Guía

GESTIÓN DE CRISIS DE CIBERSEGURIDAD EN EMPRESAS

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

Índice

Índice de figuras

Índice de tablas

1. Instituto Nacional de Ciberseguridad

1.1. ¿Qué es INCIBE?

El **Instituto Nacional de Ciberseguridad (INCIBE)** es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional.

1.2. ¿Qué es INCIBE-CERT y cuáles son sus funciones?

INCIBE-CERT es uno de los equipos de respuesta de referencia ante incidentes que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública.

Como centro de respuesta a incidentes de seguridad para entidades y ciudadanos de derecho privado español, cuenta con las siguientes **funciones [1]**:

- **Ofrecer soporte técnico y proporcionar información** para ayudar a resolver los incidentes de ciberseguridad dentro de su ámbito de actuación. Se presta soporte en todas las fases de la gestión de incidentes: detección, prevención, protección, respuesta, mitigación y recuperación.
- **Hacer uso de técnicas de detección temprana de incidentes**, permitiendo notificar a los afectados para que se tomen las medidas oportunas.
- **Contactar con proveedores de Internet y otros CERT** (nacionales e internacionales), notificar el incidente para que tomen las medidas y limitar el evento e, incluso, impedir la continuidad del mismo.

Si deseas conocer más información acerca de los servicios ofrecidos por **INCIBE-CERT**, puedes visitar el **siguiente espacio [2].**

1.3. Operadores a los que asiste INCIBE-CERT

Tipos de **operadores** a los que asiste INCIBE-CERT:

Personas y entidades de derecho privado español incidencias@incibe-cert.es	Contacto CERT (no referido a incidentes) cert@incibe-cert.es	Proveedores de servicios digitales servicios@incibe-cert.es
Operadores de infraestructuras críticas pic@incibe-cert.es	Instituciones afiliadas a RedIRIS iris@incibe-cert.es	Entidades acreditadas para la asignación de CVEs cve-coordination@incibe.es

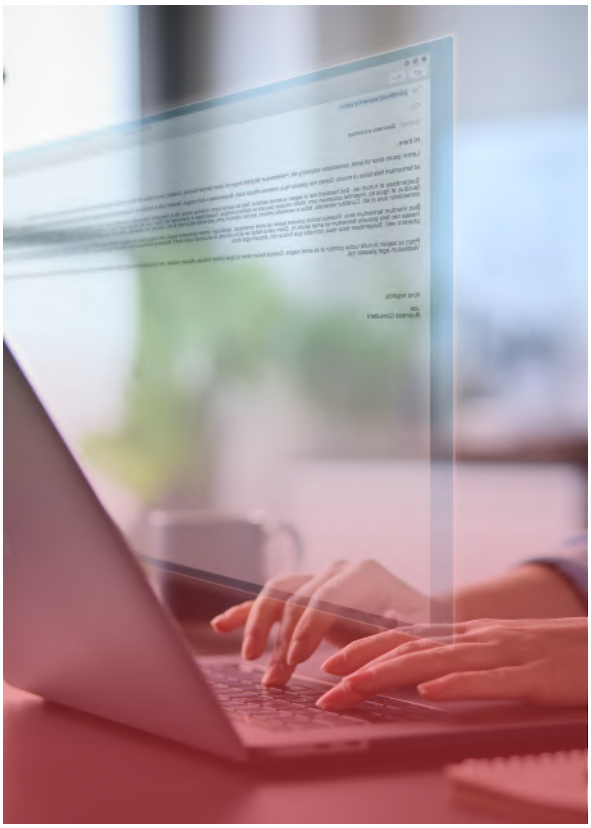
2. Introducción

2.1. Objetivo

El objetivo de esta guía de gestión de crisis de ciberseguridad es **proporcionar a las medianas empresas las herramientas y estrategias necesarias para procurar la seguridad y estabilidad** de sus operaciones frente a una crisis de ciberseguridad.

A través de este documento, se busca brindar un **plan detallado y efectivo** para prevenir, detectar y responder adecuadamente a posibles amenazas cibernéticas, minimizando así el impacto negativo en la empresa.

La guía servirá como un **recurso fundamental** para la toma de decisiones y la coordinación de acciones rápidas y eficaces en momentos de crisis, garantizando la continuidad de las operaciones y protegiendo la reputación de la empresa.



2.2. Alcance

El alcance de esta guía comprende a las empresas identificadas como medianas empresas, según lo definido en la **Recomendación 2003/361/CE**, ya que disponen de una serie de recursos que les pueden permitir aplicar adecuadamente las diferentes recomendaciones identificadas.

Categoría de empresa/efectivos y límites financieros	Número de personas empleadas	Volumen de negocios anual	Balance general anual
Microempresas	< 10	≤2 millones de euros	≤2 millones de euros
Pequeñas	< 50	≤10 millones de euros	≤10 millones de euros
Medianas	< 250	≤50 millones de euros	≤43 millones de euros
Grandes	> 250	≤50 millones de euros	≤43 millones de euros

Ilustración 1 - Tamaño de la empresa

2.3. Referencias normativas

En este apartado se identifican las normativas y los estándares de normalización que se han tenido en cuenta para elaborar esta guía y con las que está alineada.

Referencias normativas:

- **Reglamento de Ejecución (UE) 2018/151 de la Comisión, 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 para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo.
- **Ley Orgánica 3/2018 de 5 de diciembre**, de Protección de Datos Personales y Garantía de Derechos Digitales.
- **Ley 11/2022, de 28 de junio**, General de Telecomunicaciones.
- **Real Decreto-ley 12/2018, de 7 de septiembre,** de Seguridad de las Redes y Sistemas de Información.
- **Ley 34/2002, de 11 de julio**, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Estándares de normalización:

- **UNE-EN ISO/IEC 27001:2023** Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
- **UNE-EN ISO 22301:2020** Seguridad y resiliencia. Sistema de Gestión de la Continuidad del Negocio.

3. Definición de crisis de ciberseguridad

3.1. ¿Qué se considera crisis de ciberseguridad?

En primer lugar, conviene indicar la definición de qué es un **incidente de ciberseguridad**. Se puede definir como "Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa". Algunos ejemplos son: infección por *malware*, ataques de denegación de servicio o robo de datos.

Un incidente de ciberseguridad se convierte en una **crisis** cuando los daños ocasionados superan la capacidad de respuesta de la empresa afectada. Esto ocurre cuando los recursos y procedimientos habituales de la entidad no son suficientes para dar respuesta al incidente, provocando una escalada en la gravedad y el alcance del problema. Un incidente puede ser resuelto de forma estructurada en la empresa, mientras que una situación de crisis compromete gravemente la operación normal de la empresa.

Por lo general, una situación de crisis se dará con la ocurrencia de un incidente categorizado, según su peligrosidad y/o impacto, en **crítico, muy alto o alto** descrito en el **ANEXO II**.

Es esencial para las empresas estar preparadas para enfrentar ambos escenarios y contar con planes de acción adecuados para mitigar los riesgos y minimizar las consecuencias de ambas situaciones.

Las diferencias entre un incidente y una crisis incluyen la naturaleza del evento, el impacto, la duración y persistencia, así como la afectación en cuanto a reputación y confianza de la empresa. Mientras que un incidente puede manejarse internamente (por lo general, implicando únicamente al equipo de TI) y resolverse relativamente rápido, una crisis requiere, además de una respuesta técnica, una respuesta a nivel ejecutivo y organizativo, requiriendo la movilización de recursos adicionales y la toma de decisiones estratégicas para mitigar el impacto y recuperar la normalidad operativa. Recobrar la confianza perdida, en caso de no lograr una gestión adecuada de la crisis, puede requerir un esfuerzo considerable y prolongado.

Comprender las diferencias entre ambas situaciones permite a las empresas **implementar estrategias de respuesta adecuadas**, optimizar la gestión de recursos y minimizar el impacto.

3.2. Elementos claves de una crisis de ciberseguridad

A continuación, se presenta un conjunto de **elementos claves** que pueden indicar que una empresa se está enfrentando a una crisis de ciberseguridad:

- **Nivel crítico de peligrosidad e impacto:** como se ha mencionado anteriormente, el tipo de incidente está categorizado como crítico, muy alto o alto en cuanto a su criticidad e impacto.
- **Compromiso de la seguridad física:** el ataque resulta en un sabotaje a infraestructuras físicas, amenazando la vida de empleados y de la población.
- **Interrupción operativa extensa:** la empresa afectada experimenta una interrupción significativa en sus operaciones habituales, afectando a su capacidad para prestar servicios o realizar funciones básicas durante un prolongado periodo de tiempo.
- **Superación de capacidades de respuesta:** la capacidad de respuesta es insuficiente para responder ante el incidente, sobrecarga los recursos de la empresa para responder y recuperarse eficazmente, necesitando intervenciones externas o medidas de emergencia. En parte, esto puede ocurrir por tratarse de un evento inesperado.
- **Impacto financiero grave:** las pérdidas económicas derivadas son considerables, representando un alto coste de recuperación.
- **Daños reputacionales:** los efectos del incidente perjudican de manera significativa a la empresa en cuanto a la percepción pública. Puede darse una cobertura negativa en medios de comunicación y un posible impacto en el valor de las acciones de la empresa.
- **Implicaciones legales y regulatorias:** la empresa se enfrenta a importantes sanciones legales o regulatorias debido al incidente.

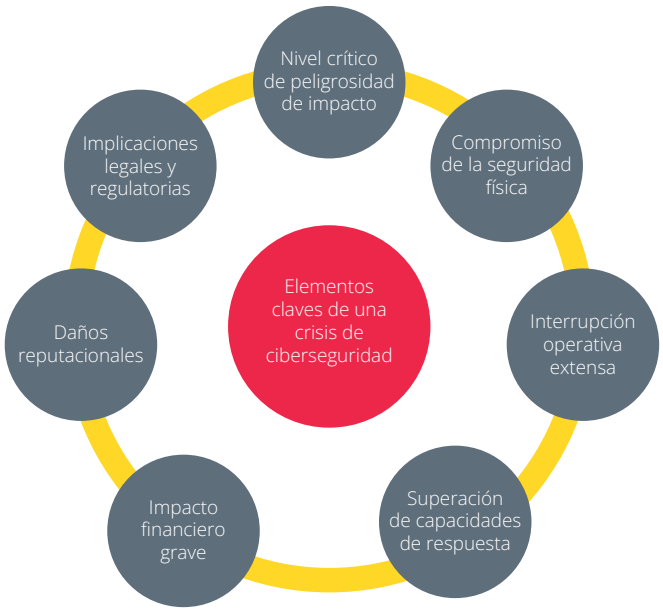


Ilustración 2 - Elementos claves de una crisis de ciberseguridad

3.3. Beneficios de contar con un plan de gestión de crisis de ciberseguridad

Como se ha mencionado, una crisis de ciberseguridad puede causar un gran impacto para las empresas, dañando su reputación y economía.

Por ello, es importante contar con un **plan de gestión de crisis de ciberseguridad** que proporcione la estrategia necesaria a las empresas para que sean capaces de resolver la situación lo antes posible y actuar de manera acorde al evento que se está produciendo.

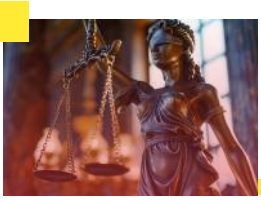
Un plan de gestión de crisis de ciberseguridad permitirá:

1. **Identificar y mitigar riesgos:** se pueden identificar posibles vulnerabilidades, amenazas y riesgos que pondrían a prueba la ciberseguridad de la empresa y que podrían provocar daños de gran importancia.

2. **Prevenir una posible crisis:** dentro del plan se establecen protocolos y procedimientos que ayudan a estar preparados ante una situación de crisis contando con una preparación adecuada que permita evitarla.

3. **Disminuir el impacto que puede causar un ciberataque:** el plan facilita las tareas a llevar a cabo ante este tipo de eventos, reduciendo el tiempo de respuesta y proporcionando información sobre los pasos a realizar para solucionar el problema a tiempo evitando la improvisación y la toma errónea de decisiones.

4. **Proteger la reputación de la empresa:** en caso de que se materialice una amenaza de estas características, contar con un plan correctamente definido y estructurado permitirá que los tiempos de respuesta disminuyan. Gracias a esta gestión, la confianza que terceros tienen en la empresa no se verá alterada.



5. **Cumplir con normativas y regulaciones:** disponer de un plan de gestión de crisis de ciberseguridad ayudará a cumplir con normativas y regulaciones existentes, evitando así posibles sanciones.

4. Buenas prácticas para la gestión de la crisis

Es imprescindible seguir una serie de buenas prácticas que engloban todas aquellas acciones y estrategias que una empresa implementa para **prevenir, manejar y resolver una crisis de manera efectiva**. Esto implica, entre otras cosas, disponer de políticas y procedimientos claros, contar con un equipo capacitado para enfrentar situaciones de emergencia, comunicarse de manera oportuna y efectiva con todas las partes involucradas y aprender de experiencias pasadas para mejorar la respuesta ante futuras crisis.

A continuación, se presentan algunas **buenas prácticas** para una adecuada gestión de crisis de ciberseguridad:

- **Determinar todas las acciones:** tener definidos todos los pasos a seguir en una crisis de ciberseguridad permitirá evitar la improvisación, clave cuando se requiere una rápida toma de decisiones.
- **Equipo de respuesta ante incidentes:** seleccionar a las personas con los conocimientos técnicos adecuados para gestionar la crisis en la empresa o contactar con un equipo especializado.
- **Coordinación:** asegurarse de una adecuada interacción, tanto con las diferentes áreas de la empresa como con las autoridades competentes a las que se debe reportar el incidente y cooperar hasta su resolución.
- **Comunicación transparente:** mantener una comunicación honesta con todo el público implicado en la crisis, tanto interno como externo. La transparencia ayuda a generar confianza y a evitar desinformación.
- **Gestión de la reputación:** durante una crisis, es importante proteger la reputación de la empresa, actuando de manera ética y responsable.
- **Aprendizaje continuo:** una vez finalizada la situación de crisis, es fundamental realizar una evaluación postcrisis para identificar fortalezas y áreas de mejora en el plan de gestión de crisis de ciberseguridad. Este aprendizaje debe ser continuo, lo que permitirá una mejor preparación para afrontar futuras crisis.

Ilustración 3 - Buenas prácticas en gestión de crisis

4.1. Fases de una crisis de ciberseguridad

Existen diferentes modelos que pueden reflejar las diferentes fases de las que se compone la **gestión de una crisis** (de manera similar a la gestión de un incidente de alto impacto), todos ellos estructurados de manera muy similar. A continuación, se indican las principales **fases en las que se puede dividir**:

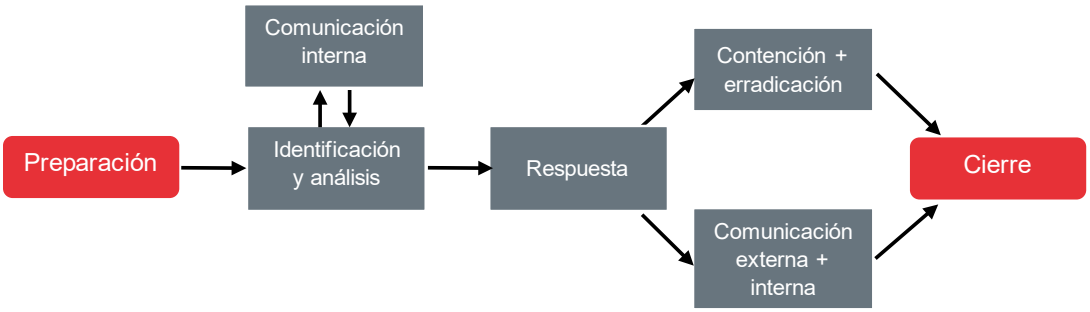


Ilustración 4 - Fases de una crisis de ciberseguridad

Dentro de cada una de las fases se lleva a cabo un conjunto de acciones. A modo de resumen, y con el fin de permitir una **visión global de la gestión de una crisis**, se describe a continuación cada una de ellas:

FASES	DESCRIPCIÓN Y ACCIONES
Fase 0: Preparación	En esta etapa se realizan planes y medidas preventivas para mitigar los posibles riesgos y daños que pueda ocasionar la crisis de ciberseguridad, antes de que esta suceda. Esto incluye la definición de roles y responsabilidades, gestión de stakeholders, definición de planes de continuidad de negocio y planes de recuperación ante desastres, realización de inventariado de activos y análisis de riesgos y ejecución de simulacros.
Fase 1: Identificación y análisis	Una vez identificado un incidente, deberá de ser notificado internamente y, además, deberá llevarse a cabo un análisis que permita determinar si cumple con los requisitos para tratar la situación como una crisis. En caso afirmativo, deberá convocarse el Comité de Crisis.
Fase 2: Respuesta y comunicación	Con la información recopilada, el Comité de Crisis tomará la decisión de activar el plan de gestión de crisis de ciberseguridad, en caso de que cumpla con los criterios previamente definidos. En este momento, se determinarán las primeras acciones de contención que permitan minimizar el impacto para, posteriormente, erradicar el incidente y recuperar los sistemas afectados. Mientras se llevan a cabo estas acciones, se debe mantener en todo momento una comunicación clara y transparente con todos los stakeholders identificados.
Fase 3: Cierre	Una vez que la crisis ha sido controlada y resuelta, el comité tomará la decisión de desactivar la situación de crisis. En este punto es importante analizar lo sucedido, identificar las áreas de mejora y extraer lecciones que puedan ser aplicadas en el futuro, mejorando la respuesta ante futuras crisis.

Tabla 1 - Breve descripción de las fases de una crisis

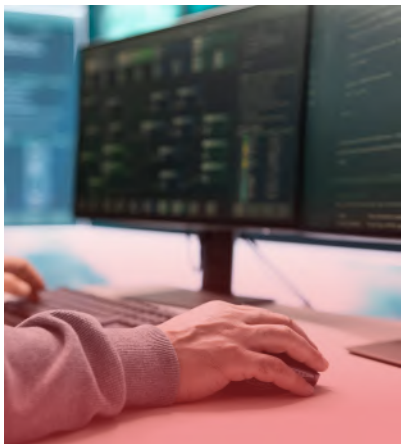
4.2. Preparación

La **fase de preparación en una crisis de ciberseguridad** es fundamental para asegurar una respuesta eficaz y eficiente cuando esta suceda. Esta etapa se desarrolla en momentos de calma, es decir, cuando la actividad de la empresa no ha sufrido ninguna interrupción. Durante esta etapa, se llevan a cabo diversas **acciones** que permitirán una preparación adecuada ante posibles incidentes de ciberseguridad que puedan desencadenar una crisis, y así conseguir una reacción adecuada en tiempo y forma cuando se materialice una amenaza de estas características.

Las **acciones principales** que se realizan en esta fase son:

- **Definir roles y responsabilidades:** crear un Comité de Crisis que involucre al personal necesario para una gestión adecuada de la misma. Cada uno tendrá roles y responsabilidades específicas para garantizar una respuesta efectiva y coordinada.
- **Gestión efectiva de los *stakeholders*:** gestionar de forma adecuada la comunicación y relación con todas las partes interesadas, tanto internas como externas. Es crucial para mantener de manera exitosa la reputación y confianza en la empresa.
- **Identificación de activos críticos:** identificar los activos de información y sistemas críticos de la empresa para priorizar su protección en caso de ciberataques.
- **Evaluación de riesgos:** realizar evaluaciones periódicas de riesgos para identificar posibles vulnerabilidades y amenazas que puedan afectar la seguridad de la información.
- **Desarrollo de un plan de continuidad de negocio (PCN):** crear y mantener actualizado un plan de continuidad de negocio, que contenga el conjunto de planes de actuación, necesarios para minimizar impacto provocado por la crisis.
- **Desarrollo de un plan de recuperación ante desastres (DRP):** crear y mantener actualizado un DRP que abarque los procesos de restauración de los datos, el *hardware* y el *software* que dan soporta a procesos críticos de la empresa ante un desastre.
- **Realización de simulacros:** probar la efectividad de las medidas identificadas. Deben desarrollarse diferentes tipos de simulacros de forma anual.

4.2.1. Principales actores en la gestión de la crisis



Para la resolución de una crisis, es fundamental la participación de diversos equipos y personas con diferentes capacidades. El personal involucrado, además de los conocimientos y la experiencia necesarios, deberá contar con competencias tales como capacidad de respuesta, de comprensión y habilidades comunicativas, entre otras.

La resolución a nivel técnico del incidente la llevará a cabo el **equipo de respuesta a incidentes** de la empresa o, en su defecto, el Departamento de Sistemas si el primero no existiese.

Serán los encargados de identificar y contener el incidente, principalmente. Para incidentes habituales y de baja criticidad, será habitualmente el único departamento involucrado. Deberán proporcionar una respuesta rápida, coordinada y efectiva.

Por otro lado, la planificación a nivel estratégico será realizada por el **Comité de Crisis**, uno de los principales actores identificados en la gestión de crisis de ciberseguridad.

4.2.1.1. Comité de Crisis

El **Comité de Crisis** es el órgano responsable de coordinar y gestionar la respuesta ante una crisis de ciberseguridad. Este comité está compuesto por diversos miembros, cuyas funciones y responsabilidades varían según los diferentes roles que forman parte del mismo. Entre las principales **funciones** del comité se incluyen:

- Evaluar y determinar el alcance y gravedad del incidente para definir las acciones a realizar.
- Analizar la información sobre el incidente.
- Definir los mensajes que se van a transmitir a las partes interesadas.
- Informar a las partes interesadas de la activación del plan de gestión de crisis.
- Realizar reuniones de seguimiento para actualizar la información de la situación.

Respecto a los miembros del **Comité de Crisis**, deberá existir una lista de candidatos, haciendo distinción entre los principales y los suplentes, para así poder cubrir cualquier necesidad. Se identifican los siguientes **roles/departamentos que componen el Comité de Crisis**:

Ilustración 5 - Comité de Crisis

Dependiendo del tipo de crisis de ciberseguridad, la constitución del Comité de Crisis puede variar, pudiendo requerir la participación de un responsable o técnico de cualquier área.

Además, es recomendable designar un rol encargado de la **coordinación de gestión de la crisis**, que se encargará principalmente de brindar apoyo en todo el proceso de respuesta ante el incidente de ciberseguridad. Sus principales **funciones** son:

- **Velar** por el cumplimiento de las acciones a realizar por cada departamento/rol.
  - Es aconsejable disponer de una ***checklist*** para asegurar que se completan todas las acciones definidas en el procedimiento.
- **Recopilar** la información y documentación necesaria de las reuniones del Comité de Crisis.
- **Dar apoyo** a los diferentes departamentos en caso de duda.

4.2.1.2. Funciones de los miembros del Comité de Crisis

Los diferentes roles/departamentos que forman parte del Comité de Crisis tendrán, principalmente, las siguientes **funciones**:

ROLES	RESUMEN DE FUNCIONES
Presidencia o Dirección General	▸ **Ostentar** la representación del Comité de Crisis. ▸ **Impulsar** la ejecución de los acuerdos adoptados en las reuniones del Comité de Crisis.
CISO/ representante de Sistemas de información	▸ **Reforzar** las medidas de seguridad en caso de que sea necesario. ▸ **Velar** por la disponibilidad e integridad de los servicios TI.
RRHH	▸ **Analizar** los recursos humanos asignados para la gestión de la crisis.
Servicios Jurídicos	▸ **Analizar** las implicaciones jurídicas sobre las acciones a desarrollar. ▸ **Elaborar** el acta de las reuniones realizadas por el Comité de Crisis.
Comunicación	▸ **Elaborar y difundir** los oportunos mensajes en redes sociales o página web. ▸ **Atender** a los medios de comunicación. ▸ **Monitorizar** redes sociales.

Tabla 2 - Funciones de los miembros del Comité de Crisis

4.2.2. Gestión efectiva de *stakeholders*

> Los ***stakeholders*** son todas las personas, grupos u organizaciones que tienen interés o están involucrados de alguna manera en la empresa y que pueden verse afectadas por las decisiones o acciones de dicha entidad.

Tienen el poder de **influir en el éxito o en el fracaso de la entidad**, por lo que es esencial gestionar sus expectativas y mantener una comunicación abierta y transparente con ellos.

En el caso de ocurrencia de una crisis de ciberseguridad en la empresa, los ***stakeholders*** que están relacionados con la empresa pueden resultar directamente afectados por las consecuencias.

En este sentido, una crisis de este tipo podría afectar a todos los que rodean a la empresa, es decir, a sus trabajadores, a sus socios, proveedores, competidores y, por supuesto, a sus clientes.

Por ejemplo, **los clientes podrían ver comprometida la seguridad de su información personal y financiera**, lo que podría causar una pérdida de confianza en la empresa y un daño a su reputación. Los empleados también podrían verse afectados, ya que la crisis de ciberseguridad podría poner en riesgo su seguridad laboral, su privacidad y su capacidad para desempeñar sus funciones de manera eficiente.

Es por ello que se recomienda elaborar un **mapa de *stakeholders*** o una **matriz de influencia** con los grupos de interés que rodean a la empresa y puedan verse afectados por la crisis. Esto permitirá que la documentación que tengamos que utilizar en una situación de crisis refleje fielmente la información de los distintos actores involucrados.

Dependiendo del incidente o evento que provoque la crisis de ciberseguridad, será necesario **analizar con detalle a todos los involucrados**, sus expectativas y las acciones a implementar con cada uno de ellos.

A continuación, se identifican los diferentes **grupos de interés** que puede tener una empresa:

GRUPOS DE INTERÉS		
Internos	**Externos**	
▸ Propietarios o accionistas ▸ Directivos y gerentes ▸ Empleados y familiares ▸ Representaciones de los trabajadores ▸ Comités y grupos de interés internos	▸ Administración pública ▸ Clientes ▸ Proveedores ▸ Competidores ▸ Autoridad competente	▸ Agencia Española de Protección de datos ▸ CERT o CSIRT ▸ Inversores ▸ Aseguradoras ▸ Medios de comunicación

Tabla 3 - Grupos de interés de una empresa

4.2.3. Inventario de activos y análisis de riesgos

Cuando hablamos de **gestión de crisis de ciberseguridad o de continuidad de negocio**, las prioridades de una empresa tienen que ir dirigidas a que esté lo mejor preparada posible para proteger sus activos.

Por ello, el **activo** de una empresa hace referencia a todo lo que tenga valor para la empresa e influya en su actividad comercial o laboral, como los procesos de negocio, la información, los equipos informáticos, las personas, las infraestructuras, los programas informáticos, etc., y cuyo deterioro suponga un agravio o coste para la empresa.

Resulta necesario considerar qué activos son susceptibles de verse afectados por una crisis de ciberseguridad o una interrupción de su actividad en caso de que esta suceda. La naturaleza de cada activo dependerá de la empresa, pero su **protección** es el fin último de la gestión de riesgos.

El **inventario de activos** **[4]** conforma el primer elemento de la cadena en un sistema de gestión de la seguridad y se define como una lista de todos aquellos recursos (*hardware*, *software*, documentos, servicios, personas...) que tengan valor y necesiten ser protegidos de potenciales riesgos. No se puede proteger lo que no se conoce; por eso, es muy importante disponer de un inventario de activos convenientemente actualizado y revisado.

Para facilitar el manejo y mantenimiento del inventario, es conveniente clasificar los activos por categorías, según su **naturaleza**:

- Datos
- Aplicaciones
- *Hardware* industrial
- Red
- Tecnología
- Personal
- Instalaciones
- Equipamiento auxiliar
- Proveedores

A continuación, se presentan los **pasos** necesarios para llevar a cabo un correcto inventariado de activos:

1. **Definir** el alcance del inventario, incluyendo todos los activos que tengan un valor importante para la empresa.

2. **Crear** una lista de activos con la información detallada de cada uno de ellos, incluyendo, al menos, el nombre (modelo, marca...), descripción, número de identificación único, tipo o grupo, propietario, responsable, ubicación y estado.

3. **Determinar** el valor de los activos, de manera que permita evaluar su impacto en el sistema. Para ello, se pueden tener en cuenta factores como la disponibilidad, integridad, confidencialidad, criticidad y su coste.

4. **Registrar** esta información en la lista de activos. Deberá ser actualizada de manera periódica (o cuando alguno de los activos sufra un cambio) para alinear toda esa información con la realidad de la empresa.

Para facilitar este proceso, se recomienda utilizar **herramientas de gestión de activos**, como *software* de inventario, escáneres de códigos de barras o dispositivos móviles que facilitan la tarea de identificar y documentar todo el *hardware* y *software* residente en una red. Sin embargo, es recomendable realizar una evaluación previa de la herramienta en entornos fuera de producción para garantizar que su funcionamiento no altera el sistema a inventariar.

Por otro lado, la valoración de los activos es importante para la evaluación de la magnitud del **riesgo [5]**. El riesgo mide tanto la probabilidad como las consecuencias de eventos (no deseables) futuros e inciertos. Por tanto, el nivel de riesgo es una estimación de lo que puede ocurrir y se valora de forma cuantitativa, como el producto del impacto (consecuencia) asociado a una amenaza (suceso), por la probabilidad de ocurrencia de la misma.

Impacto xProbabilidad =RIESGO

Ilustración 6 - Cálculo del riesgo

El impacto, y por tanto el riesgo, se valoran en términos del coste derivado del valor de los activos afectados, considerando, además, los daños producidos en el propio activo. Este análisis permite a las empresas establecer el **"apetito al riesgo"**, es decir, el nivel máximo de riesgo que la empresa está dispuesta a soportar, debiendo mantener la gestión de los riesgos por debajo de este umbral. Este concepto responde a 2 factores concretos: la capacidad objetiva de la empresa para "aceptar" pérdidas y la predisposición para asumir riesgos.

Las actividades, cuyo objetivo es mantener el riesgo por debajo del umbral fijado, se engloban en lo que se denomina gestión del riesgo. Para lograrlo, las empresas deberán realizar un análisis de riesgos y un tratamiento de los riesgos.

Para el **análisis de riesgos** y dependiendo de las necesidades, calidad de los datos y tiempo disponible las empresas pueden optar por realizar un **análisis cualitativo** (estimando el impacto y la frecuencia de los eventos, siendo este más subjetivo, menos complejo y de menor coste) **o cuantitativo** (usando datos y estadísticas y siendo este método más objetivo, complejo y de mayor coste económico).

Para el tratamiento de riesgos, las empresas pueden optar por las siguientes **estrategias**:

- **Evitar o eliminar el riesgo**, sustituyendo el activo por otro que no se vea afectado o eliminando la actividad que lo produce.
- **Reducirlo o mitigarlo** para que el nivel de riesgo se sitúe por debajo del umbral establecido.
- **Transferirlo, compartirlo o asignarlo a terceros [6]**, por ejemplo, suscri-biendo un contrato de seguros.
- **Aceptarlo**, es decir, asumir el riesgo, bien porque está por debajo del umbral acep-table o, aun siendo riesgos de impacto alto, su probabilidad de ocurrencia es baja. Otra posibilidad en la que se contemplaría la aceptación de un riesgo es que, por necesidades de negocio, se deba continuar con la operación habitual del activo a pesar de tener un riesgo inaceptable.

Los responsables que forman parte de la **toma de decisión** sobre los tratamientos de los riesgos deben estar siempre bien identificados. Adicionalmente, para los casos en los que la acción de tratamiento sea mitigar, es importante definir la estrategia a llevar a cabo para reducir el nivel de riesgo y quién será el encargado de realizar tal acción. Es recomendable llevar un **seguimiento activo de estas acciones** a través de un plan de tratamiento de riesgos (PTR) para asegurar que se llevan a cabo de forma correcta.

El **análisis de riesgos** es aquel proceso sistemático de recopilación, registro y evaluación de la información de la empresa y su entorno que conduce a recomendaciones sobre una decisión en respuesta a un tipo de riesgo. Este consiste en averiguar el nivel de riesgo que la empresa está soportando mediante la determinación de las amenazas a las que se enfrenta, la probabilidad de que se materialicen y los posibles impactos sobre los activos. Es una actividad que se debe realizar de forma recurrente con una periodicidad mínima definida por la empresa, así como en los casos en los que se produzcan cambios significativos.

Debe ser realizado de forma metódica impidiendo omisiones, improvisaciones o posibles criterios arbitrarios. En la actualidad existen diversas **metodologías y guías de buenas prácticas** que pueden ser utilizadas para realizar este análisis. Este es un conjunto de las principales metodologías de análisis de riesgos utilizadas:

METODOLOGÍAS DE ANÁLISIS DE RIESGOS	
MAGERIT v3	MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.
ISO 27005:2022	Norma que aporta directrices para la gestión de riesgos de seguridad de la información.
ISO 31000:2018	Norma global, no certificable, que aporta metodología, principios y directrices en materia de gestión de riesgos.
NIST SP800-30	Metodología creada por el Gobierno norteamericano.

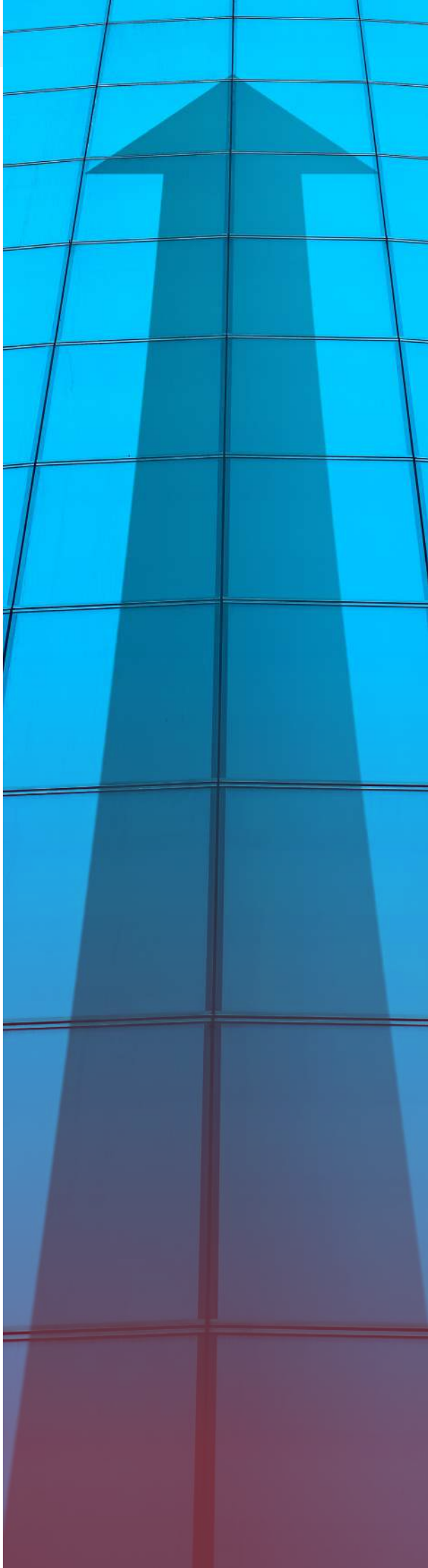
Tabla 4 - Metodologías de análisis de riesgos

4.2.4. Plan de continuidad de negocio

Una **crisis de ciberseguridad** puede tener un impacto devastador en la continuidad de negocio de una empresa, paralizando sus operaciones, dando lugar a pérdidas financieras significativas, así como dañar la reputación de la empresa y afectar a la confianza de los clientes.

Las empresas deben estar preparadas para **prevenir, protegerse y reaccionar ante un incidente de seguridad** que pueda afectarles y que podrían impactar en sus negocios, especialmente si se trata de un incidente crítico que pueda desencadenar una situación de crisis.

Es por ello que resulta fundamental que las empresas protejan sus principales **procesos de negocio**, inviertan en medidas de seguridad robustas y estén preparadas para responder y recuperarse de manera efectiva ante un incidente de este tipo.



Independientemente del tamaño de la empresa, todas las empresas deberían contar con un **plan de continuidad de negocio** y un **plan de recuperación ante desastres**, permitiendo minimizar el impacto ante una posible crisis y asegurar una rápida recuperación **[7]**.

Por otro lado, un **plan de contingencia**, además, permitirá gestionar de manera eficiente cualquier crisis inesperada, minimizando los tiempos de recuperación y garantizando una rápida vuelta a la normalidad, por lo que deberá estar en constante actualización, verificando su vigencia de forma regular.

Es importante tener en cuenta que el **plan de continuidad de negocio** no puede realizarse sin haberse llevado a cabo con anterioridad el correspondiente análisis de riesgos. Esto se debe a que, si se desconocen las posibles amenazas y/o eventos no deseados que puedan suceder en una empresa, es complicado desarrollar un plan que ayude a responder de manera rápida ante un incidente.

En este sentido, es importante tener presente el concepto de **BIA** (en inglés, *Business Impact Analysis*), que se encarga de **analizar los procesos del negocio de la empresa** para poder conocer el impacto que se produciría en caso de que ocurriera un incidente que causase la interrupción de dichos procesos y en base a esto poder priorizar la recuperación de unos procesos frente a otros.

Así pues, estos planes o ámbitos son inclusivos:

Ilustración 7 - Conjunto de planes necesarios en una empresa para asegurar la continuidad

Las fases que implica el plan de continuidad de negocio se pueden resumir en:

Fase 0: determinación del alcance

El alcance habitual son aquellos sistemas o procesos de mayor criticidad y, por tanto, los que en caso de pérdida impactarían más sobre la empresa. Lo habitual es que un plan de recuperación ante desastres esté enfocado al ámbito más técnico (es un plan reactivo ante una posible catástrofe que contempla todos los pasos para recuperar un activo), mientras que el plan de continuidad TIC tendrá un enfoque mayor en los procesos de la empresa.

Fase 1: Análisis de la empresa

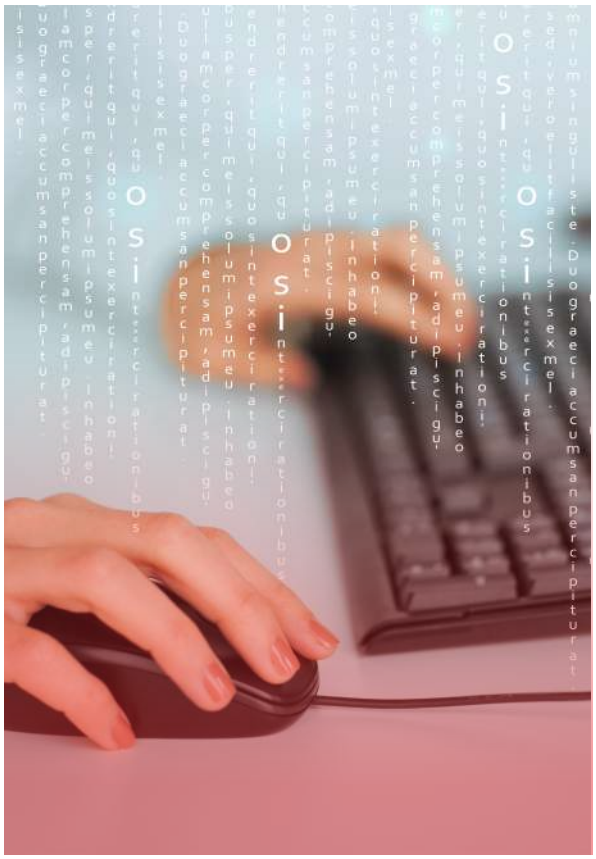
Esta fase conlleva la obtención, elaboración y comprensión de las circunstancias, tecnologías, procesos y recursos de la empresa.

La primera tarea a realizar es **mantener reuniones con el personal implicado** en los procesos seleccionados en el alcance para tener una visión general de los procesos de los que queremos mejorar la continuidad y determinar quiénes serían los responsables de los mismos. Se identificarán las dependencias de personal, proveedores, aplicaciones y necesidades temporales de dichos procesos.

Posteriormente, se elabora el **análisis de impacto sobre el negocio (BIA)**, desde el punto de vista del negocio, que contiene todas las necesidades de los procesos que se han definido en el alcance, pudiendo así clasificarlos según su criticidad y dependencia:

- **RTO:** tiempo de recuperación objetivo.
- **MTD:** tiempo máximo tolerable de caída.
- **RPO:** grado de dependencia de la actualidad de los datos (punto de recuperación objetivo).
- **ROL:** niveles mínimos de recuperación del servicio.
- **Recursos humanos y tecnológicos** empleados en el proceso.
- **Dependencias de otros procesos** internos o proveedores externos.

Este documento, junto al análisis de riesgos, define las **iniciativas** a implantar para recuperar los procesos en situación de contingencia.



En cuanto al **análisis de riesgos**, se deberán determinar las amenazas a las que está expuesta la empresa, sobre todo las que impliquen una indisponibilidad de los procesos del alcance. Una vez tengamos el listado de amenazas, se determinará la probabilidad y el impacto de cada una de ellas. En este caso, es conveniente **priorizar** aquellas que impliquen un mayor impacto. Por último, se obtendrá el producto de la probabilidad por el impacto de cada amenaza, que servirá para detectar los riesgos que se deben tratar con mayor prioridad.

El **tratamiento de estos riesgos** se detalla en el apartando siguiente.

Fase 2: Determinación de la estrategia de continuidad

A partir de la información recopilada, podremos determinar cuál es la diferencia entre las necesidades de los procesos de negocio incluidos en el alcance y las capacidades de los recursos que utilizan. De este modo, identificaremos si los recursos actuales y sus estrategias de recuperación permitirían no exceder el MTD establecido para cada proceso. En esta fase se deben **determinar las estrategias de recuperación** más adecuadas para cada caso e implementarlas en una fase posterior, valorando para cada una de ellas el coste y viabilidad de su implantación, mantenimiento, recursos necesarios, etc.

Fase 3: Respuesta a la contingencia

Este proceso comienza con la **implantación de las estrategias de recuperación i**dentificadas en la anterior fase y le seguirá una fase de clasificación y priorización de medidas, en función del proceso afectado por su implantación y la criticidad del mismo. Se deberá desarrollar toda la documentación necesaria para la respuesta ante una contingencia.

Fase 4: prueba, mantenimiento y revisión

En esta fase de realizarán pruebas de diferente complejidad sobre los entornos que se hayan definido en el alcance. Entre ellas, se deberán realizar **pruebas de todos los entornos al menos una vez al año** para cubrir el conjunto de amenazas que se hayan definido como potencialmente catastróficas.

Es necesario llevar a cabo una planificación que tenga en cuenta al personal técnico implicado, el usuario del aplicativo implicado, el personal externo, la descripción de la prueba a realizar, la descripción del resultado esperado tras su ejecución y la hora y fecha de realización. La planificación de los distintos tipos de pruebas y los detalles de las mismas será recogida en el **plan de pruebas**. Tras la prueba, deberá elaborarse un **informe** que recoja los resultados y describa las posibles incidencias surgidas para aplicar las medidas correctoras que sean necesarias.

También es importante determinar si la prueba se ha podido realizar sin exceder los tiempos marcados en el plan de continuidad para, en caso contrario, analizar si la prueba se ha realizado correctamente o si la estrategia seleccionada es la adecuada.

En cuanto al **plan de mantenimiento**, el propósito es definir la necesidad de actualizar toda la documentación tanto de forma periódica como cuando se produzcan cambios significativos, lo que permitirá que la documentación que se necesite en una situación de crisis refleje fielmente la información de los distintos actores involucrados en los procesos.

Fase 5: Concienciación

Como última fase de la implantación del plan de continuidad de negocio, se deben llevar a cabo aquellas tareas que **incrementen la concienciación del personal** en relación con la continuidad, debiendo realizarse tanto en el personal implicado como en los procesos de negocio, personal TI, etc.

En concreto, se debe plantear un proceso de concienciación que contemple la descripción de los elementos utilizados en la continuidad (análisis de impacto sobre el negocio, plan de crisis, estrategias de recuperación, etc.).

Por último, resulta conveniente realizar **resúmenes del plan de continuidad** que recojan las funciones prioritarias, los componentes del equipo de gestión de crisis y el personal crítico/operacional, ya que, por lo general, los planes de continuidad de negocio son demasiado extensos y esto puede ser clave para llevarlos a cabo correctamente mediante el uso de un esquema general que ayude a desarrollar las fases descritas anteriormente.

4.2.5. Plan de recuperación ante desastres (DRP)

El **plan de recuperación ante desastres (DRP)** es un conjunto de procesos diseñados para restablecer los sistemas y la infraestructura de una empresa después de un incidente grave o desastre. Como se ha mencionado en el apartado anterior, este plan debe de incluirse dentro del **plan de continuidad de negocio (PCN)** [8].

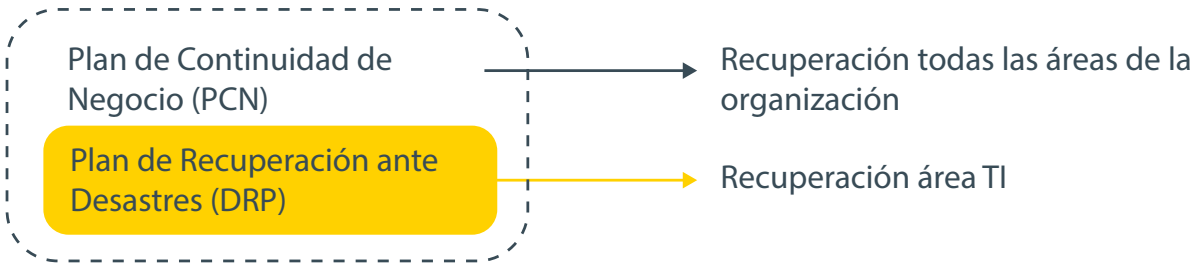


Ilustración 8 - PCN y DRP

DIFERENCIAS	
PCN	▸ Se focaliza en evitar las interrupciones en todos los sistemas de la empresa. ▸ Tiene como objetivo garantizar la continuidad de la actividad de la empresa.
DRP	▸ Se centra exclusivamente en recuperar los sistemas de información e infraestructura ▸ Tiene como objetivo garantizar la seguridad de la parte TIC. ▸ Complementa al PCN para mantener la normalidad de las operaciones de la empresa.

Tabla 5 - Diferencias entre PCN y DRP

Un DRP debe contar con los siguientes **elementos**:

- **Identificación de riesgos y evaluación de impacto:** análisis y evaluación tanto de las amenazas como las necesidades de la empresa.
- **Procedimientos de respaldo y recuperación de datos:** definición de protocolos y procesos de recuperación.
- **Infraestructura de recuperación:** establecimiento de alternativas tales como documentación y procesos de mantenimiento para la restauración de la actividad (servidores de respaldo, conexiones de red alternativas, etc.).
- **Roles y responsabilidades:** definición y asignación de roles específicos.
- **Procedimientos de comunicación:** establecimiento de canales de comunicación efectivos para informar a las partes interesadas.
- **Pruebas y entrenamiento:** realización de pruebas periódicas del DRP para asegurar la efectividad del mismo.
- **Actualización y revisión del plan:** mantenimiento del DRP actualizado y revisarlo regularmente para garantizar su eficacia.

Las **ventajas** de elaborar y disponer de un DRP son, entre otras:

- **Garantizar el respaldo** de la información y los activos de la empresa.
- **Reducir** los tiempos de recuperación ante el desastre, logrando así un menor impacto en la empresa.
- **Evitar** sanciones o multas por incumplimiento normativo.
- **Asegurar** la continuidad del negocio.
- **Mejorar** la reputación de la empresa.

Un DPR puede abarcar diferentes tipologías de escenarios de desastre y, asimismo, diferentes estrategias de recuperación:

ESCENARIOS	EJEMPLO	ESTRATEGIAS	EJEMPLO
Indisponibilidad de tecnológica y datos	▸ Fallo de comunicaciones. ▸ Ciberataques.	**Tecnología**	▸ Plan de contingencia informática.
Indisponibilidad de recursos humanos	▸ Huelgas. ▸ Epidemias. ▸ Pandemias.	**Recursos Humanos**	▸ Procedimientos operativos. ▸ Formación cruzada.
Indisponibilidad de proveedores	▸ Fallo de suministro eléctrico. ▸ Fallo de las comunicaciones.	**Proveedores**	▸ Diversificación de proveedores.

Para garantizar el respaldo de la información, se pueden seguir diferentes estrategias, que se ordenan en función del coste y de la complejidad:

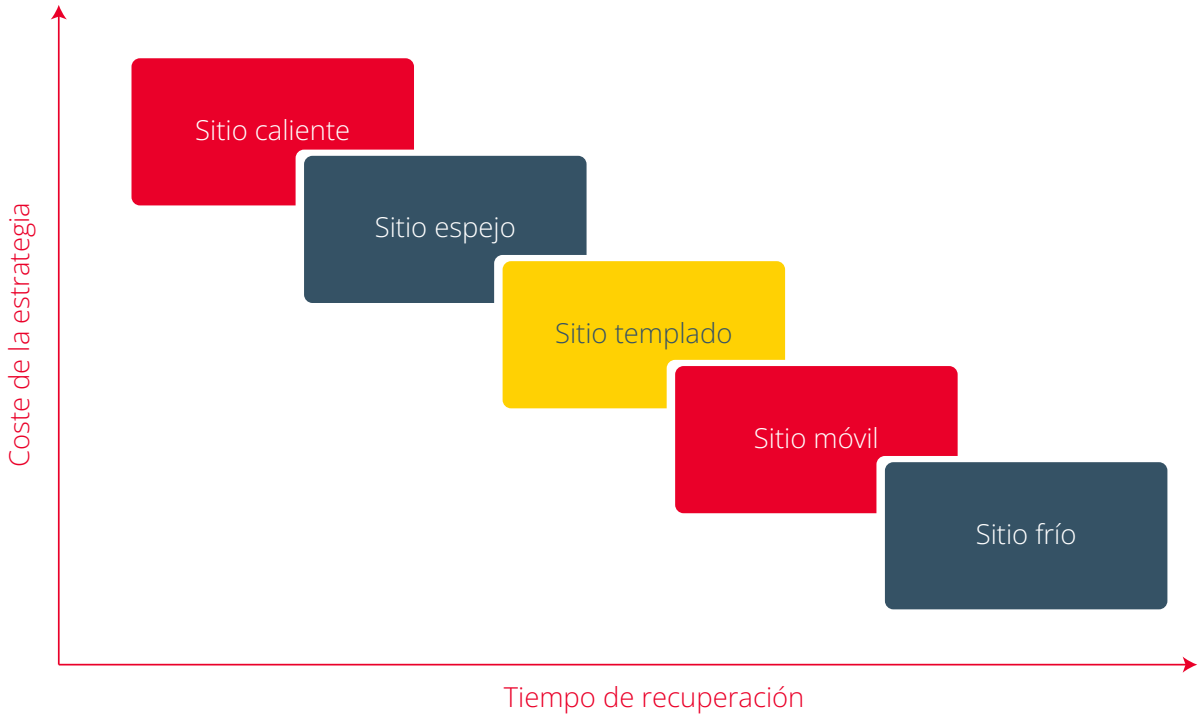


Ilustración 9 - Modelo de recuperación

MODELOS DE RECUPERACIÓN	DESCRIPCIÓN	VENTAJAS	INCONVENIENTES
Sitio frío	▸ Dispone de una infraestructura mínima. ▸ Enfocado a empresas con poca criticidad. ▸ No cuenta con *hardware*, *software*, datos y personal.	▸ Tiene un coste reducido. ▸ Es un modelo fácil de implementar. ▸ Ofrece una protección financiera de los activos físicos.	▸ Puede afectar a la rapidez de la recuperación, dependiendo de la complejidad de la tecnología utilizada. ▸ A diferencia del resto de modelos, es el que menos sensación de seguridad proporciona.
Sitio móvil	▸ Dispone de autocontenido y es reubicable. Cuenta con infraestructura IT y comunicaciones. ▸ Se trata de una alternativa útil cuando no hay instalaciones de recuperación en el área geográfica.	▸ Tiene un coste bajo. ▸ Es rápido de implementar y tiene un mantenimiento sencillo. ▸ Es un modelo que proporciona flexibilidad.	▸ La capacidad de los equipos puede ser insuficiente. ▸ No dispone de datos y en algunos casos tampoco dispone de personal.
Sitio templado	▸ Dispone de una mayor infraestructura (ordenadores personales, servidores y equipo de comunicaciones). ▸ Enfocado a empresas con baja o media criticidad. ▸ Las estaciones de trabajo están disponibles, pero el *software* puede no estar instalado.	▸ Tiene un coste menor al sitio caliente. ▸ Tiene una ubicación más ventajosa, ya que requiere de menos control, puesto que los sitios pueden ser más flexibles.	▸ No tiene test anual (sin simulacro). ▸ No cuenta con datos, personal, *hardware* o software específicos. ▸ El proveedor de servicios puede sobrevalorar las capacidades del procesamiento.
Sitio espejo	▸ Cuenta con una infraestructura idéntica en equipamiento y datos. ▸ Cada cierto tiempo se realiza un test con datos reales. ▸ Enfocado a empresas con alta criticidad.	▸ Tiene una disponibilidad 24/7 y exclusividad de uso.	▸ Tiene un coste muy elevado. ▸ Requiere de un constante mantenimiento de *hardware*, *software*, datos y aplicaciones. ▸ No cuenta con personal.
Sitio caliente	▸ Cuenta con toda la infraestructura salvo equipos y *software* muy específico o propietario. ▸ Enfocado a empresas con una alta criticidad. ▸ Las estaciones de trabajo y servidores están actualizados.	▸ Tiene una disponibilidad 24/7 y exclusividad de uso. ▸ Es un modelo que admite interrupciones de corto y largo plazo. ▸ Dispone de test anual (simulacro).	▸ Tiene un coste alto. ▸ Este modelo necesita un constante mantenimiento de *hardware*, *software*, datos y aplicaciones. ▸ Requiere que la seguridad se duplique.

Tabla 6 - Modelos de recuperación

En términos generales, un DRP se puede dividir en las siguientes **fases**:

- **Fase 1: detección y gestión del desastre.** Se detecta el desastre y se avisa a los responsables, notificándoles la contingencia. Se evalúan los daños ocasionados y se registra la incidencia.
- **Fase 2: activación del modelo de desastre.** Se activa el modelo de recuperación seleccionado por la organización (sitio frío, caliente, etc.).
- **Fase 3: recuperación de funciones críticas.** Se procede a la restauración del software y de los datos del sistema operativo.
- **Fase 4: recuperación de operaciones.** Se ejecuta la reconstrucción del Centro de Protección de Datos y la recuperación de los equipos informáticos.
- **Fase 5: actualización y mantenimiento.** Revisión y evaluación del plan y mantenimiento del mismo.

4.2.6. Simulacros

La realización de simulacros es un excelente método para **preparar** al personal ante situaciones de crisis de ciberseguridad.

Con los simulacros se comprueba si la empresa está preparada para dar una respuesta organizada y eficaz ante un incidente o evento de ciberseguridad. Permiten reforzar la capacidad de respuesta ante un incidente y, por ende, frente a una crisis, gracias a la concienciación y sensibilización del personal involucrado, además de identificar áreas de mejora en los procedimientos desarrollados.

Se recomienda definir una **persona encargada de organizar** el simulacro, la cual tendrá las siguientes **funciones**:

- **Definir** las metas, alcance y escenario del simulacro.
- **Identificar** las herramientas que se van a utilizar (ya sea documentación o tecnologías, dependiendo del tipo de simulacro realizado).
- **Velar** por una comunicación clara y coordinada.
- **Supervisar y controlar** el desarrollo del propio simulacro.

4.2.6.1. Tipos de simulacros

Dependiendo de la disponibilidad de la empresa, se pueden realizar diferentes tipos de simulacros, que evalúan y prueban los planes elaborados desde diferentes perspectivas. A continuación, se identifican tres tipos principales:

- ***Tabletop***: se trata de un ejercicio, de carácter ejecutivo, que simula una situación real dada por un incidente o evento de ciberseguridad. Este enfoque se realiza desde un punto de vista teórico.
  - Los **objetivos** principales de este tipo de ejercicios son:
    - Poner a prueba la capacidad de respuesta de las personas involucradas ante posibles amenazas o ataques de ciberseguridad.
    - Evaluar los planes o procedimientos elaborados por la empresa, analizando si cubren las necesidades de la misma.
    - Detectar áreas de mejora.
  - Es importante destacar que estos ejercicios no interrumpen la operatividad normal de la empresa.
- **Simulación en paralelo:** se trata de una prueba que simula un incidente dentro de un entorno controlado.
  - El objetivo principal de esta prueba es evaluar la capacidad de respuesta la empresa ante un incidente de ciberseguridad que interrumpe, parcialmente, la operatividad de la empresa.
  - Permite operar de manera normal mientras se prueba un determinado componente o proceso.
- **Interrupción total:** se trata de una prueba planificada que recrea escenarios de incidentes graves.
  - El objetivo principal de esta prueba es evaluar la capacidad de respuesta de la empresa ante situaciones críticas y la recuperación del control sobre sus sistemas TI.
  - Se replica un incidente que interrumpe totalmente la operatividad normal de la empresa, por lo que es necesario buscar un momento en el que impacte lo menos posible (por ejemplo, en horario nocturno o en fin de semana).

4.2.6.2. Etapas de un simulacro

Es importante diferenciar las etapas en las que consta un simulacro, identificando principalmente tres:

- **Contexto:** en esta etapa se definen los objetivos y el alcance del simulacro.
  - Dependiendo del tipo de simulacro, en esta etapa se pueden encontrar acciones tales como asignación de roles, introducción al escenario, entrega de documentación, etc.
- **Gestión de la crisis:** en este momento del ejercicio se simula el incidente de ciberseguridad y se evalúa la respuesta de las partes involucradas en la gestión de la crisis, ya sea desde un punto de vista teórico o práctico, según el tipo de simulacro realizado.
- **Fin del simulacro:** en esta última etapa del simulacro, se analiza todas las acciones ejecutadas y se extraen las lecciones aprendidas.
  - Se evalúa la respuesta por parte de las partes involucradas.
  - Se recopilan las observaciones realizadas por las partes involucradas y el organizador.
  - Se identifican las áreas de mejora.
  - Se elabora un informe con toda la información anterior.

Una vez finalizado el ejercicio, se deberán implementar todas las lecciones aprendidas identificadas en el informe final. Esto permitirá revisar y actualizar los procesos y procedimientos de respuesta a incidentes de ciberseguridad en base a dicho informe.

A continuación, se muestra un ejemplo de las fases de un simulacro, en concreto, un *tabletop*:

Ilustración 10 - Ejemplo de fases de un simulacro tabletop

4.3. Identificación y análisis

Esta fase consiste en la correcta **detección e identificación de los incidentes** que se pueden dar en el ámbito de la empresa, de tal manera que, posteriormente, se puedan analizar y, en función de su impacto en el negocio, valorar si se debe declarar una situación de crisis.

La cantidad de eventos que se pueden considerar un incidente de seguridad de la información son infinitos y muy diversos entre sí, pero, en cualquier caso, las empresas deben estar siempre preparadas para reaccionar de la forma más adecuada a los mismos.

Para facilitar la tarea de **detección de posibles incidentes**, se debe tener en cuenta los vectores de ataque más comunes en el ámbito de la ciberseguridad **[9]**, como pueden ser los ataques vía email, vía web, mediante elementos removibles (por ejemplo, un *pendrive*), ataques de fuerza bruta o suplantación de elementos originales por ejecutables maliciosos, entre otros.

Además de tener en cuenta los vectores de ataque más comunes, una de las claves para poder determinar si ha ocurrido un **incidente de seguridad de la información** es detectar posibles señales de la ocurrencia de los mismos.

Detectar estas señales y determinar si se trata o no de un incidente de seguridad es uno de los puntos más difíciles de llevar a cabo por las empresas, debido principalmente al alto número de falsos positivos, la complejidad del análisis y correlación de los datos recogidos a través de distintas fuentes (SIEM, antivirus, etc.) y el profundo conocimiento técnico, sumado a la experiencia necesaria para poder sacar conclusiones claras sobre lo ocurrido.

Las señales que se pueden encontrar en el ámbito de la empresa se pueden dividir en dos tipos:

- **Precursor**: señales que indican que un incidente puede ocurrir en un futuro (por ejemplo, la detección a través los *logs* de una web de que se ha realizado un escaneo de vulnerabilidades sobre la misma).
- **Indicadores**: señales que indican que un incidente ya ha ocurrido o está ocurriendo actualmente (por ejemplo, una alerta lanzada por el antivirus indicando que se ha detectado un archivo malicioso).

Las fuentes más comunes que pueden ser de gran utilidad para la detección de precursores e indicadores son: **IDS/IPS, SIEM [10]** antivirus, *software* de comprobación de integridad de los ficheros, servicios de monitorización, logs (de sistemas operativos, de red, de aplicación, etc.), información sobre nuevas vulnerabilidades y *exploits* y detección de comportamientos anómalos por parte de personas internas o externas a la empresa.

El siguiente paso consiste en **analizar estas señales que han sido detectadas** para, en primer lugar, comprobar que no se trate de falsos positivos, y seguidamente determinar si se trata de un incidente o, en su defecto, la anomalía viene derivada de otra razón como puede ser un error de usuario. Para facilitar esta tarea se puede tener en cuenta una serie de **buenas prácticas**, como, por ejemplo, el perfilado de redes y sistemas, disponer de una política de retención de *logs*, realizar una correcta correlación de eventos, contrastar con distintas fuentes información sobre incidentes y realizar una buena coordinación para trabajar en equipo entre las distintas áreas implicadas.

Tras determinar que se ha producido un **incidente de seguridad de la información**, este debe ser adecuadamente documentado, incluyendo información relevante como los sistemas, redes y servicios afectados, la descripción del incidente, indicadores relacionados, información de contacto según el alcance del incidente, etc.

Finalmente, es fundamental **identificar la criticidad e impacto** del mismo, de tal manera que, si se trata de un evento con afectación importante para la empresa, se pueda llegar a considerar la situación de crisis (**ver apartado 4.2**), en cuyo caso el primer paso es notificar internamente el incidente y convocar de manera inmediata al **Comité de Crisis**.

Este proceso de **notificación interna** debe estar bien definido especificando los contactos a los que se debe avisar, mediante qué canales y qué información es la que se debe incluir en relación al incidente implicado. Como **ejemplo de los canales** que se podrían utilizar para la notificación interna se propone lo siguiente:

1. Realizar la notificación a través de una herramienta interna habilitada con estos fines.
2. En caso de que no sea posible la notificación a través de la herramienta, se debe realizar mediante correo electrónico a un buzón dedicado.
3. Si ninguna de las opciones anteriores se pudiera llevar a cabo, la siguiente opción sería la comunicación vía telefónica con la persona designada para ello o, en su defecto, con los contactos de backup si no hubiera respuesta por parte del contacto de referencia.

Ilustración 11 - Factores para convocar al Comité de Crisis

4.4. Respuesta y comunicación

Durante la reunión del Comité de Crisis, lo primero que se debe decidir es si con la información recopilada del incidente se debe activar el **plan de gestión de crisis de ciberseguridad**. En caso de activación del plan, seguidamente se deben adoptar acciones relacionadas con la **contención** del incidente. Elegir las estrategias adecuadas de contención en función de la naturaleza de los incidentes y aplicarlas con la mayor inmediatez es fundamental para evitar que la situación se agrave.

Algunos ejemplos de medidas de contención serían la desconexión de un sistema potencialmente comprometido de la red, el apagado de un determinado servidor o la inhabilitación de ciertos servicios.

A continuación, se indican ciertos aspectos a tener en cuenta para **seleccionar** las mejores **estrategias de contención** según cada caso:

- Necesidad de **preservar evidencias**, teniendo en cuenta la posibilidad de que deba ser utilizada en procesos judiciales, en cuyo caso es imprescindible realizar una adecuada recolección de las evidencias y posterior cadena de custodia.
- Priorización de los activos que sustentan **los procesos críticos** del negocio.
- **Disponibilidad** de los servicios.
- **Recursos** y tiempo necesarios para implementar la estrategia.
- **Alcance** de la estrategia de contención (contención total o parcial).
- **Tiempo** durante el cual se va a mantener la estrategia implantada.

Es conveniente tener predefinidas ciertas estrategias de contención ante los incidentes más comunes, pero, como ya se ha mencionado anteriormente, ante la complejidad y diversidad de los incidentes, la empresa debe estar lo suficientemente preparada para tomar acciones inmediatas.

Tras esta primera fase de contención, el siguiente paso es **erradicar** el incidente de manera que se pueda volver a un estado de funcionamiento normal en la empresa.

Para llevar a cabo esta erradicación, y estando claro qué elementos han sido afectados y de qué manera, se procede a eliminar cualquier elemento no deseado surgido durante el incidente, como, por ejemplo, archivos infectados con *malware* o cuentas de usuarios comprometidas.

Posteriormente, comienza la fase de recuperación, en la cual se realiza la vuelta a la normalidad. Esta consiste en, tras el análisis del incidente y el conocimiento generado sobre este, recuperar los sistemas, archivos o cualquier elemento afectado, realizar el cambio de contraseñas comprometidas, corrección de vulnerabilidades, actualización de sistemas y aplicaciones con últimos parches disponibles, refuerzo de seguridad de las redes o mejora de los sistemas de monitorización y alertas, entre otras muchas acciones, según el incidente sufrido.

Estos procesos, según el alcance e impacto de los incidentes, pueden ser muy complejos y requerir mucho tiempo y esfuerzo, por lo que deben realizarle de manera escalonada y **priorizando** las acciones de recuperación para actuar primero sobre los elementos más críticos.

Durante esta fase, y en paralelo a las acciones de respuesta ante incidentes, se deberá también **notificar** sobre la situación a aquellos agentes externos que, en cumplimiento con las leyes aplicables, deban ser informados de manera obligatoria, así como a las partes interesadas que la empresa decida incluir en el flujo de comunicación.

Para ello, una vez reunido el Comité de Crisis y activado el plan de gestión de crisis, se debe poner en marcha el **plan de comunicación** de la empresa, el cual debe estar previamente definido por la entidad, y en el que se deben detallar los pasos a desarrollar para lograr una transmisión efectiva y coherente de información. Dicho plan debe estar alineado con los valores, principios, misión y visión de la empresa.

El **plan de comunicación debe de tener claramente definido**, entre otras cosas, lo siguiente:

- Las **estrategias** generales que se van a llevar a cabo.
- Los **canales** de comunicación a las autoridades competentes, como lo son: correos electrónicos, formularios, etc. Se deberán establecer también canales seguros y alternativos, considerando la posibilidad de que los principales se hayan visto afectados.
- El **portavoz** o portavoces en la comunicación, además de todos los roles que se deseen involucrar en el equipo de comunicación.
- La **audiencia** objetivo (todos los *stakeholders*).
- Las **metas** específicas que se desean alcanzar con las diferentes actividades de comunicación.

Con la finalidad de construir un mensaje adecuado para todos los stakeholders, se debe diseñar un **mensaje clave** que permita transmitir de manera transparente y contundente. Debe responder a las siguientes cuestiones:

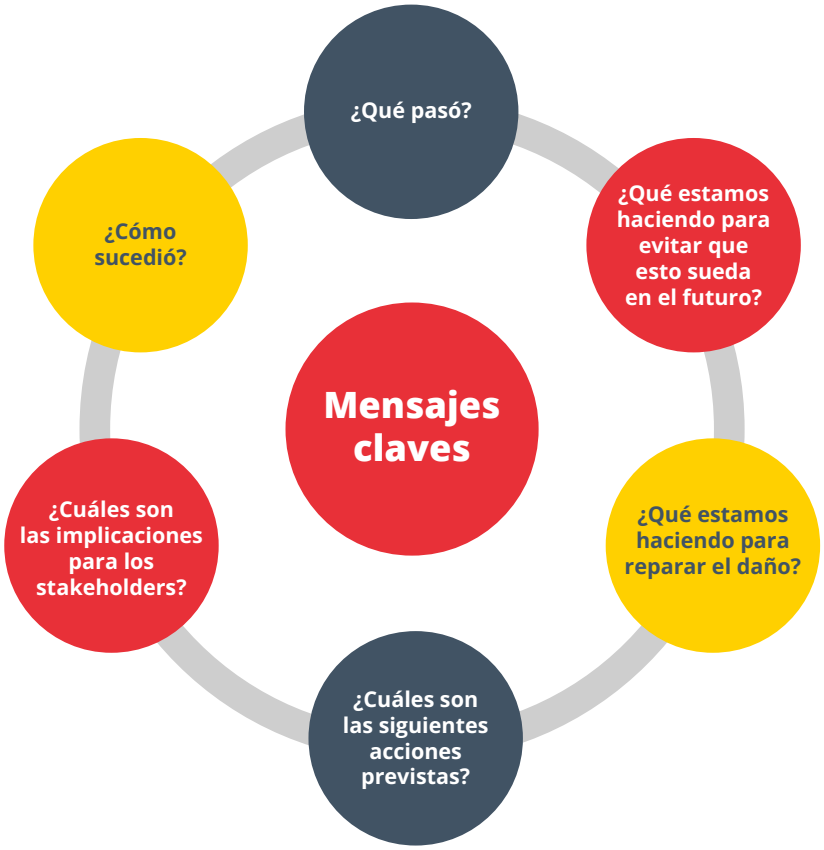


Ilustración 12 - Mensajes claves

Por otra parte, en caso de sufrir una crisis de ciberseguridad, es recomendable evitar:

- **Permanecer inactivos**, es decir, no hacer absolutamente nada.
- **Mentir** o negar lo que está sucediendo.
- En las comunicaciones emitidas, **nombrar** el o los responsables de la crisis.
- **Comunicar** públicamente el impacto de lo sucedido y los daños ocasionados.

4.5. Cierre

La **desactivación** del plan de gestión de crisis de ciberseguridad es el punto de cierre del proceso de gestión de la crisis, cuya decisión es competencia del Comité de Crisis. En esta fase, y con el objetivo de ayudar a esta toma de decisiones, también se debe realizar una **revisión** del estado actual de las amenazas de ciberseguridad (previo informe del grupo técnico y/o responsable) para valorar si el incidente efectivamente ha sido solucionado.

Si la amenaza ha sido mitigada y la empresa puede volver a desarrollar sus funciones y actividades correctamente, se procederá formalmente al cierre de la crisis.

Es importante resaltar que la desactivación de la crisis **debe ser comunicada** ante todos los *stakeholders* y las autoridades competentes, a través de los canales que hayan sido anteriormente definidos y con las pautas desarrolladas en el apartado de comunicación.

4.5.1. Lecciones aprendidas

Es necesario precisar que el cierre de la crisis de ciberseguridad no termina con la mitigación de la amenaza, sino que se debe realizar una **auditoría** detallada de cada una de las etapas, acciones realizadas y grupos involucrados, con el objetivo de identificar mejoras aplicables en las medidas de seguridad de la empresa y en el procedimiento seguido.

Se deben documentar tanto las prácticas que funcionaron correctamente y que, por tanto, pueden mantenerse, como aquellos puntos que necesitan mejoras significativas. Con toda esta información se puede **desarrollar un plan de mejora** en el que establecer prioridades y plazos para la implementación de los cambios.

Es conveniente solicitar ***feedback*** por parte del equipo encargado de responder al incidente, así como de los empleados afectados para conocer diferentes opiniones.

Con esta práctica se deberá dar respuesta, entre otras, a las siguientes **cuestiones**:

Ilustración 13 - Lecciones aprendidas

5. Gestión de crisis ocasionadas por incidentes en proveedores (cadena de suministro)

Actualmente, la mayoría de las empresas necesitan **servicios externos** que den soporte a su actividad para poder desarrollarla de manera satisfactoria y eficiente. Así pues, además de asegurar al máximo los sistemas, es imprescindible **exigir el mismo nivel de seguridad a los proveedores externos**, ya que no solo hay proteger la información de manera interna, sino que los proveedores deben ser responsables de custodiarla con un nivel de seguridad adecuado antes, durante y al finalizar la prestación del servicio **[11]**.

Además, no puede obviarse la importancia de que un proveedor sea víctima de un ataque de ciberseguridad que afecte a la empresa, ya que, adicionalmente a la filtración o pérdida no deseada de datos confidenciales, supone una **grave afectación a la reputación**, dado que será sinónimo de no haber puesto el cuidado necesario a la hora de elegir proveedores que cumplan adecuadamente las medidas de seguridad indispensables.

Para ello, es primordial desarrollar una **política de seguridad general en proveedores [12]**, la cual será explicada en el siguiente apartado.

5.1. Elaboración de política de seguridad general en proveedores

Esta política permite **gestionar las relaciones con proveedores**, de manera que todo el personal externo que desarrolle servicios para la empresa se vea obligado a cumplir con sus directrices y facilitar su aplicación dentro de su ámbito de actuación.

A continuación, se propone una serie de aspectos fundamentales a tener en cuenta para la elaboración de dicha política, sin perjuicio de que cada empresa elabore a mayores una **política de seguridad específica para los proveedores**:

Requisitos de seguridad y control en los productos y/o servicios contratados:

Es necesario definir los requisitos de seguridad mínimos que deben tener los productos y/o servicios que se contratan. Dichos requisitos deberán ser coherentes con la política de seguridad de la información. Con el fin de velar por la seguridad de los productos y/o servicios proporcionados por los proveedores, se podrán **implantar los mecanismos de control que se consideren oportunos**, como, por ejemplo, auditorías, ya sea de forma periódica o de manera esporádica, siempre que se considere conveniente.

Resulta importante mencionar de nuevo el **"apetito de riesgo"** de la empresa, es decir, el nivel de peligro que está dispuesta a asumir cuando contrata un producto y/o servicio con un proveedor en concreto, ya que, en ocasiones, puede ser interesante asumir cierto riesgo si mejora la rentabilidad o, por el contrario, puede no ser recomendable contratar los servicios y/o productos de un determinado proveedor, debido al alto riesgo que presenta por no disponer de las medidas de seguridad pertinentes.

Cláusulas contractuales de seguridad de la información

Se deben elaborar cláusulas contractuales en materia de seguridad de la información que establezcan de manera detallada los puntos más relevantes que deben reflejarse en el contrato con el proveedor en cuestión. Estas cláusulas deberán recoger aspectos como el tipo de información al que accederá el proveedor, cómo va a acceder a ella, qué situaciones podrían dar lugar a la finalización del contrato, etc.

Para ello, resulta fundamental elaborar un **acuerdo de confidencialidad** en el que se garantice la seguridad de la información tratada durante el desarrollo del contrato, asegurando de que no se divulgará a terceros no autorizados ni se utilizará fuera del ámbito laboral habitual.

En relación con lo anterior, es importante tener en cuenta que, por defecto, **toda aquella información relacionada con el negocio** (documentación, programas, aplicaciones, estrategias de negocio...) será considerada confidencial y su tratamiento e intercambio se realizará, en todo caso, siguiendo el marco de lo acordado en el contrato de servicios.

Únicamente podrá considerarse **información no confidencial** aquella a la que se pueda acceder a través de medios de difusión pública (periódicos, radio...).

Definición de responsabiliades para ambas partes

Se deben especificar las responsabilidades tanto por parte del proveedor como por parte de la empresa, para el caso de que se produzca un incumplimiento del contrato.

Se debe asegurar de que todo el personal integrante de los proveedores con los que existe una relación contractual **desarrolle sus funciones de manera responsable y diligente**, aplicando los procedimientos establecidos para manejar la información facilitada (por ejemplo, manteniendo bajo control los sistemas de autenticación proporcionados a cada usuario y estableciendo contraseñas robustas).

Acuerdos de nivel de servicio (ANS)

Como se ha tratado anteriormente, es importante **asegurar la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información** manejada por los proveedores, así como de los servicios que presten.

Para ello, se debe elaborar un **contrato** en el que se especifique claramente qué producto y/o servicio se compromete el proveedor en cuestión a prestar a la empresa contratante, incluyendo los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de la tecnología de la información y comunicación.

Además, resulta primordial definir de manera exacta el servicio prestado evitando de este modo ambigüedades o confusiones, así como **establecer la manera en que van a colaborar el proveedor y la empresa** (por ejemplo, si se contrata un servicio de mantenimiento con una empresa informática, se deberá especificar en qué consiste exactamente ese mantenimiento y cómo va a llevarse a cabo, evitando alusiones genéricas como "servicio de mantenimiento informático", que no proporcionen más especificaciones).

Adicionalmente, es de especial relevancia también **definir los parámetros e indicadores necesarios** para asegurar que los servicios prestados por los proveedores están cumpliendo con lo acordado, como podría ser, por ejemplo, los tiempos de respuesta o de resolución de incidencias. De esta manera, se pueden asociar penalizaciones en caso de incumplimiento de estos parámetros.

Controles de seguridad obligatorios

Se deben definir los **controles de seguridad** que el proveedor en cuestión debe cumplir de manera obligatoria para establecer una relación contractual con la empresa contratante (por ejemplo: ¿a qué información van a poder acceder y cómo?, ¿a qué servicios y componentes informáticos va a poder acceder el proveedor?, ¿se están cumpliendo los ANS acordados previamente? En caso de que se produzca una incidencia, ¿cómo se va a gestionar?, ¿se están utilizando métodos de identificación y autenticación robustos?, ¿se ha establecido una política de buenas prácticas en el uso de medios tecnológicos?).

Se deberá **evaluar el grado de cumplimiento** de cada uno de los controles definidos.

Certificaciones en materia de ciberseguridad

Es conveniente solicitar a los proveedores con los que se pretende **contratar productos y/o servicios** (sobre todo, si van a tratar datos especialmente sensibles o los servicios que ofrecen son críticos o esenciales) garantías de su cumplimiento respecto a la calidad de la gestión de la seguridad de la información (por ejemplo: Certificación ISO 27001 de Sistemas de Gestión de la Seguridad de la Información o Certificación ISO 22301 de Gestión de Continuidad de Negocio).

En este sentido, cabe destacar la **importancia de exigir estos certificados**, incluso aunque la ley no lo requiera para la contratación de todos los proveedores. De esta manera, aunque sea necesario tener un control mínimo de los proveedores contratados, se puede evitar llevar a cabo **controles más exhaustivos** para comprobar que cumplen en todo momento con las medidas de seguridad necesarias.

Terminación de la relación contractual

Se debe garantizar, una vez que finalice el contrato con el proveedor, que este dispone de las **instrucciones pertinentes** en relación con los pasos a seguir para garantizar, en todo momento, la seguridad de la información a la que ha accedido durante la relación contractual. Se deberá señalar qué activos han de ser devueltos y cómo, se deben eliminar los permisos de acceso del proveedor a los sistemas internos y/o instalaciones, se deben aportar las directrices que el proveedor debe seguir para el borrado de la información facilitada por la empresa, etc.

Concienciación del personal en materia de ciberseguridad

Es esencial que todos los miembros de las empresas proveedoras con las que se colabora estén **concienciados y actualizados** en materia de ciberseguridad para evitar así fugas de información no deseadas a causa de errores humanos.

Tal y como se ha señalado al principio de este apartado, las pautas expuestas no constituyen una lista cerrada, siendo únicamente un conjunto de mínimos a considerar para elaborar la política de seguridad general. Sin perjuicio de lo anterior, **cada empresa deberá añadir todos aquellos controles** que considere oportunos para evaluar la seguridad del proveedor en cuestión, en función de los productos y/o servicios prestados, elaborando así su política de seguridad específica.

5.2. Gestión de crisis originadas por un incidente significativo en un proveedor

De manera análoga al **plan de gestión de crisis** que se ha desarrollado en la presente guía, en caso de que el proveedor de una empresa sufra un incidente significativo, este deberá ser tratado adecuadamente siguiendo un procedimiento similar al que se ha definido previamente, enmarcado en las mismas fases.

5.2.1. Preparación

En primer lugar, lo más importante será estar preparado para hacer frente a un incidente en un proveedor, pudiendo detectarlo y subsanarlo a tiempo. Para ello, se proponen las siguientes **buenas prácticas**:

Registro de proveedores

Es necesario llevar un **control documentado de todos aquellos proveedores** que han trabajado o trabajan actualmente con la empresa, así como de sus trabajadores, y categorizarlos según su criticidad (dependiendo esta de los procesos de negocio a los que presten servicio y la información que manejen). Para los procesos más críticos se podrán identificar proveedores alternativos para garantizar la continuidad del negocio.

Establecer un plan de notificación de incidentes

Es primordial establecer el **procedimiento a seguir en caso de que se produzca un incidente de seguridad**. Debe incluir los requisitos para llevar a cabo la notificación, los criterios para considerar un incidente como mitigado, el canal a través del cual transmitir la información, los tiempos, etc. Deberá identificarse un responsable de seguridad por parte de cada proveedor, que actuará como punto de contacto en estas situaciones.

Realización de auditorías

Con el objetivo de **detectar posibles vulnerabilidades o cambios en los servicios prestados** por los proveedores que puedan dar lugar a un riesgo de seguridad. Es responsabilidad de cada empresa contratar únicamente a aquellos proveedores que demuestren cumplir con las medidas de seguridad exigidas por la legislación vigente o por las políticas internas de la empresa.

5.2.2. Identificación y análisis

En esta fase el **proveedor afectado** por el incidente será el que **notifique** a la empresa con la que mantiene una relación contractual sobre la situación y los posibles riesgos para la seguridad de la información.

En esta notificación se deberá detallar qué servicios, sistemas y/o redes se han visto impactados por el incidente, cuál o cuáles han sido los vectores de ataque, qué consecuencias implica y de qué manera podría afectar a la empresa contratante.

Es importante llevar una excelente **coordinación y comunicación** entre ambas partes para realizar un seguimiento a tiempo real de la situación y evolución de la misma.

Dentro de estas tareas de cooperación, es fundamental determinar si ha podido haber afectación sobre la infraestructura de TI o la información confidencial de la empresa contratante. En caso afirmativo, se debe profundizar en el grado de criticidad e impacto del incidente para, en caso de cumplir con las condiciones necesarias y considerarse una crisis de ciberseguridad, **convocar al Comité de Crisis**.

5.2.3. Respuesta y comunicación

Durante la reunión del Comité de Crisis se deberá decidir si se debe **activar el plan de gestión de crisis de ciberseguridad** de la empresa, en cuyo caso se seguirán a partir de este momento las pautas definidas en el mismo.

Como medidas de contención, y después de analizar en detalle las implicaciones sobre los sistemas y redes internos, se debe valorar la **aplicación de acciones** como:

- **Revocar los accesos** del personal del proveedor a sistemas internos.
- **Desconexión** de sistemas, redes o aplicaciones suministradas por el proveedor.
- **Limitación de servicios** ofrecidos por el proveedor.

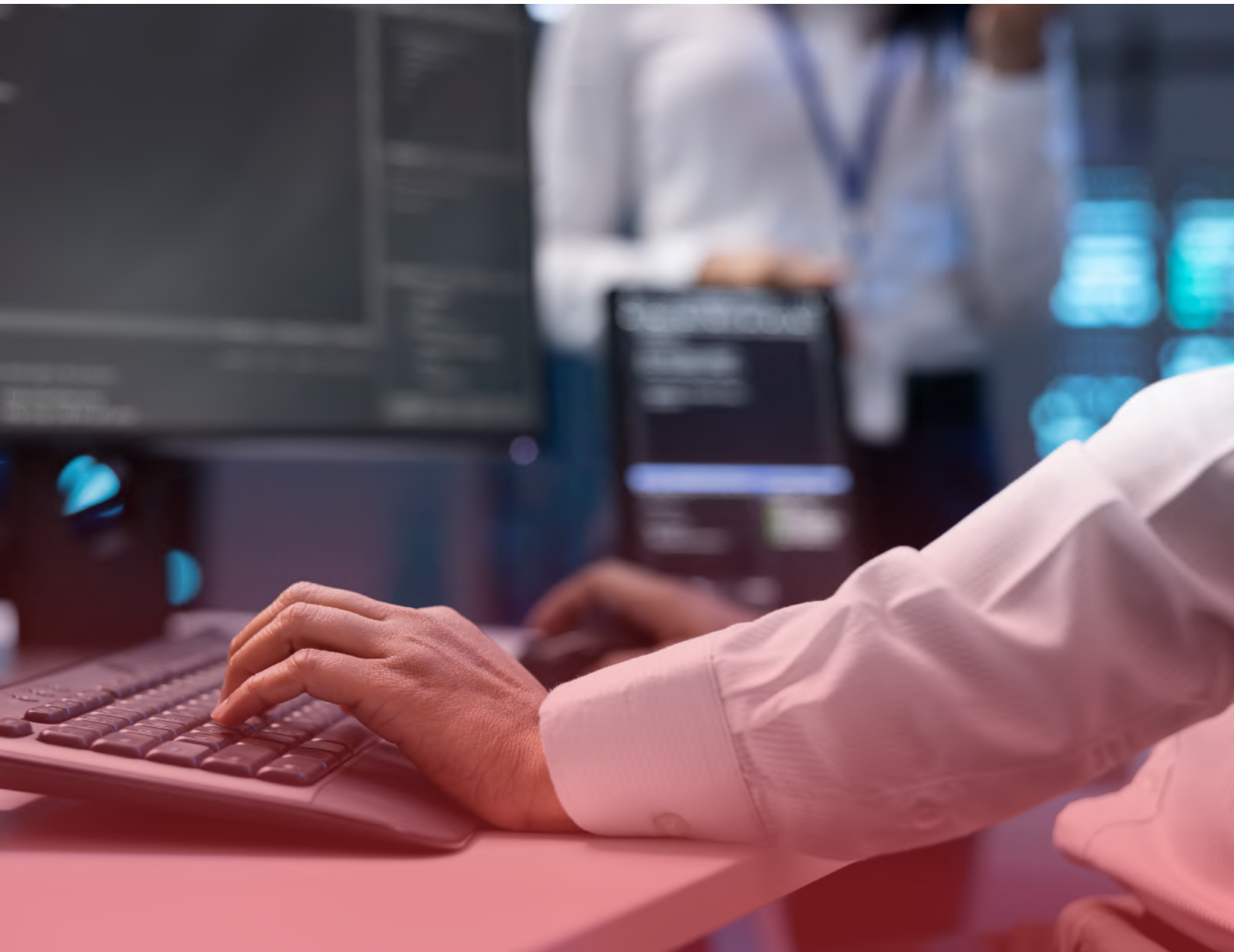
Posteriormente, se procederá a la erradicación y recuperación de los activos afectados, tal y como se explica en el plan de gestión de crisis.

Si aplicara realizar comunicaciones externas sobre el incidente de seguridad de la información sufrido internamente a través de un proveedor, las pautas también son las mismas que se indican en el **plan de comunicación** mencionado.

5.2.4. Cierre y lecciones aprendidas

Las acciones de esta fase se corresponden también con las descritas en las buenas prácticas para la gestión de crisis de ciberseguridad, centrándose en la revisión de los procedimientos y estrategias definidos. No obstante, en el caso específico de incidentes derivados de proveedores, es necesario revisar aspectos de mejora relacionados con la seguridad en la gestión de proveedores. Algunas de estas **medidas** pueden ser:

- **Revisar y actualizar las medidas de seguridad** establecidas en el contrato con el proveedor, con el objetivo de hacerlas más restrictivas.
- **Valorar la posibilidad de realizar un cambio de proveedor** en caso de que no cum-pla con las medidas de seguridad exigidas.
- **Mejorar las tareas de seguimiento y monitorización** sobre los servicios prestados por el proveedor.



6. Anexo

Anexo I: Guía práctica

A continuación, se indica en una representación gráfica, las **fases y principales acciones** que componen la gestión de una crisis de ciberseguridad.

Ilustración 14 - Guía práctica de gestión y notificación

Anexo II: Nivel de peligrosidad y nivel de gravedad de un incidente

Según lo establecido en la **"Guía nacional de notificación y gestión de ciberincidentes" [13]**, se incluyen a continuación dos tablas que se pueden emplear como referencia para determinar el nivel de peligrosidad e impacto, respectivamente, de un incidente. Se consideran cinco niveles: crítico, muy alto, alto, medio y bajo.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES		
Nivel	**Clasificación**	**Tipo de incidente**
Crítico	Otros	APT
Muy alto	Código dañino	Distribución de *malware*
		Configuración de *malware*
	Intrusión	Robo
	Disponibilidad	Disponibilidad
		Interrupciones
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Código dañino
		Servidor C&C (mando y control)
	Intrusión	Compromiso de aplicaciones
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (denegación de servicio)
		DDoS (denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	*Phishing*
Medio	Contenido abusivo	Discurso de odio
	Orientación de información	Ingeniería social
		Explotación de vulnerabilidades conocidas
	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
	Vulnerable	Criptografía débil
		Amplificador
		DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
Bajo	Contenido abusivo	*Spam*
	Obtención de información	Escaneo de redes *(scanning)*
		Análisis de paquetes *(sniffing)*
	Otros	Otros

Tabla 7 - Nivel de peligrosidad de un ciberincidente

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
Crítico	Afecta apreciablemente a la seguridad nacional
	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas
	Afecta a una infraestructura crítica
	Afecta a sistemas clasificados SECRETO
	Afecta a más del 90% de los sistemas de la organización
	Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios
	El ciberincidente precisa para resolverse más de 100 jornadas-persona
	Impacto económico superior al 0,1% del PIB actual
	Extensión geográfica supranacional
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales
Muy alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales
	Afecta apreciablemente a actividades oficiales o misiones en el extranjero
	Afecta a un servicio esencial
	Afecta a sistemas clasificados RESERVADO
	Afecta a más del 75% de los sistemas de la organización
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios
	El ciberincidente precisa para resolverse entre 30 y 100 jornadas-persona
	Impacto económico entre el 0,07% y el 0,1% del PIB actual
	Extensión geográfica superior a 4 CC. AA. o 1 TIS
	Daños reputacionales a la imagen del país (marca España)
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales
Alto	Afecta a más del 50% de los sistemas de la organización
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios
	El ciberincidente precisa para resolverse entre 5 y 30 jornadas-persona
	Impacto económico entre el 0,03% y el 0,07% del PIB actual
	Extensión geográfica superior a 3 CC. AA.
	Daños reputaciones de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros
	Daños reputaciones de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros

Tabla 8 - Nivel de impacto de un ciberincidente

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
Medio	Afecta a más del 20% de los sistemas de la organización
	Interrupción en la prestación del servicio superior al 5% de los usuarios
	El ciberincidente precisa para resolverse entre 1 y 5 jornadas-persona
	Impacto económico entre el 0,001% y el 0,03% del PIB actual
	Extensión geográfica superior a 2 CC. AA.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación)
Bajo	Afecta a los sistemas de la organización
	Interrupción de la prestación de un servicio
	El ciberincidente precisa para resolverse menos de 1 jornadas-persona
	Impacto económico entre el 0,0001% y el 0,001% del PIB actual
	Extensión geográfica superior a 1 CC. AA.
	Daños reputacionales puntuales, sin eco mediático
Sin impacto	No hay ningún impacto apreciable

Tabla 8 - Nivel de impacto de un ciberincidente

Anexo III: Formulario de notificación a la autoridad competente

La **"Guía nacional de notificación y gestión de ciberincidentes" [13]**, además, especifica los datos que se deben cumplimentar a la hora de notificar un incidente de ciberseguridad, los cuales están disponibles en la siguiente tabla:

QUÉ NOTIFICAR	DESCRIPCIÓN
Asunto	Frase que describa de firma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
OSE/PSD	Denominación del operador de servicios esenciales o proveedor de servicios digitales que notifica.
Sector estratégico	Energía, transporte, financiero, etc.
Fecha y hora del incidente	Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente.
Fecha y hora de detección del incidente	Indicar con la mayor precisión posible cuándo ha detectado el ciberincidente.
Descripción	Describir con detalle lo sucedido.
Recursos tecnológicos afectados	Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones...
Origen de incidente	Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.
Taxonomía (clasificación)	Posible clasificación y tipo de ciberincidente en función de la taxonomía descrita.
Nivel de peligrosidad	Especificar el nivel de peligrosidad asignado a la amenaza. **Ver anexo II**
Nivel de impacto	Especificar el nivel de impacto asignado al incidente. **Ver anexo II**
Impacto transfronterizo	Indicar si el incidente tiene impacto transfronterizo en algún Estado miembro de la Unión Europea. Especificar.
Plan de acción y contramedidas	Actuaciones realizadas hasta el momento en relación al ciberincidente. Indicar el plan de acción seguido junto con las contramedidas implantadas.
Afectación	Indicar si el afectado es una empresa o un particular y las afectaciones que tiene.
Medios necesarios para la resolución	Capacidad empleada en la resolución del incidente en jornadas-persona.
Impacto económico estimado (si se conoce)	Costes asociados al incidente, tanto de carácter directo como indirecto.
Daños reputacionales (si se conocen)	Afectación a la imagen corporativa del operador.
Adjuntos	Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).
Regulación afectada	ENS / RGPD / NIS / PIC / Otros
Se requiere actuación FFCCSE	Sí / No
Extensión geográfica (si se conoce)	Local, autonómico, nacional, supranacional, etc.

Tabla 9 - Formulario de notificación

7. Referencias

[1] Respuesta a incidentes: https://www.incibe.es/incibe-cert/incidentes/respuesta-incidentes

[2] Servicios operadores: https://www.incibe.es/incibe-cert/servicios-operadores

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of: https://eur-lex.europa.eu/eli/dir/2022/2555

[4] Primeros pasos para clasificar la información de tu organización: https://www.incibe.es/empresas/blog/primeros-pasos-clasificar-informacion-tu-organizacion

[5] Evitando riesgos de ciberseguridad desde el puesto de trabajo: https://www.incibe.es/empresas/blog/evitando-riesgos-ciberseguridad-el-puesto-trabajo

[6] El riesgo ciber, máxima prioridad para pymes y autónomos. https://www.incibe.es/empresas/blog/el-riesgo-ciber-maxima-prioridad-pymes-y-autonomos

[7] Plan de contingencia y continuidad de negocio: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

[8] Plan de contingencia y continuidad de Negocio: https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio

[9] Los 10 vectores de ataque más utilizados por los ciberdelincuentes: https://www.incibe.es/empresas/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes

[10] ¿Qué son y para qué sirven los SIEM, IDS e IPS? https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

[11] Sector cadena de suministros: https://www.incibe.es/incibe-cert/sectores-estrategicos/cadena-de-suministros

[12] Relación con proveedores. Políticas de seguridad para la pyme: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf

[13] Guía nacional de notificación y gestión de ciberincidentes: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa