1. Qué es un incidente de seguridad

Son **diferentes** las definiciones que se pueden encontrar al respecto.

De acuerdo con la normativa **ISO 27001** un incidente de seguridad de la información seria:

> ***"un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información".***

De forma más simplificada, I**NCIBE** define un incidente de ciberseguridad como:

> ***"cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa".***

1. Qué es un incidente de seguridad

Es interesante matizar que los términos "suceso" y "evento' son sinónimos y se podrían definir como:

- **Suceso:** ocurrencia o cambio de un conjunto particular de circunstancias [*UNE guía 73:2010*].
- **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*].
- **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*].

1. Qué es un incidente de seguridad

Se debe tener presente pues que un evento de seguridad de la información se refiere a algo que puede afectar a los niveles de riesgo, sin afectar de forma necesaria al negocio o a la información. Sin embargo, un incidente de seguridad de la información se refiere a algo que afecta de forma negativa tanto a los procesos del negocio como a la información.

Algunos ejemplos de incidentes de ciberseguridad serían los siguientes:

- accesos no autorizados a información corporativa (intrusiones, amenazas persistentes avanzadas, etc.).
- código dañino en los sistemas corporativos (gusanos, troyanos, virus, ransomware, rootkits, backdoors (RAT), downloaders, etc.).
- código no autorizado en los sistemas corporativos (por ejemplo, software pirata).
- Ataques remotos (denegación de servicio, reconocimiento activo del perímetro, etc.).
- ataques a los contenidos (Defacement, distribución de contenido fraudulento o malicioso, etc.).

1. Qué es un incidente de seguridad

Es habitual encontrar a diario en prensa noticias sobre incidentes de ciberseguridad que comprometen las actividades de las organizaciones o los datos de los ciudadanos, como los prolíficos ataques por ransomware (secuestro de información a cambio de beneficio económico), ataques de denegación de servicio, ataques a cadena de suministro (supply chain attack), ciber espionaje, campanas de phishing, etc. Y es que, existe una gran variedad de ciber amenazas por las que un actor hostil puede alcanzar sus objetivos o motivaciones:

- Ciber espionaje (robo de información en beneficio propio o de un tercero como un estado u organización).
- Ciberdelito (beneficio económico, daño reputacional, etc.).
- Ciberterrorismo (provocación de daños en el plano físico, ataques a infraestructuras críticas, etc.).
- Ciberactivismo (reivindicación ideológica, protesta, etc.).
- Ciberguerra (superioridad en el ciberespacio...).

1. Qué es un incidente de seguridad

No obstante, los incidentes de ciberseguridad no siempre son causados por atacantes, sino que pueden estar asociados a accidentes o errores no intencionados. En cualquier caso, deben ser gestionados de la forma más idónea posible, esto es, minimizando al máximo su impacto, restaurando los niveles de operación lo antes posible y previniendo, en la medida de lo posible, la ocurrencia de los mismos.

1. Qué es un incidente de seguridad

NORMATIVA DE REFERENCIA

En este apartado se citan los estándares más utilizados actualmente en gestión de incidentes de ciberseguridad, tanto a nivel nacional como internacional.

ISO 27035

La familia de normas relativas a la gestión de la seguridad de la información por excelencia es la norma ISO 27000 y dentro de ella, el estándar definido en gestión de incidentes de seguridad de la información es la norma ISO 27035, publicada en 2011. Se trata de la estandarización del informe técnico ISO/IEC TR 18044, publicado en 2004, el cual define los objetivos a cumplir en la gestión de incidentes de seguridad y como llegar a alcanzarlos en todo su ciclo de vida.

Los objetivos que marca la norma ISO 27035, de aplicación en cualquier ámbito a la hora de llevar a cabo la gestión de incidentes de seguridad, se pueden resumir en:

- Detección y gestión de los eventos de seguridad que se produzcan determinando si corresponden o no a un incidente.

1. Qué es un incidente de seguridad

- respuesta a los incidentes de forma proporcional, ágil y adecuada de manera que se minimice el impacto asociado a los incidentes acontecidos.
- Extracción de lecciones aprendidas a partir de los incidentes gestionados de forma que se mejore el estado global de la seguridad corporativa, incluyendo la optimización de los procedimientos de gestión de incidentes.

1. Qué es un incidente de seguridad

NORMATIVA DE REFERENCIA

NIST

NIST es el acrónimo De Instituto Nacional De Estándares Y Tecnologia (Nationa! Institute Of Standards And Technology), organismo dependiente del departamento de comercio de Estados Unidos.

Como resultado de la creciente cantidad de ciberataques a sistemas de infraestructuras críticas y al impacto que dichos ataques pudieran tener en el contexto de la seguridad nacional de Estados Unidos, el 12 de febrero de 2013 el presidente Barack Obama redactó la orden ejecutiva (EO) de Mejora De Ciberseguridad De Infraestructuras Criticas (executive order 13636 - Improvingcritical Infastructure Cybersecurity) en donde se delegaba en el NIST el desarrollo de un marco de trabajo para la reducción de riesgos asociados con este tipo de entornos, con el soporte del gobierno, la industria y los usuarios.

Algunos de los requerimientos NIST CSF fueron:

1. Qué es un incidente de seguridad

- Identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura critica.
- Proporcionar un enfoque prioritario, flexible, repetible, basado en el rendimiento y rentabilidad.
- Ayudar a identificar, evaluar y gestionar el riesgo cibernético.
- Incluir orientación para medir el desempeño de la implementación del marco de ciberseguridad.
- Identificar áreas de mejora que deben abordarse a través de la colaboración futura con sectores particulares y organizaciones que desarrollan estándares.

A raiz de este trabajo, NIST ofrece un conjunto de documentos de libre descarga, la serie NIST SP 800, que describe las políticas de seguridad informática, procedimientos y directrices que proporcionan información que cubre tanto la gestión como las prácticas operativas de seguridad de la información.

Con respecto a las acciones de respuesta a incidentes de ciberseguridad, NIST cuenta con una guía especializada [6] dentro de esta serie, denominada "Computer Security Incident Handling Guide. Recommendations Of The National Institute Of Standards

1. Qué es un incidente de seguridad

And Techology (Sp 800-61)" que pretende ayudar a las organizaciones a obtener la capacidad de respuesta ante incidentes necesaria, así como dar una serie de directrices y pautas para llevar a cabo una completa gestión de un incidente de seguridad.

1. Qué es un incidente de seguridad

NORMATIVA DE REFERENCIA

ENS

En España, el esquema nacional de seguridad (ENS) es una normativa que aplica al sector público y puede servir de orientación al sector privado, cuyo objeto es el establecimiento de los medios electrónicos que permita la adecuada protección de la información. Tal y como recoge el Real Decreto 3/2010:

"La finalidad del esquema nacional de seguridad es la creación de 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, que permita a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios…".

En las decisiones en materia de ciberseguridad, de acuerdo con el ENS, se contemplan los siguientes principios básicos:

1. Qué es un incidente de seguridad

- La seguridad se entenderá como un **proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.
- **El análisis y gestión de riesgos** será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- **Prevención, reacción y recuperación**. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
- **Líneas de defensa**. El sistema ha de disponer de una estrategia de protección formada por múltiples capas de seguridad. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
- **Reevaluación periódica**. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

1. Qué es un incidente de seguridad

- La seguridad como función diferenciada. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El centro criptológico nacional (CCN) es el encargado de la difusión de guías especificas para el mejor cumplimiento del ENS y ofrece una serie de directrices para la gestión de incidentes, que engloban aspectos como la clasificación (taxonomía) de los incidentes, su peligrosidad, su impacto, e incluso por qué es necesario notificar un incidente o cuáles son los incidentes de obligada notificación.

Uno de los principales documentos relacionado con estas directrices es la guía de seguridad de las tic **CCN-STIC 817 "Esquema Nacional De Seguridad. Gestión De Ciber incidentes"** publicada por el CCN en abril de 2020.

El CCN desarrolla esta guía 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:

1. Qué es un incidente de seguridad

> ***"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"***

El objeto de dicha guía es ayudar al cumplimiento del ENS a través del establecimiento de las capacidades de respuesta ante incidentes y su adecuado tratamiento, dirigiéndose especialmente a equipos de respuesta a incidentes, responsables de seguridad de la información, responsables de sistemas de la información y en general, a gestores del ámbito de la ciberseguridad y administradores de sistemas de información y/o comunicaciones.

Otra guía nacional interesante a mencionar en este epígrafe, y que va alineada con la publicada por el CCN, es la "guía nacional de notificación y gestión de ciber incidentes" aprobada por el consejo nacional de ciberseguridad el día 21 de febrero de 2020 y que se define como:

1. Qué es un incidente de seguridad

> ***"La referencia estatal respecto a la notificación de ciber incidentes (bien sea la comunicación de carácter obligatoria o potestativa), así como en lo relativo a la demanda de capacidad de respuesta a los incidentes de ciberseguridad.***
>
> ***Asimismo, este documento se consolida como una referencia de mínimos en el que toda entidad, pública o privada, ciudadano u organismo, encuentre un esquema y la orientación precisa acerca de a quién y cómo debe reportar un incidente de ciberseguridad acaecido en el seno de su ámbito de influencia."***

Esta guía remarca que la gestión de incidentes de ciberseguridad, y particularmente la notificación a su autoridad competente o de referencia, constituye un imperativo legal para determinadas organizaciones públicas y privadas de España, tal y como se verá en siguientes puntos de este libro.

Adicionalmente a las guías citadas, mencionar que desde INCIBE-CERT se ha publicado el anexo "**Procedimiento de gestión de ciber incidentes para el sector**

1. Qué es un incidente de seguridad

privado y la ciudadanía" que pretende servir de apoyo en las tareas propias de la gestión de incidentes de seguridad y en las particularidades de la comunicación con este organismo si corresponde.

el marco regulador a nivel nacional viene definido tomando como referencia la siguiente normativa, tal y como se indica en la guía nacional de notificación y gestión de ciber incidentes:

De carácter general:

- Ley orgánica 10/1995, de 23 de noviembre, del código penal.
- Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales.
- Ley 9/2014, de 9 de mayo, general de telecomunicaciones.
- Real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

1. Qué es un incidente de seguridad

- Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de
- La ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Disposición adicional novena. Gestión de incidentes de ciberseguridad que afecten a la red de internet de la ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Reglamento de ejecución (UE) 2018/151 de la comisión europea de 30 de enero de 2018 por el que se establecen normas para la aplicación de la directiva (UE) 2016/1148 del parlamento europeo y del consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales.

De carácter particular al ámbito del sector público:

- Ley 11/2002, de 6 de mayo, reguladora del centro nacional de inteligencia.
- Ley 40/2015 de 1 de octubre, de régimen jurídico del sector público.

1. Qué es un incidente de seguridad

- Real decreto de 421/2004, de 12 de marzo, por el que se regula el centro criptológico nacional.
- Real decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad, para las entidades del sector público de su ámbito de aplicación. Modificado en RD 951/2015.
- Instrucción técnica de seguridad de notificación de incidentes de seguridad publicada en BOE n º 95 de 18 de abril de 2018.

De carácter particular al ámbito de las infraestructuras criticas:

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real decreto 704/2011, de 20 de mayo, por el que se aprueba el reglamento de protección de las infraestructuras críticas.
- Plan Nacional de Protección de Infraestructuras Criticas (PNPIC), aprobado mediante Instrucción núm. 1/2016, de la Secretaría de Estado de Seguridad.

1. Qué es un incidente de seguridad

- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.
- Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de 21 de octubre de 2015.

De carácter particular a las redes militares y de defensa:

- Real Decreto 998/2017, de 24 de noviembre, por el que se desarrolla la estructura orgánica básica del MDEF y modifica el Real Decreto 424/2016, de 11 de noviembre.
- Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.
- Orden DEF 166/2015, 21 de enero, que desarrolla la organización básica de las FAS (deroga la Orden Ministerial 10/2013).

1. Qué es un incidente de seguridad

TAXONOMÍA DE LOS INCIDENTES

Puesto que no todos los incidentes poseen las mismas particularidades ni tienen las mismas implicaciones, cada organización debe establecer una taxonomía de los incidentes a gestionar, lo que ayudará posteriormente a su análisis, contención y erradicación.

Crear una taxonomía no es una tarea sencilla. Puede haber diferentes formas de clasificar los incidentes y no siempre es fácil o posible determinar cual es la mejor. Muchas organizaciones a menudo terminan desarrollando su propia taxonomía para uso interno. No obstante, se recomienda adoptar taxonomías inspiradas en las proporcionadas por organismos de referencia, de forma que incluyan un mapeo de las clasificaciones de incidentes con un marco legal. De acuerdo con la "Guía de Seguridad de las TIC CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciber incidentes", son varios los factores a considerar a la hora de establecer criterios de clasificación: tipo de la amenaza (código dañino, intrusiones, fraude, etc.), origen de la amenaza, la categoría de seguridad de los sistemas afectados, el perfil de los usuarios comprometidos, el número y tipología de los sistemas involucrados en el incidente, el impacto que el incidente puede tener en la organización, etc.

1. Qué es un incidente de seguridad

ENISA (European Union Agency for Cybersecurity) ha publicado varios documentos relacionados con las taxonomías, como son "ENISA Report: Information sharing and common taxonomies between CSIRTs and Law Enforcement (Dec 2015)", "ENISA Report: A good practice guide of using taxonomies in incident prevention and detection (Dec 2016)" o "Reference Incident Classification Taxonomy (Jan 2018)". Este último documento es el que tanto la Guia CCN-STIC 817 como la Guía Nacional de Notificación y Gestión de Ciber incidentes toman como referencia para establecer su propuesta de taxonomía, que viene a resumirse en la siguiente tabla:

1. Qué es un incidente de seguridad

CLASIFICACIÓN/TAXONOMÍA DE LOS INCIDENTES		
Clasificación	Tipo de incidente	Descripción
Contenido abusivo	*Spam*	Correo electrónico masivo no solicitado.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej.: ciberacoso, amenazas a colectivos o personas.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con la pornografía infantil, apología de la violencia, etc.
Código dañino	Sistema infectado	Sistema comprometido con *malware*.
	Servidor de C&C (*Command and Control*, Mando y Control)[19]	Contacto de los sistemas afectados con servidor de Mando y Control.
	Distribución de *malware* o configuración del mismo	Recurso usado para la distribución de *malware* o bien que aloje ficheros de configuración del mismo.
Information Gathering (Obtención de información)	Escaneo de Redes	Envío de peticiones a un sistema para descubrir información de la tecnología utilizada, servicios ofrecidos, así como de vulnerabilidades que puedan presentar
	Análisis/interceptación de paquetes (*Sniffing*)	Observación y registro del tráfico de red.
	Ingeniería Social	Obtención de información a través de engaño, bulos, etc.
Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema mediante la explotación de vulnerabilidades conocidas (habitualmente disponen de un identificador estandarizado denominado CVE[20]).
	Intento de acceso con vulneración de credenciales	Intento de acceso a través de ataques de fuerza bruta, ruptura de contraseñas, etc.
	Ataque desconocido	Ataque empleando un *exploit*[21] desconocido
Intrusión	Compromiso de cuenta con/sin privilegios	Compromiso de un sistema en el que atacante puede haber adquirido una cuenta con privilegios (Ej.: cuenta de Administrador) o sin ellos.
	Compromiso de aplicaciones	Compromiso de una aplicación a través de la explotación de vulnerabilidades de *software*. Ej.: inyección SQL, inyección remota de código, etc.
	Intrusión física	Por ejemplo, acceso no autorizado al Centro de Proceso de Datos (CPD).

1. Qué es un incidente de seguridad

Disponibilidad	Denegación de Servicio (DoS) o Denegación Distribuida de servicio (DDoS)	Ataque que afecta a la disponibilidad de los sistemas.
	Mala configuración	Una configuración incorrecta del *software* que pueda provocar una caída de un determinado servicio.
	Sabotaje	Sabotaje físico. Ej.: corte de cables, incendios provocados.
	Interrupciones	Perdida de disponibilidad por causas ajenas no intencionadas. Ej.: un desastre natural.
Compromiso de la información	Acceso no autorizado a la información	Ej.: robo de credenciales de acceso mediante interceptación de tráfico o el acceso a documentación en papel.
	Modificación no autorizada de información	Ej.: modificación por un atacante de una entrada en una base de datos.
	Pérdida de datos	Ej.: por fallo de disco duro o robo físico.

1. Qué es un incidente de seguridad

Fraude	Uso no autorizado de recursos	Uso de recursos corporativos para fines inadecuados.
	Derechos de autor	Ofrecimiento o instalación de *software* carente de licencia o protegido por derechos de autor.
	Suplantación de identidad	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos. Habitualmente se hace a través de técnicas de ingeniería social[22].
	Phishing	Suplantación de otra entidad a través del correo electrónico con la finalidad de convencer al usuario para que revele sus credenciales.
Por explotación de vulnerabilidades	Criptografía débil, servicios con acceso potencial no deseado, revelación de información, etc.	Servicios que presentan debilidades o malas configuraciones que ponen en riesgo la seguridad de los mismos haciéndolos susceptibles a ataques.
Ataques dirigidos	Amenazas Persistentes Avanzadas (APT) [3]	Ataques dirigidos, sofisticados, con tácticas de anonimato y persistencia avanzadas.
Otros	Otros	Cualquier tipo de incidente que no tenga cabida en ninguna categoría definida

1. Qué es un incidente de seguridad

Clasificación/Taxonomía de incidentes según la "Guía nacional de notificación y gestión de incidentes", y la "Guía de seguridad CCN-STIC 817" que toma como referencia las recomendaciones de ENISA.

En ocasiones, un mismo incidente puede encajar en varias de las categorías propuestas en la relación anterior. La organización deberá por tanto establecer un criterio homogéneo para la clasificación principal de incidentes de seguridad, con independencia de que de manera secundaria cada incidente se asocie a más categorías.

Es importante en este punto hablar de un criterio de referencia fundamental para la gestión de cada incidente, el nivel de Peligrosidad del mismo. Se define el **Nivel de Peligrosidad del incidente** como un indicador que determina la potencial amenaza que supondría un ataque exitoso. Este indicador dependerá de las propias características de la amenaza y su comportamiento. Habitualmente se determinan cinco niveles de peligrosidad que suelen venir asociados a un código de colores:

1. Qué es un incidente de seguridad

De acuerdo a la **Guía Nacional de notificación y gestión de ciber incidentes,** la correspondencia entre un incidente y su nivel de peligrosidad sería la siguiente:

- NIVEL DE PELIGROSIDAD CRÍTICO:
  - Amenazas Persistentes Avanzadas.
- NIVEL DE PELIGROSIDAD MUY ALTO:
  - Código dañino (Distribución Configuración de malware).
  - Intrusión (Robo de información).
  - Disponibilidad (Sabotaje, interrupciones).
- NIVEL DE PELIGROSIDAD ALTO:
  - Contenido abusivo (Pornografía infantil, contenido sexual o violento inadecuado).
  - Código dañino (Sistema infectado, Servidor de Mando y Control (C&C)).
  - Intrusión (Compromiso de aplicaciones o de cuentas con privilegios).
  - Intento de intrusión.

1. Qué es un incidente de seguridad

- Disponibilidad (Denegación de servicio (DoS), Denegación distribuido de servicio (DDoS).
- Compromiso de la información Acceso no autorizado a la información,
- modificación no autorizada de información, pérdida de datos).
- Fraude (Phishing).

- NIVEL DE PELIGROSIDAD MEDIO:
  - Contenido abusivo (Discurso de odio).
  - Obtención de información (Ingeniería social).
  - Intento de intrusión (Explotación de vulnerabilidades conocidas, intento de acceso con vulneración de credenciales).
  - Intrusión (Compromiso de cuentas sin privilegios).
  - Disponibilidad (Mala configuración).
  - Fraude (Uso no autorizado de recursos, derechos de autor, suplantación de identidad).
  - Explotación de vulnerabilidades (Criptografía débil, amplificador de ataques DDoS, servicios con acceso potencial no deseado, revelación de información, sistema vulnerable).

1. Qué es un incidente de seguridad

- NIVEL DE PELIGROSIDAD BAJO:
  - Contenido abusivo (Spam).
  - Obtención de información (Escaneo de redes, análisis de paquetes).
  - Otros.

Es importante también determinar el **nivel de impacto** asociado a un incidente, para ello se tienen en cuenta diferentes parámetros: impacto en la Seguridad Nacional o en la Seguridad Ciudadana, alteración en la prestación de un servicio esencial o en una infraestructura crítica, topología de la información o sistemas afectados, grado de afectación a las instalaciones de la organización, posible alteración en la prestación del servicio normal de la organización, tiempo y costes propios y ajenos hasta la recuperación post incidente, pérdidas económicas, daños reputacionales o extensión geográfica afectada.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto:

1. Qué es un incidente de seguridad

En la **Guía Nacional de notificación y gestión de ciber incidentes** se proporciona de forma orientativa los criterios considerados de determinación del nivel de impacto de los ciber incidentes. Algunos ejemplos:

- NIVEL DE IMPACTO CRÍTICO:
  - Afecta apreciablemente a la seguridad nacional o 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.
- NIVEL DE IMPACTO 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 sistemas clasificados RESERVADO.

1. Qué es un incidente de seguridad

  - Afecta a un servicio esencial.
  - Daños reputacionales elevados.
- NIVEL DE IMPACTO ALTO:
  - Afecta a más del 50% de los sistemas de la organización.
  - Extensión geográfica superior a tres CC.AA.
- NIVEL DE IMPACTO MEDIO:
  - Afecta a más del 20% de los sistemas de la organización.
  - El ciber incidente precisa para resolverse entre 1 y 5 Jornadas-Persona.

Son claros los beneficios de adoptar un sistema de clasificación. Por ejemplo, clasificar correctamente los incidentes permite a los equipos de respuesta asignar la prioridad adecuada a cada uno de ellos, asegurando que se tratan en primer lugar o que se asignan más recursos a aquellos casos más críticos (de acuerdo con su nivel de peligrosidad o impacto).

Un sistema de clasificación definido puede facilitarnos también aspectos como la elaboración de informes, la agregación y búsqueda de datos en los incidentes, o la alimentación de la plataforma de inteligencia de amenazas. Disponer de una

1. Qué es un incidente de seguridad

taxonomía permite además obtener indicadores más precisos sobre el tipo de incidentes que está sufriendo una organización, lo que podría ayudar al equipo de seguridad a identificar cuáles son las principales amenazas que dan lugar a ellos y adoptar medidas paliativas en su conjunto.