos no presentan síntomas claros. En ocasiones, pequeños indicios (tales como alteraciones en un archivo de configuración del sistema, por ejemplo) pueden ser los únicos indicadores de la ocurrencia de un ciberincidente.

40. 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)**[8] y del **Sistema de Alerta Temprana de Internet (SAT-INET)**[9] da adecuada respuesta a todas estas necesidades.

6.3 LA PELIGROSIDAD DE LOS CIBERINCIDENTES

41. 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[10] 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.

42. 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) o de Internet (SAT-INET).

[7] A estos efectos, el CCN-CERT viene prestando soporte y ayuda a los organismos de las AA.PP. españolas a determinar la verosimilitud y certidumbre de los ciberincidentes.
[8] 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.
[9] 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.
[10] *Peligrosidad*: Cualidad de peligroso. (DRAE, edición 22ª). En otros textos puede denominarse como criticidad.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES[11]			
NIVEL	**AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)**	**VECTOR DE ATAQUE**	**CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE**
CRÍTICO	**Ciberespionaje**	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
MUY ALTO	**Interrupción de los Servicios IT / Exfiltración de datos / Compromiso de los servicios**	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	**Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación**	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL. - Spear phising / pharming	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	**Logro o incremento significativo de capacidades ofensivas / Desfiguración de páginas web / Manipulación de información**	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de activos y vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	**Ataques a la imagen / menosprecio / Errores y fallos**	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

[11] En relación con las entidades del ámbito de aplicación del ENS.

6.3.1 DOCUMENTACIÓN DE LOS CIBERINCIDENTES

43. 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.

6.3.2 NIVEL DE IMPACTO DEL CIBERINCIDENTE EN LA ORGANIZACIÓN

44. 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.

45. Así, la gestión de los ciberincidentes debe priorizarse en base a distintos criterios, entre los que destacan:

- Impacto Funcional del Ciberincidente: El Equipo de Respuesta de Ciberincidentes (ERC) debe considerar la forma en que el ciberincidente puede impactar en la funcionalidad de los sistemas afectados.
- El Impacto del ciberincidente en la Información o los Servicios: Puesto que los ciberincidentes pueden afectar a la confidencialidad e integridad de la información tratada por el organismo y/o a la disponibilidad de los servicios prestados, el ERC debe considerar cómo el ciberincidente puede impactar en el desenvolvimiento competencial del organismo o en su imagen pública.
- Recuperación del ciberincidente: Puesto que el tipo de ciberincidente y la superficie de activos atacada determinará el tiempo y los recursos que deben destinarse a la recuperación, el ERC, con la ayuda oportuna de otros departamentos del organismo, debe considerar el esfuerzo necesario para regresar a la situación pre-ciberincidente y su oportunidad.

Estos criterios pueden cambiar si en el transcurso del proceso de su gestión se modificasen las circunstancias ó conocimiento que se tiene del ciberincidente.

46. El cuadro siguiente muestra cómo debe determinar el organismo afectado **el Nivel de Impacto Potencial**[12] de los Ciberincidentes en la organización.

Nivel	Descripción
I0 – IRRELEVANTE	• No hay impacto apreciable sobre el sistema • No hay daños reputacionales apreciables

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

I1 – BAJO	• La categoría más alta de los sistemas de información afectados es BÁSICA • El ciberincidente precisa para resolverse menos de 1 JP[13] • Daños reputacionales puntuales, sin eco mediático
I2 – MEDIO	• La categoría más alta de los sistemas de información afectados es MEDIA • Afecta a más de 10 equipos con información cuya máxima categoría es BÁSICA • El ciberincidente precisa para resolverse entre 1 y 10 JP • Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación)
I3 – ALTO	• La categoría más alta de los sistemas de información afectados es ALTA • Afecta a más de 50 equipos con información cuya máxima categoría es BÁSICA • Afecta a más de 10 equipos con información cuya máxima categoría es MEDIA • El ciberincidente precisa para resolverse entre 10 y 20 JP • Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros
I4 – MUY ALTO	• Afecta a sistemas clasificados RESERVADO • Afecta a más de 100 equipos con información cuya máxima categoría es BÁSICA • Afecta a más de 50 equipos con información cuya máxima categoría es MEDIA • Afecta a más de 10 equipos con información cuya máxima categoría es ALTA • El ciberincidente precisa para resolverse entre 20 y 50 JP • Daños reputacionales a la imagen del país (marca España) • Afecta apreciablemente a actividades oficiales o misiones en el extranjero • Afecta apreciablemente a una infraestructura crítica

[13] JP – Jornada-persona; estimación del esfuerzo necesario para realizar una tarea cuya unidad equivale a una jornada de trabajo ininterrumpido de un trabajador medio.

I5 - CRÍTICO	• Afecta a sistemas clasificados SECRETO • Afecta a más de 100 equipos con información cuya máxima categoría es MEDIA • Afecta a más de 50 equipos con información cuya máxima categoría es ALTA • Afecta a más de 10 equipos con información clasificada RESERVADO • El ciberincidente precisa para resolverse más de 50 JP • Afecta apreciablemente a la seguridad nacional • Afecta gravemente a una infraestructura crítica

Tabla 4 – Criterios de determinación del Nivel de Impacto

6.4SEGUIMIENTO POR PARTE DEL CCN-CERT

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

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

Estado	Descripción
Cerrado sin actividad	No hay respuesta por parte del organismo.
Solicita más información	El organismo afectado requiere más información por parte del CCN-CERT para el correcto cierre del incidente.
Cerrado (Ha existido ciberincidente)	La detección ha resultado positiva y ha afectado a los sistemas del organismo.
Cerrado (Sin impacto)	La detección ha resultado positiva pero el organismo no es vulnerable o no se ve afectado.
Cerrado (Falso positivo)	La detección ha sido errónea.
Cerrado (Sin respuesta)	Pasado un periodo de 60 días, si el ciberincidente no ha sido cerrado por el organismo, es cerrado por el Sistema de Alerta Temprana correspondiente, con este estado.
Abierto	Habitualmente, este estado aparece cuando el ticket no se gestiona debidamente por el organismo afectado. A los ciberincidentes con este estado se les pasa al estado adecuado (habitualmente, "cerrado sin actividad").

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

49. Dicho seguimiento se realizará en función del nivel de peligrosidad del ciberincidente, en base a la siguiente tabla:

Nivel de Peligrosidad	Obligación de notificación del ciberincidente al CCN-CERT(*)	Cierre del ciberincidente (días naturales)	Precisiones
BAJO	No	15	- Se cierran automáticamente por los Sistemas de Alerta Temprana a los 60 días con el estado "Cerrado – Sin respuesta". - El Sistema de Alerta Temprana no renotifica el aviso al organismo afectado.
MEDIO	No	30	
ALTO	Sí	45	
MUY ALTO	Sí	90	- No debe asignarse nunca el estado "Cerrado – Sin respuesta) - El Sistema de Alerta Temprana re-notifica el aviso al organismo afectado cada siete días hasta recibir respuesta.
CRÍTICO	Sí	120	

Tabla 6 - Tipo de seguimiento a realizar por parte del CCN-CERT, según Nivel de Peligrosidad

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.

6.5 TIPIFICACIÓN DE CAUSAS Y HECHOS DEL CIBERINCIDENTE

50. Ante la avalancha de datos disponibles, es conveniente disponer de unos pocos indicadores suficientemente representativos de la seguridad del sistema, para obtener unas métricas que permitan sustentar la toma de decisiones, especialmente, en dos aspectos: cumplimiento normativo y ejecución de proyectos.

51. Así, tal y como recoge la Guía CCN-STIC 815[14], será necesario recopilar la siguiente información que permita un tratamiento posterior:

<u>En relación al momento del ciberincidente:</u>

- Fecha y Hora de detección del ciberincidente.
- Fecha y hora de notificación,
- Fecha y hora de resolución y cierre.
- Impacto o consecuencias.

[14] Guía CCN-STIC 815 Métricas e Indicadores en el ENS.

En relación con los activo(s) involucrados:

- Nivel de degradación del activo afectado: alta, media o baja.
- Dimensión de la seguridad afectada: Confidencialidad, Disponibilidad e Integridad (si las dimensiones trazabilidad y autenticidad se ven afectadas se considerará como un caso en que se encuentra afectada la integridad de la información).

Causa del Ciberincidente:

Causas (raíz) del ciberincidente (marcar las que procedan)		Anexo II del ENS [15]
Código	**Descripción**	
C.1	incumplimiento o carencia de normativa de seguridad	org.1 org.2
C.2	incumplimiento o carencia de procedimientos de seguridad	org.3
C.3	incumplimiento del proceso de autorización	org.4
C.4	fallo técnico u operativo de identificación o autenticación	op.acc.1 op.acc.5
C.5	fallo técnico u operativo de los controles de acceso	op.acc.2 op.acc.4
C.6	acceso local no autorizado	op.acc.6
C.7	acceso remoto no autorizado	op.acc.7
C.8	ausencia o deficiencia de la segregación de funciones y tareas	op.acc.3
C.9	entrada de datos incorrectos que no han sido detectados a tiempo	
C.10	configuración inadecuada	op.exp.2 op.exp.3
C.11	ausencia o deficiencia de mantenimiento	op.exp.4
C.12	inadecuada ejecución de un cambio	op.exp.5
C.13	falta de concienciación del personal	mp.per.3
C.14	defectos de formación del personal	mp.per.4
C.15	puestos de trabajo no despejados	mp.eq.1
C.16	información remanente no autorizada	mp.si.5
C.17	defectos en la especificación de una aplicación SW	mp.sw
C.18	defectos en la implantación de una aplicación SW	mp.sw.2
C.19	entrada en operación de equipamiento (SW, HW, COMMS) defectuoso	mp.sw.2
C.20	servicio externo: causados por negligencia del proveedor	mp.ext.2
C.21	servicio externo: que no se han comunicado dentro de los plazos y cauces acordados	mp.exp.2
C.22	servicio externo: el proveedor responsable ha incumplido las obligaciones acordadas	mp.exp.2

Tabla 7 – Incidencias en la resolución del Ciberincidente

[15] Nomenclatura empleada en el ENS, que recoge los tres grupos en que se engloban las medidas de seguridad: marco organizativo [org], marco operacional [op] y medidas de protección [mp].

6.6MÉTRICAS E INDICADORES

52. 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.

6.7 RECOLECCIÓN Y CUSTODIA DE EVIDENCIAS

53. 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[16].

54. 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.

55. 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[17], 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[18].

56. 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:

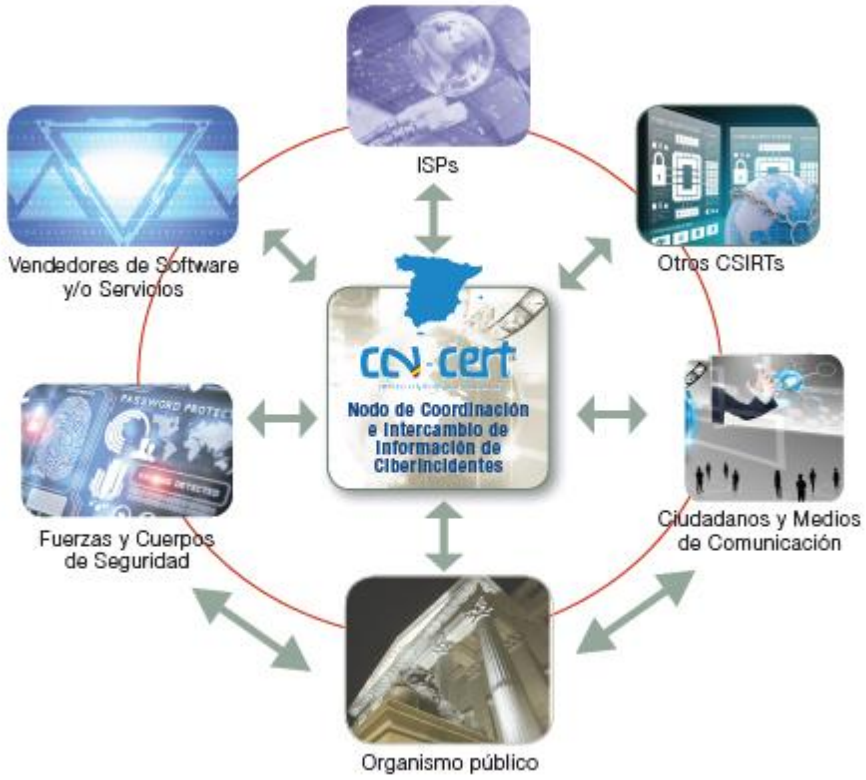
- Persecución del delito: Si, como consecuencia del ciberincidente, pudiera procesarse al atacante, será necesario custodiar adecuadamente las pruebas del delito hasta que se hayan completado todas las acciones legales.
- Retención de datos: Todos los organismos deben poseer políticas de retención de 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.

[16] 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.
[17] Y trabajar, a partir de entonces, con copias del sistema.
[18] 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.

6.8 INTERCAMBIO DE INFORMACIÓN Y COMUNICACIÓN DE CIBERINCIDENTES

57. 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, vendedores de software, etc.) se desarrollarán a través del CCN-CERT, en su función de **Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las AA.PP.**



Comunicación a Terceros de Información de Ciberincidentes

58. Independientemente de lo anterior, el Equipo de Respuesta a Ciberincidentes debe analizar con el Departamento de Relaciones Institucionales del organismo, con la Asesoría Jurídica y con la Alta Dirección los criterios y procedimientos de información a terceros antes de que ocurra un ciberincidente. De lo contrario, podría darse el caso de que información confidencial contenida en la información de los ciberincidentes pueda entregarse a terceros no autorizados, lo que, además de representar un daño a la imagen del organismo y una falta grave de incumplimiento legal, podría dar lugar a la exigencia de responsabilidad patrimonial de la entidad, por daños y perjuicios ocasionados a terceros.

59. Como se ha dicho, 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.

60. 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.

7. 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

7.2MÉTRICAS DE EFICACIA

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

7.3 MÉTRICAS DE EFICIENCIA

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	950%
		Frecuencia medición	trimestral
		Frecuencia reporte	anual

7.4INDICADORES CRÍTICOS DE RIESGO (KRIS19)

M5	**Indicador**	Rotación de personal	
	Objetivo	Estabilidad del equipo de gestión de incidentes	
	Método	A = número de personas que dejan el equipo de respuesta de incidentes durante el periodo de cómputo T = número de personas que forman parte del equipo al final del periodo de cómputo fórmula: A / T	
	Caracterización	Objetivo	0%
		Umbral amarillo	20%
		Umbral rojo	50%
		Frecuencia medición	anual
		Frecuencia reporte	anual

M6	**Indicador**	Madurez del personal	
	Objetivo	Experiencia del equipo de gestión de incidentes	
	Método	Q(x) = número de meses de experiencia en gestión de incidentes del x% más nuevo de los miembros del equipo ejemplo: si Q(25) = 24m, indica que el 25% del personal tiene menos de 24 meses de experiencia en la materia	
	Caracterización	Objetivo	Q(25) > 24m && Q(50) > 36m
		Umbral amarillo	Q(25) < 12m || Q(50) < 24m
		Umbral rojo	Q(25) < 6m || Q(50) < 12m
		Frecuencia medición	anual
		Frecuencia reporte	anual

M7	**Indicador**	Peligrosidad del acceso a servicios externos	
	Objetivo	Medir si el salir al exterior está causando problemas al organismo	
	Método	Medimos NI: el número de incidentes de nivel de peligrosidad MUY ALTO o CRÍTICO Medimos NS: número de sesiones en Internet originadas por el organismo fórmula: NI / NS	
	Caracterización	Objetivo	crecimiento anual 0%
		Umbral amarillo	10%
		Umbral rojo	30%
		Frecuencia medición	trimestral
		Frecuencia reporte	anual

[19] Key Risk Indicators (Indicadores críticos de riesgo)

M8	**Indicador**	Peligrosidad del acceso externo a los servicios del organismo	
	Objetivo	Medir si admitir entradas desde el exterior está causando problemas al organismo	
	Método	Medimos NI: el número de incidentes de nivel de peligrosidad MUY ALTO o CRÍTICO Medimos NS: número de sesiones web o ftp de las que el organismo es servidor fórmula: NI / NS	
	Caracterización	Objetivo	crecimiento anual 0%
		Umbral amarillo	10%
		Umbral rojo	30%
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

M9	**Indicador**	Peligrosidad del correo electrónico	
	Objetivo	Medir si admitir email desde el exterior está causando problemas al organismo	
	Método	Medimos NI: el número de incidentes de nivel de peligrosidad MUY ALTO o CRÍTICO Medimos NE: número de correos recibidos fórmula: NI / NE	
	Caracterización	Objetivo	crecimiento anual 0%
		Umbral amarillo	10%
		Umbral rojo	30%
		Frecuencia medición	trimestral
		Frecuencia reporte	anual

8. ANEXO B. ELEMENTOS PARA EL INFORME DE CIERRE DEL CIBERINCIDENTE[20]

- **Nivel de Peligrosidad (final) del ciberincidente.**
- **Resumen de las acciones realizadas para:**
  - Contención del ciberincidente,
  - Erradicación del ciberincidente y
  - Recuperación de los sistemas afectados.
- **Impacto del ciberincidente, medido en:**
  - Número de equipos afectados
  - Valoración del impacto en la imagen pública del Organismo
  - Dimensión/es (Confidencialidad, Integridad, Disponibilidad, Autenticación, Trazabilidad, Legalidad) de la seguridad afectada/s
  - Porcentaje de degradación sufrido en los servicios ofrecidos a los ciudadanos
  - Porcentaje de degradación sufrido en los servicios internos del Organismo
  - Valoración del coste del incidente directamente imputable al incidente:
  - en horas de trabajo
  - Coste de compra de equipamiento o software necesario para la gestión del incidente
  - Coste de contratación de servicios profesionales para la gestión del incidente.

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

9. ANEXO C. INTRODUCCIÓN A LA HERRAMIENTA LUCÍA

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.

9.1 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) y Red SARA (SAT-SARA).
- Posibilitar la comunicación de incidentes de seguridad desde plataformas externas en aquellos organismos que utilicen otra tecnología (v.g., Remedy).

9.2 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).

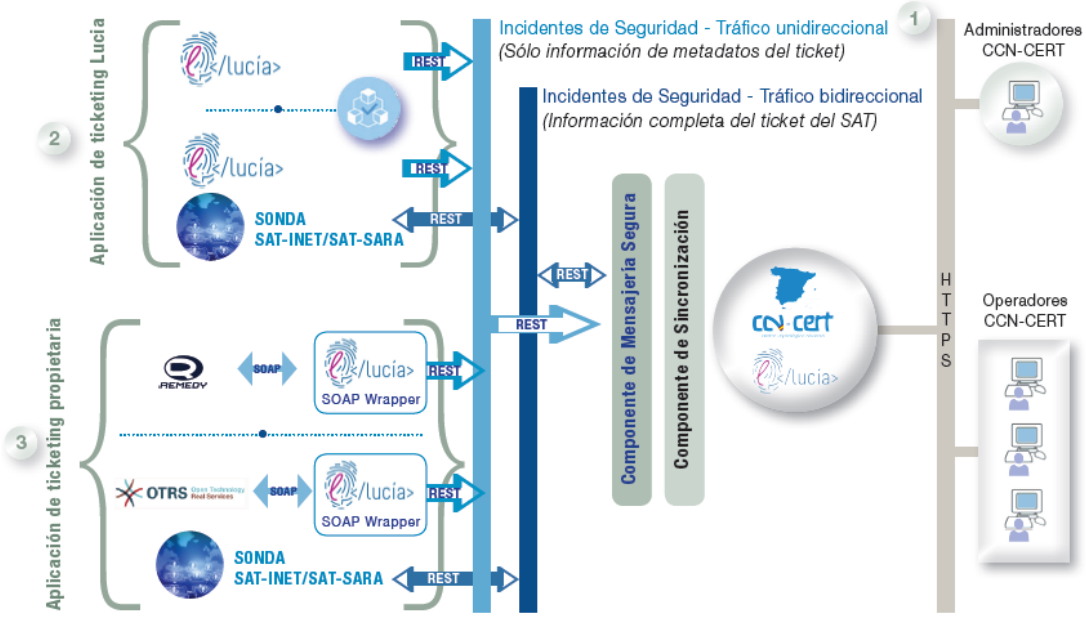
Entre sus características principales destacan las siguientes:

- 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.

9.3 ARQUITECTURA

El siguiente gráfico muestra el diagrama conceptual de arquitectura del sistema LUCIA.



(1) Incidentes de Seguridad -Tráfico unidireccional *(Sólo información de metadatos del ticket)*
Incidentes de Seguridad –Tráfico bidireccional *(Información completa del ticket del SAT)*

(2) Aplicación de Ticketing LUCIA

(3) Aplicaciones Ticketin Propietaria

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

- Sincronización Unidireccional: El componente 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.

Este componente 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 (organismos adscritos a los Sistemas de Alerta Temprana SAT-INET y SAT-SARA): El componente de Sincronización Bidireccional, permitirá dotar al sistema de la funcionalidad desarrollada en el Componente de Sincronización Unidireccional desde el propio servidor central LUCIA RT-IR hacia ciertos LUCIA desplegados en ciertos organismos en los que el CCN-CERT dispone de sondas.

  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.

9.4 INTERCONEXIÓN: CONECTORES

La plataforma permite la integración de aquellos organismos que ya dispongan de sistemas de ticketing con la instancia LUCIA del CCN-CERT.

Para lograrlo, implementa una capa de integración SOAP[21] para la conexión con sistemas estándar denominado "SOAP Wrapper" que permite la comunicación REST con la plataforma RT, así como la comunicación SOAP con plataformas externas.

La existencia de la capa REST de integración permite acometer desarrollos a medida para sistemas que no dispongan de interfaces de integración SOAP.

En la actualidad, LUCIA dispone de un conector BMC Remedy, existiendo la posibilidad futura de integrar otras herramientas, tales como OTRS, HP Service Manager, Track, RedMine, Mantis, etc.

[21] 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)).

10.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 con-figuraciones 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	STIC 401 GLOSARIO 2.358 CROSS-SITE REQUEST FORGERY Acrónimos: CSRF, XSRF

petición entre sitios cruzados	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	STIC 401 GLOSARIO Ver: • http://en.wikipedia.org/wiki/Phishing

"fishing" pescando). Spear phishing ("lanza")	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 (Remote Acces Tool) Herramienta para Acceso Remoto	Pieza de software que permite a un "operador" controlar a distancia un 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]

11.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.
- Guía CCN-STIC 403 Gestión de incidentes de seguridad.
- Guía CCN-STIC 815 Métricas e Indicadores en el ENS.
- NIST SP 800-61 (Rev 2) Computer Security Incident Handling Guide (Aug., 2012).
- NIST SP 800-150 (Draft) Guide to Cyber Threat Information Sharing (Oct., 2014).