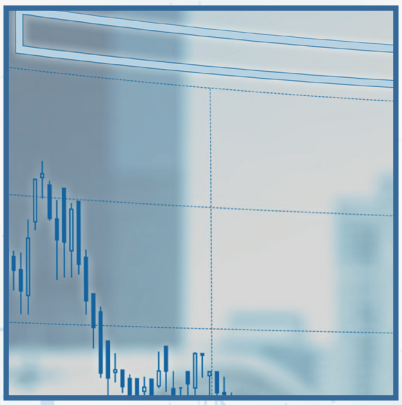
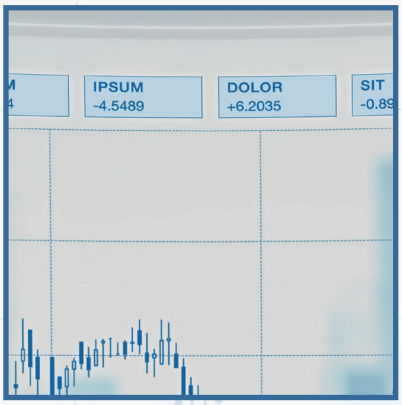
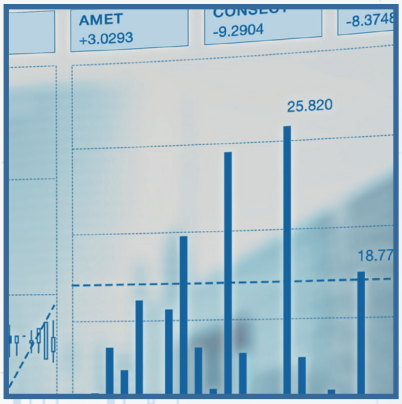
GESTIÓN DE CIBERCRISIS

BUENAS PRÁCTICAS EN LA GESTIÓN DE CRISIS DE CIBERSEGURIDAD







CCN-CERT BP/20

INFORME DE BUENAS PRÁCTICAS

OCTUBRE**2020**

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.11.19 08:21:50 +01'00'

Centro Criptológico Nacional, 2020

Fecha de Edición: octubre de 2020

Índice

1. Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción

Por crisis se entiende cualquier circunstancia, deliberada o fortuita, ocasionada internamente o no, que produce un desequilibrio en una organización con su servicio, clientes, accionistas, trabajadores y representantes sindicales, autoridades u otras empresas o entidades, afectando o dañando la imagen y reputación pública, con la consecuente pérdida económica o incumplimiento legal, pudiendo poner en peligro su viabilidad económica y/o futuro profesional.

Otra definición más breve podría ser: situación de **baja probabilidad** que cuando sucede genera un **gran impacto** y cuyos efectos **perduran en el tiempo**.

Ante una crisis, tres son los elementos a tener en cuenta: la **amenaza** a la organización, el elemento **sorpresa** (imprevisible e inesperado) y el **corto período** de tiempo que se exige para la toma de decisiones. En todo caso, es preciso gestionar las amenazas o circunstancias antes, durante y después de que se produzcan, teniendo claro que no es necesario que exista un problema real para encontrarse en una situación de crisis. Basta con que cualquier rumor o evento transcienda a la opinión pública para que se acelere el proceso e, incluso, y dado el momento actual de las redes sociales, se propague sin control, haciendo cundir el pánico entre los grupos de interés anteriormente citados. Esto hará que la gestión de crisis se dificulte aún más.

La gestión de todo tipo de crisis es una disciplina que ha tenido un importante desarrollo en la última década y desde muy distintos campos, particularmente los relacionados con la Seguridad de la Información (SGSI) y la Comunicación. Al tratarse de situaciones de especial gravedad, que puede llegar a comprometer, no solo el funcionamiento de la organización, sino incluso su futuro, esta gestión ha pasado a ser cada vez más una capacidad imprescindible para un número creciente de organizaciones. Entre los muchos factores que han propiciado su desarrollo cabe destacar, entre otros, la mayor exigencia en cuanto a la prestación de servicio, el incremento de la responsabilidad social y el impacto potencial de las redes sociales sobre su reputación e imagen.

En este contexto, empieza a existir ya un corpus de conocimiento, de base muy heurística, que orienta en cuáles son **los recursos más adecuados** para que las organizaciones desarrollen esta capacidad y en **las prácticas de gestión más aconsejables** con el objetivo de afrontar con éxito crisis de cualquier tipo.

Los efectos de una crisis en una organización se producen sobre:

Toda crisis implica una **toma de decisiones bajo presión**, con **tiempo e información limitados** y en **diversos frentes en paralelo,** y con muchos agentes y personas interviniendo.

Con independencia del origen que cause la crisis, se hace patente la **componente de gestión** que su resolución implica. Para ello, la organización afectada necesita haberse dotado de las **capacidades y estructuras de gestión** adecuadas que le han de permitir abordarla con garantías de éxito.

Por lo tanto, en toda crisis se identifican **dos esferas de actuación** distintas:

- **Operativa y de respuesta técnica al incidente**: la que tiene que ver con el motivo que la origina y cuyos efectos inmediatos deben ser contenidos y resueltos por un equipo de respuesta especializado. Un equipo o capacidad de respuesta a ciberincidentes que, detectando rápidamente ataques y amenazas, minimice la pérdida o la destrucción de activos tecnológicos o de información, mitigue la explotación dañina de los puntos débiles de las infraestructuras y alcance la recuperación de los servicios a la mayor brevedad posible[1]. Una actividad compleja que debe contemplar la adopción de métodos de recopilación y análisis de datos y eventos, metodologías de seguimiento y procedimientos de tipificación de su peligrosidad y priorización.
- **Organizativa y estratégica** en la medida en que su impacto afecta a diferentes ámbitos de la organización (servicio, operativa, imagen y reputación, relación con el regulador, grupos de interés, presencia en redes sociales, etc.) y requiere de una respuesta coordinada a alto nivel, determinando los canales de comunicación con otras unidades o entidades, propias y/o ajenas

Las capacidades y estructuras de gestión necesarias para hacer frente a una crisis no se improvisan cuando esta surge, es imprescindible desarrollarlas con antelación.

Las capacidades y estructuras de gestión necesarias para hacer frente a una crisis no se improvisan cuando esta surge, es imprescindible desarrollarlas **con antelación** para disponer de la preparación necesaria en ese momento.

1 Guía CCN-STIC 817_Gestión de Ciberincidentes: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

A modo de marco de referencia, las Figuras 1 y 2 muestra el perfil genérico de una crisis y sus fases principales, alrededor de las cuales se articulará la propuesta de buenas prácticas desarrollada en el presente documento:

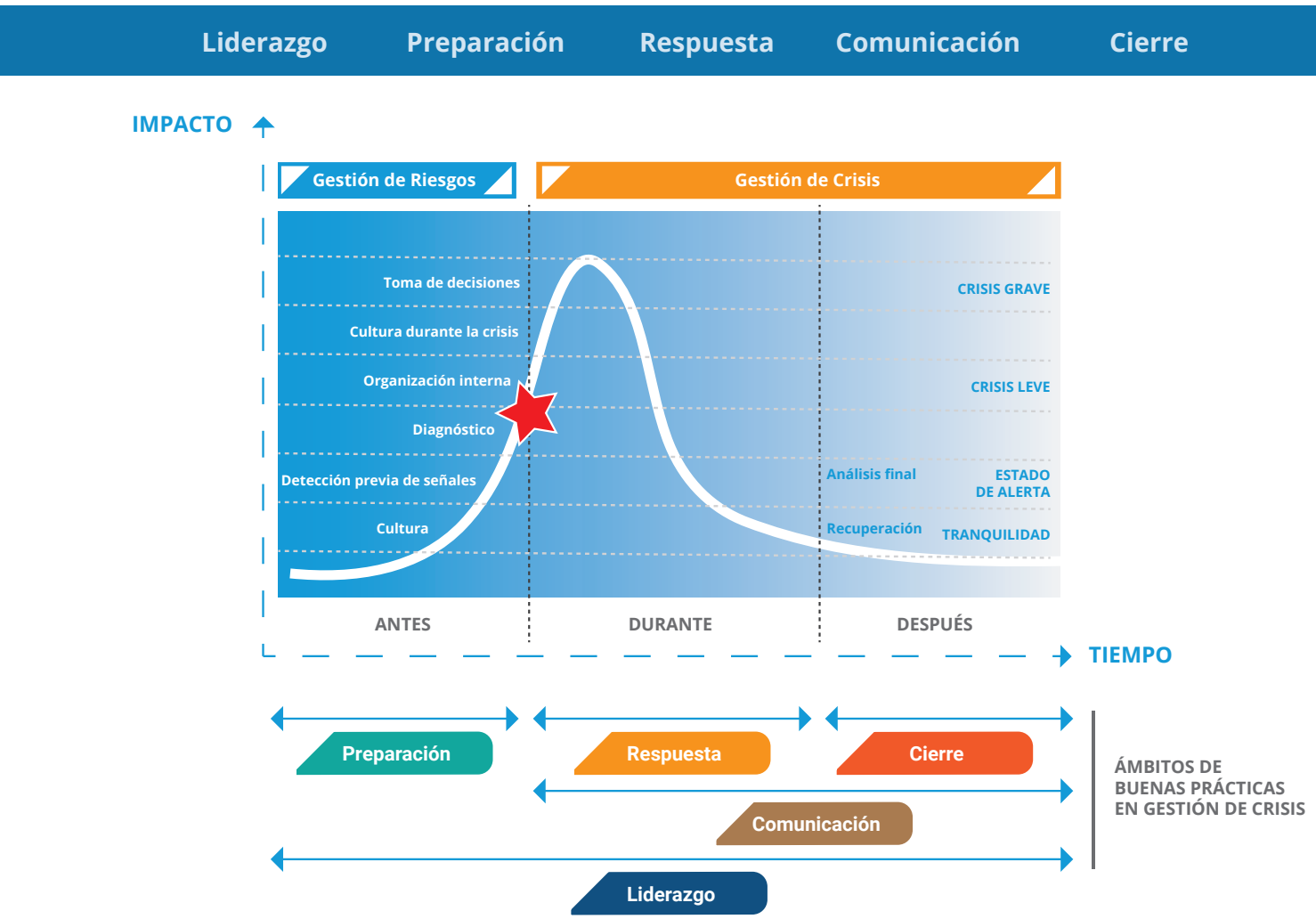


Figura 1. Perfil de una crisis[2]

Figura 2. Ámbitos fundamentales para abordar una crisis

2 Buenas prácticas en la gestión de crisis Institut Cerdá (Figuras 1 y 2)

En este sentido, se ha de insistir en la importancia de haber realizado un **trabajo previo** que haga que la organización esté preparada cuando surja la crisis: el **análisis de riesgos**, el **desarrollo de los planes de actuación** asociados y la **definición de las estructuras de gestión** adecuadas deben asegurar que se realiza, de forma constante, un **ejercicio de prospectiva** de modo que sea posible estimar el tipo de ciberataque más probable para adelantarse al problema diseñando el modo de gestionarlo ante el mínimo indicio de materialización.

Centrándonos en la materia de este Informe, podemos **definir**, pues, una **cibercrisis** como un acontecimiento del ámbito de la ciberseguridad con **gran impacto** sobre la actividad de la organización y que requiere tomar **decisiones rápidas** con información limitada. La probabilidad de ese acontecimiento dependerá del grado de preparación previa de la organización: será muy pequeña si se han tomado un gran número de medidas preventivas y progresivamente mayor cuanto menor sea el trabajo de prevención llevado a cabo con anterioridad.

La presente guía de buenas prácticas en la gestión de ciberincidentes se basa en análisis detallados de episodios reales recientes de los que se derivan recomendaciones para abordar crisis en general, particularizando en cada caso la buena praxis para el gobierno de crisis derivadas de incidencias de ciberseguridad.

Para ello se plantea un decálogo de trece (13) buenas prácticas[3], resumidas en la Figura 3, que se consideran componentes fundamentales del modelo de éxito para abordar una crisis y que está organizado en los cinco ámbitos apuntados anteriormente -**liderazgo, preparación, respuesta, comunicación y cierre**- relacionados con el perfil genérico de una crisis.

En el apartado 4 se desarrollan dichas buenas prácticas de gestión de crisis por ciberincidentes.

Figura 3. Resumen de buenas prácticas

3 Este decálogo de buenas prácticas procede de una adaptación de la publicación del Institut Cerdà "Monografía 4. Buenas prácticas en la gestión de crisis" de diciembre de 2018 (Fuente: Institut Cerdà)

3. Casos de estudio

Con el objetivo de ilustrar de un modo concreto las buenas prácticas que se detallan en los siguientes epígrafes, los Anexos 1, 2 y 3 desarrollan ejemplos didácticos sobre cibercrisis que resumen las recomendaciones del CCN-CERT ante este tipo de situaciones. Si bien estas buenas prácticas son comunes para todos los casos de gestión de cibercrisis, no todas las crisis provocadas por ciberincidentes exigen el mismo tipo de actuaciones.

El objetivo de estos casos de estudio es mostrar de forma práctica las principales acciones que se han de llevar a cabo ante las situaciones concretas que se detallan.

1

Ciberespionaje:

en este anexo se explican las cuestiones necesarias a tener en cuenta en la gestión de cibercrisis ante un caso de ciberespionaje.

2

Ransomware:

en este anexo se explican las cuestiones necesarias a tener en cuenta en la gestión de cibercrisis provocada por un ataque dirigido a través de malware del tipo ransomware.

3

Extorsión y sustracción de fondos:

en este anexo se explican las cuestiones necesarias a tener en cuenta en una gestión de cibercrisis ante posibles ataques que tienen por objeto la extorsión y sustracción de fondos de la víctima.

4

Resumen de las conclusiones principales:

en este anexo se resumen las conclusiones principales de los casos de estudio anteriormente expuestos.

4. Buenas prácticas en la gestión de crisis por ciberincidentes

BP.1 Liderazgo, valores y control

Es importante liderar, tomar y mantener la iniciativa durante la crisis y, si esta se pierde, buscar las oportunidades que permitan recuperarla. Tomar medidas razonables es casi siempre mejor que no hacer nada; eso sí, **partiendo de una preparación y un Plan previamente acordado**. Será más fácil adoptar las medidas oportunas en un breve período de tiempo (que suele ser lo habitual en esas situaciones) si hay algún tipo de trabajo previo que si no lo hay. De este modo, se evitará caer en el nerviosismo o la improvisación demasiado presentes en estos momentos.

En el caso de los ciberincidentes es fundamental la función de Responsable de Seguridad de la Información, que será el primero en categorizar el evento y la idoneidad o no de convocar el Comité de Crisis.

Por otra parte, si con anterioridad a una crisis, las organizaciones se han labrado una **reputación** con valores explícitos que han respetado durante toda su actividad, superarán en confianza, credibilidad y capacidad de empatía a las que no lo hacen. Dará igual si es una organización grande o pequeña, si su historia está basada en unos principios éticos y profesionales, les será mucho más sencillo ganarse la confianza de todos sus grupos de interés y, por tanto, de superar la situación.

La toma de decisiones debe partir de la alta dirección que es la única que tiene la capacidad de asegurar los recursos materiales y humanos necesarios, así como de los distintos niveles de toma de decisiones. En el caso de los ciberincidentes es fundamental la función de **Responsable de Seguridad de la Información,** que será el primero en categorizar el evento y la idoneidad o no de convocar el **Comité de Crisis**, asumiendo que la pronta notificación del mismo no sólo beneficia a la propia organización, sino que redunda en un incremento de la seguridad general, de sector y del país, por lo que su realización es un compromiso ético ante la sociedad.

BP.2 Planes y protocolos estructurales

Las crisis se preparan en tiempos de normalidad. Todo lo que no se prevea entonces es prácticamente imposible improvisarlo durante la emergencia. Es verdad que la prevención perfecta es prácticamente inalcanzable: el riesgo cero no existe; pero una de las claves para una gestión efectiva de la crisis viene determinada por la capacidad de **anticipación e identificación de los ámbitos más vulnerables** (**gestión de riesgos**) que pueden llegar a transformarse en situaciones críticas. La identificación de estos riesgos potenciales en el negocio será clave para, llegado el caso, saber cómo responder y reducir su impacto lo máximo posible.

Las crisis se preparan en tiempos de normalidad.

Desde este punto de vista, las ciberamenazas exigen un **constante ejercicio de prospectiva** para ser conscientes de las debilidades de la organización y, de esta forma, poder preparase y anticiparse.

En muchos análisis de crisis se constata que el principal problema es que **el riesgo que la ha desatado no había sido considerado** y, por lo tanto, no había habido una planificación rigurosa para gestionar dicho riesgo, dejando a la organización en un estado de permanente vulnerabilidad.

En este sentido muchas organizaciones (así lo recogen por ejemplo estándares internacionales como la ISO 27001 y 22301 para la implantación de un SGSI[4]) confeccionan **Planes de Gestión de Crisis**, siguiendo diversas metodologías como la de BCM[5], donde se indican las tareas necesarias que permitirán tener la capacidad de gestionar una crisis e identificar las principales acciones a ejecutar para dar respuesta a una situación grave o un desastre. Estos planes suelen contar un **Manual de Crisis** que sirven como marco de referencia para, llegado el caso, contar con un guion de las acciones a llevar a cabo en materia de continuidad, contingencia, comunicación, recursos humanos, etc., con una asignación clara de responsabilidades.

Dichos Planes deben ser convenientemente difundidos entre la propia organización y sus responsables a través de ejercicios o sesiones formativas sobre los mismos.

BP.2

4 Sistema de Gestión de la Seguridad de la Información que recoge un conjunto de políticas, procedimientos y directrices para una correcta protección de los activos de la información de cualquier organización.
5 Del inglés *Business Continuity Management* (BCM), un programa integral que incorpora la continuidad del negocio, la recuperación de desastres y la gestión de crisis.

Un **Comité de Crisis** debe ser el máximo órgano decisorio para la gestión unificada de una situación de crisis y tendrá que estar previamente definido. Su principal cometido será acelerar el proceso de toma de decisiones para solventar incidencias, definiendo las prioridades, estableciendo la estrategia y la táctica a seguir. Deberá fijar los principales escenarios a tener en cuenta, cómo actuar y cómo contarlo, dirigiendo todos los equipos de recuperación y comunicación.

Figura 4. Comité de crisis

Debe estar compuesto por un grupo pequeño de personas con distintos perfiles, ejecutivas y muy resolutivas, con capacidad de reacción ante situaciones de estrés y agilidad en la dirección de los equipos y toma de decisiones. Estará liderado por el Responsable del Comité de Crisis, figura con máxima capacidad de decisión (CEO de la compañía o máximo responsable del organismo, en caso del sector público). Junto a ellos deberían tener representación cada una de las áreas básicas en una organización: Responsables de Seguridad de la Información (RSI), Infraestructura, Procesos, Recursos Humanos, Legal y Comunicación. Porque la gestión de una crisis, aunque su origen sea un ciberincidente, no es algo exclusivo del equipo de seguridad, sino que implica a toda la organización.

Será este Comité el que decida si se está ante una crisis o no, su nivel o grado (en función de los niveles previamente acordados), el establecimiento de las medidas y el reparto de responsabilidades, así como los distintos niveles de comités, con diversos responsables en cada caso; desde el operativo que debe contener y resolver el incidente, hasta el de coordinación y comunicación que velará por la reputación de la organización, establecerá la política informativa, con los mensajes más adecuados y los canales oportunos.

BP.3

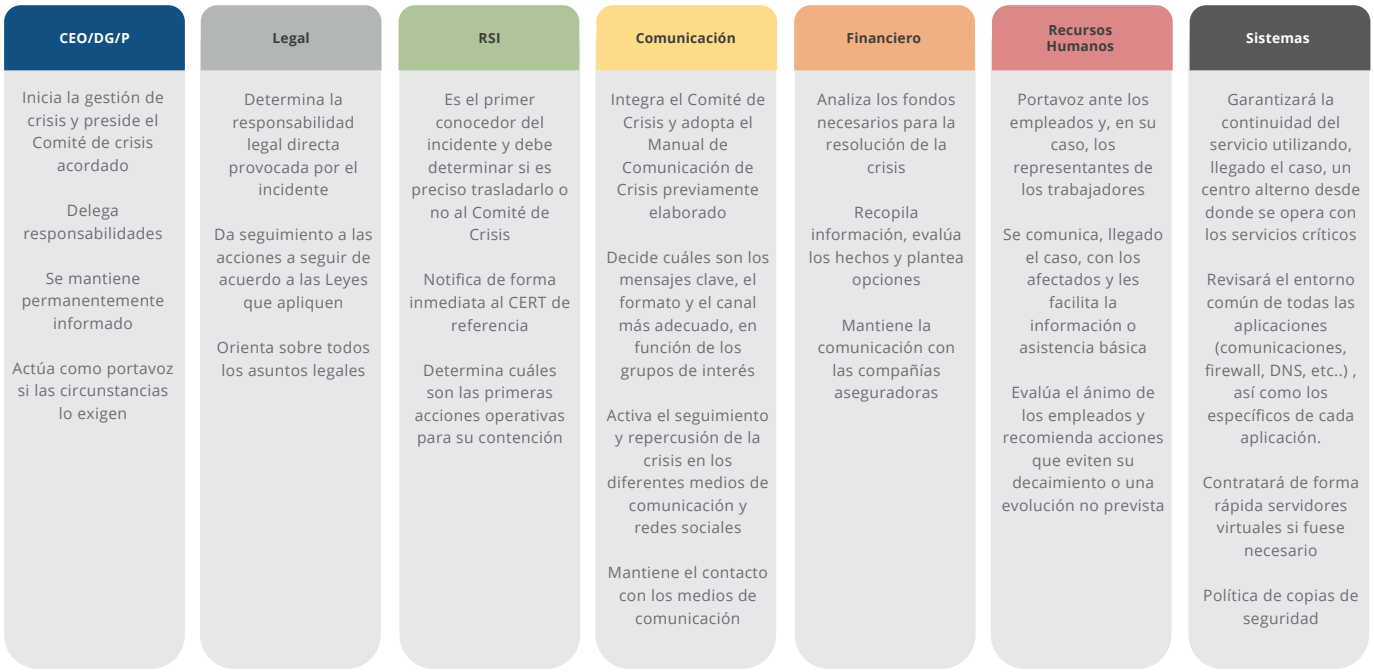


Figura 5. Comité de Crisis y sus responsabilidades

Desde el punto de vista operativo cabe esperar que en función del nivel del ciberincidente establecido en base a los criterios de peligrosidad e impacto se haya establecido previamente el Comité adecuado para su gestión.

A modo orientativo y aunque depende del tamaño y de las capacidades de la organización, un esquema de gestión es el siguiente.

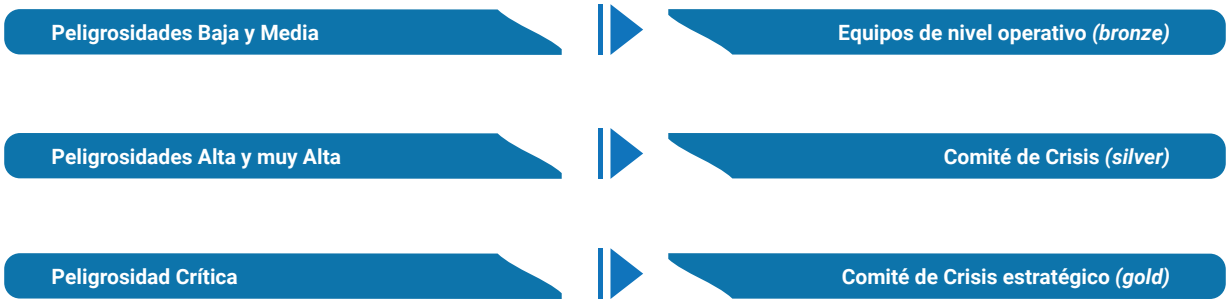


Figura 6. Comité de Crisis según el Nivel

En realidad, los incidentes con peligrosidad baja y media no deberían requerir la convocatoria de un comité de crisis, porque no estamos ante una situación que se pueda definir como tal. Bajo la responsabilidad directa del RSI, los equipos técnicos tienen el conocimiento suficiente para solucionar el problema desde un punto de vista operativo.

Esta configuración de comités no es excluyente, la constitución de uno de los niveles superiores implica, en general, el mantenimiento de la actividad de los anteriores. Es decir, en un ciberataque de categoría crítica la cúpula de la organización (Consejero/a Delegado/a, Dirección General y miembros previamente designados) será quien tome las decisiones finales dentro del Comité *gold* según las aportaciones tanto del comité *silver*, compuesto -por ejemplo- por representantes de direcciones funcionales y con probablemente más de un equipo *bronze* trabajando en aspectos operativos, muy especializados y concretos. En cambio, otros ciberincidentes requerirán sólo la intervención de un comité *bronze* quizá con implicación puntual del *silver*.

Cuando la organización es grande, la misma dimensión y la complejidad normalmente asociada a sus operaciones justifican la existencia de los distintos niveles de comités mencionados, mientras que compañías pequeñas o medianas dispondrán un único Comité de Crisis.

En este sentido, decidir sobre qué nivel de la organización y sobre qué estructura ha de recaer la gestión es también un elemento a considerar para decidir el nivel del incidente/crisis.

Establecido / Origen	Atributo	Nivel 1 BAJO	Nivel 2 MEDIO	Nivel 3 ALTO	Nivel 4 MUY ALTO	Nivel 5 CRÍTICO
Otros atributos de Gestión de Crisis	Declaración de Crisis	No	No	Opcional	Sí, Nivel Muy Alto	Sí, Nivel Crítico
	Ámbito de gestión / Gobierno de la crisis	No requiere Comité de Crisis / RSI / Equipo Respuesta Incidente	Sí requiere Comité de Crisis / BRONZE TEAM	Sí requiere Comité de Crisis / SILVER TEAM	Sí requiere Comité de Crisis / SILVER TEAM	Sí requiere Comité de Crisis Alta Dirección / GOLD TEAM

Figura 7. Criterios de gestión

BP.4 Control permanente de la superficie de exposición

Un elemento clave en la gestión de crisis es poner constantemente a prueba los planes, procedimientos y configuraciones diseñadas. Debe realizare a través de iniciativas para la evaluación de la superficie de exposición de las entidades, identificando las vulnerabilidades asociadas a sus servicios y aplicaciones.

En esta aproximación, el objetivo esencial es promover la confianza de los ciudadanos en la utilización de los medios electrónicos, al tiempo que se promueve su uso de una manera segura donde la superficie de exposición a la ciberamenaza sea medible, controlada y adaptada al ecosistema en cuestión: sector público, infraestructuras críticas, centros de investigación, universidades, sector salud, etc...

Un elemento clave es la evaluación de la superficie de exposición de las entidades, identificando las vulnerabilidades asociadas a sus servicios y aplicaciones.

En definitiva, lo que es sentido común, ser capaces de medir la seguridad. Si medimos podemos gestionar y si gestionamos avanzamos buscando un equilibrio entre las capacidades y funcionalidades que nos brinda la tecnología y un empleo seguro de la misma.

Por otro lado, hay que tener en cuenta que el enfrentarse a una crisis es esencialmente un ejercicio de gestión que involucra equipos humanos de distinta índole (intervención física, asignación de recursos, comunicación interna y externa, gestión de stakeholders, coordinación, etc.) y que para que un equipo rinda adecuadamente en el momento de máxima exigencia debe estar bien entrenado. Por ello es aconsejable la realización periódica de **simulacros** de distinto tipo (operativos o de sobremesa) que sometan sus componentes a las situaciones de gestión que con toda probabilidad la crisis les impondrá, de modo que en un entorno de incidencia simulada el equipo se ejercite y se hagan aflorar mejoras de distinto tipo para que estén disponibles en una situación real.

BP.4

BP.5 Gestión adecuada de grupos de interés. Stakeholders

Los grupos de interés o ***stakeholders*** son personas o colectivos del entorno de la organización que se pueden ver afectados por cualquier actividad que esta realice. Durante una cibercrisis es muy probable que haya interacción con alguno de ellos, por ser parte activa de la situación o incluso por ser parte tanto o más afectada que la propia organización.

Por esta razón se aconseja desarrollar el denominado "**Mapa de *stakeholders***" donde los distintos niveles jerárquicos de la organización deben identificar aquellos a los que puede afectar la crisis.

La visión tradicional de los grupos de interés ha comprendido clientes, proveedores y poderes públicos, además de los propios accionistas (*shareholders*). Hoy en día –y, una vez más, como consecuencia de la ubicuidad de las posibilidades de comunicación y el peso de la opinión pública- hay que considerar grupos adicionales en función de tres grandes áreas y, por supuesto, en función de la actividad de la organización:

Grupos

- **Internos** ····· *miembros del Consejo de Administración/accionistas, empleados actuales y anteriores por categorías y departamentos; familiares y representantes sindicales.*
- **Externos** ····· *autoridades y gobiernos, organismos reguladores y supervisores, CERT o CSIRT[6] de referencia, Agencia Española de Protección de Datos, clientes, proveedores, pacientes, público en general, inversores, compañías de seguros, asociaciones, competencia, prescriptores, etc.*
- **Medios de comunicación** ····· *incluyendo los tradicionales y los online (redes sociales, blogs, etc).*

En función del incidente habrá que revisar todos los grupos de interés, sus expectativas y la estrategia a seguir con cada uno de ellos.

En el caso concreto de los ciberincidentes toman una **importancia fundamental** los Grupos de Respuesta a Incidentes de Seguridad: **CERT** que proporcionan servicios de soporte y gestión ante este tipo de eventos. En algunos casos, y en función de la peligrosidad o su impacto en la organización, la notificación al CERT de referencia es obligatoria. Por ejemplo, en España, todos aquellos incidentes catalogados con una peligrosidad de Alto, Muy Alto o Crítico[7], dentro del Sector Público, deben ser notificados al CCN-CERT, del Centro Criptológico Nacional. Dicha clasificación

6 CERT (*Computer Emergency Response Team*) y CISRT (*Computer Security Incident Response Team*) son términos empleados para referirse al mismo tipo de Equipos o Capacidades. El término CERT está registrado por CERT Coordination Center (CERT/CC) por lo que es necesario tener su permiso para su utilización.
7 Dentro de una escala de cinco valores: Bajo, Medio, Alto, Muy Alto y Crítico.

se realiza en función de diferentes criterios como, el tipo de la amenaza, su origen, los sistemas y usuarios afectados o el impacto que el incidente puede tener en la organización[8].

Más allá de esta notificación es **indispensable ser conscientes de su disponibilidad** y de su **función garante de la seguridad de la información** tanto a nivel de la compañía individual como del tejido organizacional e institucional del país.

Hay que tener en cuenta que al ser la misión de los CERT el constituirse como **recurso permanente de ciberseguridad**, sus conocimientos y los medios de actuación de que disponen están en **constante actualización**.

En este contexto, otro grupo de interés fundamental es la **Autoridad competente** que gestiona la ciberseguridad a nivel nacional. Como se comenta en la BP7 sobre Coordinación, en determinadas situaciones la organización está obligada a notificar el incidente. Por esta razón, es una buena práctica tener prevista esta comunicación: el organismo pertinente, la información a aportar, etc.

Otra cuestión es la afectación para la propia organización de un ciberincidente que genere una crisis en un proveedor relevante. La dependencia de la cadena de suministro es algo que debe estudiarse y, en determinados casos, exigirse certificaciones o garantías a los proveedores respecto a su protección frente a ciberataques. La Figura 8 resume las estrategias genéricas de gestión de proveedores en materia de ciberseguridad.

Figura 8. Estrategias de continuidad en la cadena de suministro

8 Véase: Clasificación/Taxonomía de los ciberincidentes. Guía CCN-STIC 817 Gestión de Ciberincidentes (ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html)

BP.6 Diagnóstico inicial y escenarios posibles

El primer paso en la gestión y posterior resolución de una cibercrisis es llevar a cabo un **diagnóstico**[9] de lo que está sucediendo. En el análisis de crisis reales muy a menudo se observa que por no disponer de un diagnóstico inicial la organización muestra un comportamiento errático durante la emergencia, pierde la iniciativa, va a remolque de los acontecimientos y sufre una clara pérdida de reputación.

A pesar de que, en los primeros momentos de la crisis, la información es a menudo confusa e incompleta, es muy importante entender lo que está pasando y sus posibles afectaciones a corto y medio plazo (posibles escenarios). Este ejercicio permite **priorizar actuaciones y tomar las primeras decisiones**; y a medida que se disponga de más información se irá afinando el proceso.

En la fase de diagnóstico, además, es muy necesario clasificar la crisis en curso según su gravedad percibida y posible impacto de modo que puedan anticiparse decisiones de gestión posteriores. Para ello es imprescindible **definir previamente un esquema de clasificación y escalado de los incidentes**. Este esquema debe incluir niveles de gravedad e impacto, así como los criterios de evaluación y clasificación a utilizar.

En el Anexo 4 se muestra un ejemplo de **criterios de evaluación y clasificación** que puede servir de inspiración para dicho diseño, tomando como punto de partida los establecidos para la clasificación del Nivel de peligrosidad y del Nivel de impacto potencial de la Guía de Seguridad de las TIC CCN-STIC 817 y de la Guía Nacional de Notificación y Gestión de Ciberincidentes[10], a los cuales se añaden a modo de sugerencia otros posibles conceptos a considerar que ayudan a discernir la naturaleza crisis y la conveniencia de activar el respectivo comité de crisis.

Este primer diagnóstico se debe incluir la **notificación inicial al CERT** de referencia para recibir soporte alineado con el problema, indicaciones de actuación específicas y herramientas de diagnóstico y operación complementarias y actualizadas. Todo ello permite una reacción rápida que, en muchos casos, o bien atajará el ataque en su totalidad o limitará de un modo importante sus impactos sobre la organización y sobre el tejido empresarial afectado.

Según la naturaleza de la organización afectada y del tipo de incidente que se esté dando puede haber obligación de hacer esta notificación[11]. En este caso las autoridades competentes podrán pedir toda la información sobre el incidente que consideren necesaria para su resolución y para la minimización de su impacto sobre la seguridad nacional[12].

9 Si es posible acertado, pero lo más importante es hacerlo ya que supone un ejercicio prospectivo que permite anticipar ámbitos de actuación que el mero enfoque en el problema a tratar no facilita.
10 Guía Nacional de Notificación y Gestión de Ciberincidentes y la ya citada Guía CCN-STIC 817
11 Por la Directiva NIS, transpuesta al ordenamiento jurídico español mediante el Real Decreto-Ley 12/2018, de 7 de septiembre, para los Operadores de Servicios Esenciales, o por la RGPD en caso de fuga de datos.
12 En algunos casos, dada la gravedad o la situación mediática del ciberincidente, se ha activado la Comisión Permanente de Ciberseguridad, como órgano supremo a nivel nacional donde se han tratado determinados ciberincidentes.

BP.7 Coordinación

La coordinación es la clave de la buena resolución de una cibercrisis. Incluso organizaciones que se han preparado adecuadamente para abordar una situación grave de este tipo tienen tendencia a improvisar. **Y la improvisación y la falta de coordinación son ingredientes de una receta para el fracaso.**

Por esta razón, el disponer de un **Comité de Crisis,** tal y como se ha reseñado anteriormente, con experiencia y capacidad de gestión es uno de los primeros y más importantes pasos a seguir durante una crisis, pues estas personas serán las que asuman y asignen responsabilidades, competencias y recursos para solucionar el problema.

Esta coordinación es indispensable en la toma de decisiones y su ejecución, así como en las tareas de comunicación, por lo que la figura del portavoz de este Comité es muy relevante.

En la actuación más operativa, aparece como fundamental la figura del **Responsable de Seguridad de la Información** (RSI) ya que sobre ella pivotará esta coordinación al ser el punto de contacto de los **equipos operativos de actuación** (*bronce*[13]), el propio **Comité de Crisis** (*silver* o *gold*) y el **CERT de referencia**.

Por otro lado, en este contexto es importante mencionar que las cibercrisis en muchos casos implican pérdida de informaciones confidenciales cuya gestión está sujeta al Reglamento General de Protección de Datos (RGPD). Por esta razón es una buena práctica que, además del RSI, en la resolución de la crisis esté también directamente involucrada la figura **Responsable del Tratamiento de Datos**, formando parte del Comité de Crisis para asegurar que la información confidencial recibe el tratamiento adecuado y asegurando la correcta coordinación con el resto de miembros.

Esta coordinación viene en gran medida condicionada por aspectos tales como:

Aspectos

- *Los valores de la organización y su cultura, es decir, que dichos valores sean compartidos.*
- *El trabajo previo realizado para identificar riesgos y determinar planes de acción que, inevitablemente, incorporan la necesidad de coordinación.*
- *El grado de ejercitación del comité y su buena dinámica de equipo.*
- *La existencia de una relación madura con los stakeholders, lo cual facilita las tareas de coordinación con los distintos agentes de la crisis.*

Se observa, por lo tanto, que **la gestión de crisis es una disciplina holística** que va más allá de la existencia de herramientas y recursos específicos (manual de crisis, comités ...) y que bascula alrededor de una **conciencia del riesgo ciber** y de una **cultura general de cobertura** de este y otros riesgos que se identifiquen.

13 Ver Anexo 6 para las definiciones sobre los tipos de comités.

BP.8 Iniciativa y proactividad

Del análisis de la gran variedad de cibercrisis se observa que, en muchos casos, el ciberataque encuentra a la organización con falta de tensión para cambiar su prioridad desde el día a día y hacia la crisis. No realiza un diagnóstico adecuado y pierde un tiempo inicial que, por una parte, da ventaja a los agresores al no asegurar **la rápida intervención del CERT** y, por otra, hace que vaya a remolque de los acontecimientos.

Esto supone la adopción de una **política esencialmente reactiva**, más enfocada a dar respuesta a las críticas o presiones que se reciben del entorno que a definir y comunicar la estrategia que se adopta para solucionar la situación.

Por estas razones es tan importante que, ante un primer aviso de crisis, la organización **reaccione con rapidez y contundencia** haciendo una **notificación inicial sin dilación indebida** y tome la iniciativa. Se trata, por lo tanto, de que la organización sea proactiva y no reactiva, que tome sus decisiones con rapidez y que se posicione para liderar la gestión de la crisis.

Un aspecto que demuestra iniciativa y proactividad ante los ciberriesgos lo constituye el que la organización -en el caso de que no disponga de recursos propios- tenga con antelación acordada una intervención rápida por parte de una empresa de servicios especializada ante un ciberataque. De este modo, la actuación de esta empresa, que conocerá los sistemas y protecciones de la organización, permitirá -en coordinación con el CERT de referencia- una muy rápida actuación, lo cual es imprescindible en este tipo de situaciones.

Del mismo modo que se ha comentado en la BP-7 sobre coordinación, la incorporación en las actuaciones del conocimiento especializado del CERT facilita la toma de conciencia y la proactividad. Todo ello es patente en los casos descritos en los anexos.

BP.8

BP.9 Discurso unificado y fuente oficial de información

Una vez que se haya considerado que un incidente ha pasado a la categoría de crisis es fundamental proceder a la elaboración de la información más adecuada teniendo en cuenta: tiempo o prioridad y grupo de interés (stakeholder). En función de estos dos parámetros, y asesorados por el área de Comunicación, se definirán el tipo de información a ofrecer, los mensajes clave, el formato y el canal o medio (reuniones informales, videoconferencias, correos electrónicos, listas de distribución, llamadas, intervenciones presenciales, discursos, juntas de accionistas, *Dark Site*[14], mensajería como WhatsApp o Telegram, etc.)

No hay que olvidar que lo mejor que puede pasar en una crisis, es que la principal fuente de información sea la **propia organización**. Para que esto ocurra es imprescindible que la compañía sea proactiva y lleve la iniciativa, aunque sin caer en la precipitación. Además, es muy importante que el Comité de Crisis fije unos mensajes claros de los que nadie de la organización debería salirse, por lo que sea cual fuere el formato y canal escogido, la información será la misma, sin caer en contradicciones.

Lo mejor que puede pasar en una crisis, es que la principal fuente de información sea la propia organización.

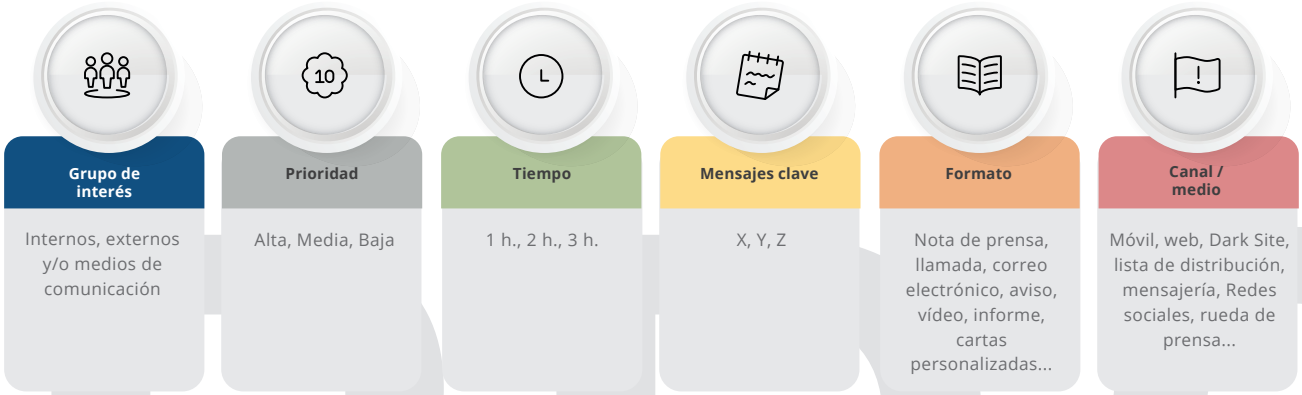


Figura 9. Matriz de ejemplo a la hora de planificar la comunicación de crisis[15]

14 Sitios web confeccionados de cara a la irrupción de una posible crisis que puede dañar la imagen y la reputación de una organización, pero que no son visibles públicamente hasta que se presenta alguna dificultad en la que se decide poner online. Sus objetivos son:
-Estar preparado para reaccionar inmediatamente en el caso de que una crisis irrumpa.
-Proteger y mantener el funcionamiento normal del sitio web de la organización.
Tener un sitio al que puedan dirigirse todos los públicos involucrados en una crisis (periodistas, autoridades, familiares, entre otros).

15 Carles Montaña. Taller de Comunicación de Crisis. Escuela de Periodismo UAM-El País

Dichos mensajes deben tener las siguientes características:

- *Nunca se debe negar la realidad. No mentir nunca y ser transparentes*
- *Dar siempre la versión de la organización, situándose como la fuente de información más creíble y precisa*
- *Transmitir confianza. Actuar con serenidad, firmeza y profesionalidad*
- *Demostrar una cuidadosa atención, respeto y un compromiso total hacia todos los involucrados*
- *Pedir disculpas y asumir las responsabilidades si fuese necesario (no culpar a otros)*
- *Poner en valor todas las acciones realizadas*
- *Asegurar que la actividad/negocio es viable*

Proactividad y discurso unificado

Por lo tanto, **proactividad y discurso unificado** son componentes muy importantes de la política comunicativa que debe tener en cuenta no sólo la información externa (medios de comunicación, web, redes sociales, etc.) sino también que esa unicidad de mensaje se practique también internamente, hacia el propio personal, proveedores y/o clientes. Hay que tener muy presente que, en caso de crisis, cualquier empleado de la compañía puede actuar -voluntaria o involuntariamente- como fuente de información sobre lo que está sucediendo.

Para el caso de ciberincidentes hay que considerar de un modo especial la necesidad de un **equilibrio entre una comunicación externa abierta** -la cual puede advertir a los agresores de que se ha descubierto el ataque y se está actuando, aspecto que quizá no sea conveniente en un primer momento- y el hecho de **compartirlo rápidamente con el CERT de referencia** quien, a su vez, se coordinará con otras organizaciones y estamentos nacionales e internacionales.

Por lo tanto, es importante diseñar un **discurso único** y, a la vez, modular el ritmo y la cadencia en su comunicación.

BP.10 Transparencia, empatía y asunción de responsabilidades

Tal y como se ha señalado, la mentira, la narración sesgada de los hechos, el mutismo o la pasividad son las peores opciones comunicativas cuando ocurre un ciberincidente. Para proteger la reputación de la organización debe evitarse la incertidumbre. Esta actitud es también relevante en la rápida notificación al CERT de referencia ya que ello redunda en un beneficio global.

En general, una sociedad madura acepta que a una organización las cosas no siempre funcionen como se desearía y que pueden aparecer imponderables. Lo que no se entiende, ni se acepta, es que sus responsables no reaccionen a tiempo o de forma inadecuada.

Mantener la transparencia durante una crisis no es fácil, pero el daño se puede compensar o minimizar mediante la adopción de una **política abierta y responsable** que, aunque a corto plazo pueda levantar críticas, a la larga produzca una mejora de la credibilidad y reputación de la organización.

Este planteamiento no quiere decir que haya que contar absolutamente todo. Por regla general es preciso ganar tiempo hasta conseguir conocer mejor el alcance de la situación. Por ello, se evitará mencionar las causas del incidente, su responsable, datos que la investigación pueda revelar o las posibles consecuencias para la organización o para otro grupo de interés.

Se evitará mencionar las causas del incidente, su responsable, datos que la investigación pueda revelar o las posibles consecuencias para la organización o para otro grupo de interés.

BP.10

BP.11 Puesta en valor de las acciones adoptadas

Las crisis tienen muchos momentos en los que, a pesar del trabajo intenso y de las muchas actuaciones simultáneas que se están llevando a cabo, no se dispone de resultados que se puedan presentar a la opinión pública y grupos de interés.

En un contexto como el descrito anteriormente de proactividad y transparencia este es un buen momento para **poner en valor todas las medidas tomadas** hasta el momento por la organización, tanto las preventivas (coordinación con el CERT y otras instituciones, desarrollo de planes previamente diseñados, inversión en recursos,), como las correctivas (equipos de intervención, comités de crisis, subcontrataciones, ejecución de contratos, revisión de protocolos, etc.).

De este modo se transmite un mensaje múltiple:

Mensaje múltiple

La organización se preocupa por su entorno inmediato y sus grupos de interés, por ello se preparó con antelación, cuenta con protocolos de actuación, comité de crisis, etc.

A pesar de no disponer todavía de resultados concretos, se está haciendo todo lo posible para conseguirlos mediante el despliegue de medios y recursos, tal y como se había planificado.

Se está trabajando estrechamente con otros organismos, instituciones o autoridades para su pronta resolución.

Por lo tanto, la compañía está haciendo todo lo que está en sus manos para resolver la situación y, en estas condiciones, sin duda se conseguirá.

En resumen, **cualquier crisis representa una oportunidad** para demostrar la capacidad de la organización para solventar una situación compleja, mostrando que la gestión del evento disruptivo está siendo la adecuada.

BP.11

BP.12 Cierre formal de la crisis

La crisis no termina con la Crisis. En muchos casos la presión del día a día hace que estos acontecimientos no se cierren del modo más adecuado. La principal práctica para un cierre correcto es dedicar tiempo y recursos a evaluar los daños y, sobre todo, a recopilar unas **lecciones aprendidas** e implementarlas en la realidad de la organización, así como en comunicar dicho cierre, tanto a nivel interno como externo.

La realización, por lo tanto, de los **análisis pertinentes**, el levantamiento de **conclusiones**, la **definición de un plan de acción** y el **seguimiento de su implantación** son pasos indispensables en el cierre de la cibercrisis y en muchas ocasiones se realizan sólo a medias.

La comunicación posterior sobre las actividades que se llevaron a cabo y sobre el cierre formal del episodio es una buena manera de transmitir, tanto a los *stakeholders* como a la opinión pública en general, el mensaje de que **se aprendió de lo sucedido** y que la organización está mejor preparada para al futuro. También es un buen momento para **mostrar agradecimiento** a toda aquella persona o institución que colaboró en la resolución de la situación.

Esta comunicación no sólo es pertinente de cara al exterior, sino que tiene todo el sentido hacerla en paralelo en **clave interna.** De este modo, se mandan los mensajes de agradecimiento por la labor realizada y de la importancia de estar preparados ante situaciones de este tipo, lo cual potencia el estado de alerta de los miembros de la organización.

La crisis no termina con la Crisis.

BP.12

BP.13 Implementación de lecciones aprendidas

Esta buena práctica está muy relacionada con la anterior y, de hecho, es una extensión de ella. De todos modos, se quiere enfatizar la necesidad de hacer un esfuerzo de resumen de lo sucedido sintetizándolo en **acciones concretas a implementar**. Como se ha indicado, en muchas ocasiones el día a día hace difícil un análisis detallado y la adopción inmediata de las medidas más urgentes y necesarias puede hacer pensar que ya se sacaron conclusiones de lo sucedido y se actuó en consecuencia.

Esa actitud es una reacción muy superficial; es necesario desarrollar análisis en profundidad y **planes de mejora con objetivos concretos y evolución medible**, no estando satisfechos con las relaciones causa-efecto más inmediatas (por ejemplo, "se trató de un error humano" pero ¿por qué la persona se equivocó?) sino buscando también **orígenes sistémicos** del problema que puedan relacionarlo con legislaciones existentes (entonces, ¿se debe ir más allá de lo meramente normativo? ¿se deben buscar nuevas colaboraciones con el regulador?), con buenas prácticas abandonadas (¿por qué se dejó de hacer aquello?), con estructuras comunicativas inadecuadas (¿por qué no nos entendieron? ¿nos explicamos correctamente?), etc.

No conformarse con **explicaciones simples** es una característica que forma parte de los valores de una organización resiliente y, a la vez, es una condición necesaria para conseguir la resiliencia.

En resumen, hay que tratar las crisis como un yacimiento de aprendizaje organizacional, obteniendo conclusiones de lo sucedido mediante análisis en profundidad y ajuste a dichos aprendizajes de los planes de acción e inversión futuros.

BP.13

5. Conclusiones y recomendaciones

Los distintos casos descritos en los anexos reflejan la gestión de la crisis desde el punto de vista del CCN-CERT de manera que se visualiza de un modo muy claro cómo abordar una cibercrisis y la importancia de disponer de un soporte tecnológico adecuado.

Como síntesis de lo expuesto en los casos, se pueden presentar las **conclusiones principales siguientes**:

- Para gestionar una hipotética crisis es necesario haberla previsto, contar con un Comité de Crisis y diferentes planes y manuales para ello e, incluso, realizar ejercicios o simulacros de la misma.

- No existe suficiente conciencia sobre la importancia de la seguridad de la información en las organizaciones, ya sea por no haber aparecido en sus prioridades o bien por una falsa sensación de seguridad provocada por la disponibilidad de recursos (sistemas y protecciones) que resultan ser insuficientes.

- En muchos casos, no existe una persona que asuma de un modo claro la función de Responsable de Seguridad de la Información. Esta función, propia o externa, es indispensable en el mundo actual.

- Es fundamental que la alta dirección de la organización conozca la amenaza en general, el posible impacto sobre el servicio y el grado de preparación y, por lo tanto, sus carencias.

- La inversión en ciberseguridad debe ser una prioridad para las organizaciones. A pesar de la dificultad en calcular su retorno financiero exacto (como en toda inversión en seguridad, sea del tipo que sea), dada la cada vez mayor frecuencia de los ciberataques y el gran impacto que tienen tanto en afectación al servicio prestado como en salvaguarda de la información y reputación de la propia organización, no debe existir ninguna duda en llevarla a cabo.

- En este contexto, hay que disponer de sistemas que, a la vez que proteger, faciliten la gestión ante un ataque (Firewalls[16], SIEM[17], EDR[18]), así como la disponibilidad de recursos humanos (propios o externos) para la supervisión permanente de la red.

- La rápida notificación de un ciberataque al CERT de referencia se muestra como un paso fundamental para la resolución del incidente y la minimización de su impacto.

- La formación y concienciación del personal de la organización es primordial. Muchos ataques se evitan si el personal que trabaja con medios informáticos es consciente de los riesgos que ello supone y de las amenazas que afectan a la organización

- La comunicación es clave para una correcta gestión de una crisis. Tener previamente identificados todos los grupos de interés o stakeholders a los que saber qué decir y cómo en cada momento. Para ello es necesario un único discurso compartido por los distintos miembros de la organización, que se muestre total transparencia a la vez que se asuman responsabilidades si es necesario y que se ponga en valor las acciones realizadas.

- El factor "seguridad de la información" debe ser tenido en cuenta en toda estrategia que la organización adopte. La adopción masiva del teletrabajo durante la crisis del Covid-19 es un ejemplo de ello ya que no todo el mundo tuvo en cuenta ese riesgo al tener que trabajar desde los domicilios. Esto provocó una mayor incidencia de la amenaza.

16 Firewall: Tecnología de hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea el tráfico de computadoras entre redes con diferentes niveles de seguridad, basándose en un conjunto de reglas y otros criterios.
17 SIEM: sistema que permite almacenar los registros (logs) de distintas fuentes de manera segura y correlarlos extrayendo información que podría pasar desapercibida si se analizan los distintos orígenes de la información por separado.
18 EDR: Endpoint Detection Response

Anexo 1.
Caso de estudio Ciberespionaje

La situación geopolítica de los últimos años marca una tendencia creciente en relación con las operaciones de ciberespionaje. Estas capacidades las componen los denominados grupos APT (amenaza persistente avanzada, del inglés *Advanced Persistent Threat*), que consisten en personal muy especializado, con grandes conocimientos técnicos y dotados de muchos recursos económicos y materiales, que llevan a cabo las intrusiones en las redes objetivo para permanecer ocultos durante el mayor tiempo posible y extraer información de ellas. Esta capacidad está dirigida tanto al sector público como al privado, y suele provenir de países que desean mejorar su posición a nivel político, estratégico o económico.

En definitiva, el ciberespionaje es un ciberataque específico y dirigido que intenta ser lo más sigiloso posible y permanecer en el objetivo el mayor tiempo posible, a diferencia del ciberdelito que es más ruidoso ya que busca un beneficio económico a corto y medio plazo.

¿Qué suele suceder en este tipo de crisis?

En el caso más común, los atacantes envían correos electrónicos dirigidos a unos usuarios concretos para engañarles y conseguir que abran el adjunto o enlace dañino incluido. De esta forma, consiguen infectar el equipo del usuario que les permite el control remoto de la máquina y, una vez dentro de la red, intentan progresar por ella. Para ello, ejecutan comandos y/o herramientas adicionales con las que buscan obtener credenciales de usuarios con privilegios de administrador en el dominio y así tomar el control completo de la red de la organización atacada.

También se puede dar el caso de que el grupo APT haya obtenido credenciales legítimas de acceso remoto a los sistemas de la víctima, tales como VPN o sesiones de escritorio remoto.

Cuando el atacante ha conseguido penetrar en la red objetivo, realiza labores de reconocimiento para detectar dónde se ubica la información de su interés y cómo puede acceder a ella para, posteriormente, robarla. Esta extracción de la información puede hacerla mediante el mismo código dañino con el que infectó a los receptores del correo o por vías alternativas, como correo electrónico o servicios en la nube en internet, para dificultar su detección.

Normalmente, la forma de actuar del atacante hace que sea muy difícil detectarlo ya que busca permanecer largos periodos de tiempo dentro de la red objetivo para así poder robar la mayor cantidad de información posible.

Detección de este tipo de ataques

En gran cantidad de casos, la intrusión es comunicada por terceros a la organización. No obstante, es posible que la intrusión sea detectada por el organismo y organización víctima al ver incoherencias o comportamientos extraños en la red.

Objetivo

El objetivo de este tipo de ataque suele ser el robo de información, de tecnología o de cualquier tipo de documentación. Es importante destacar que la actividad de los grupos APT no se limita a atacar a sus víctimas, sino que también comprometen otros sistemas para usarlos como parte de su infraestructura de ataque, bien como servidores de mando y control, bien como máquinas de salto y/o gestión.

Qué debe hacer una organización en este tipo de situaciones

Medidas de prevención para evitar este tipo de ataques:

Como norma general se ha observado que, para penetrar en los sistemas, los grupos de APT obtienen las credenciales de acceso mediante técnicas de phishing o, cada vez en mayor medida, mediante la obtención de credenciales disponibles en internet y la dark web.

Esto es exitoso, en parte, debido a la **mala praxis de reutilización de contraseñas** por parte de los usuarios. No hacen falta operaciones sofisticadas para tener esas credenciales. Al final el error humano es la principal vía de entrada. Por este motivo, resulta imprescindible implementar políticas robustas que incluyan el cambio periódico de contraseñas, así como concienciar y sensibilizar a los empleados de un organismo u organización de las principales amenazas y procedimientos que los ciberatacantes emplean para la consecución de sus objetivos.

Asimismo, la formación y concienciación del personal de la organización es imprescindible. Muchos ataques se evitan si el personal que trabaja con medios informáticos es consciente de los riesgos que ello supone y de las amenazas que afectan a la organización

Recomendaciones en la fase inicial de la gestión de la crisis

Recomendaciones

- *Actuar con prontitud. La rápida notificación de un ciberataque al CERT de referencia se muestra como un paso fundamental para la resolución del incidente y la minimización de sus impactos. Es preciso reseñar que este tipo de incidentes suelen clasificarse con una peligrosidad de Muy Alto y Crítico por su grave impacto en la organización por lo que, en el caso del Sector Público español, debe comunicarlo obligatoriamente al CCN-CERT, tal y como ya se ha mencionado anteriormente.*
- *Se debe mantener una reunión con los responsables de seguridad de la información.*
- *Es necesario avisar a la Dirección de la empresa, así como mantenerla informada con las novedades de la investigación.*
- *Reunión del Comité de Crisis creado previamente al efecto. Será este grupo el que deba gestionar la situación y aplicar los planes dispuestos al efecto.*

Actuaciones que se realizan en la gestión de este tipo de crisis:

Los primeros pasos en la gestión de este tipo de crisis es **detectar desde cuándo está el atacante robando información** para valorar la brecha generada. Para ello se realizan, en la mayoría de los casos, las siguientes acciones:

Actuaciones

- *El equipo de respuesta al incidente analizará los registros (logs) disponibles, fundamentalmente los de los equipos de seguridad perimetral con el intermediario de navegación (proxy) y los cortafuegos corporativos. En este punto es importante tener en cuenta que numerosas organizaciones borran los logs cada poco tiempo y, por tanto, es posible que no se pueda disponer de información completa. Por ello, se recomienda aumentar la capacidad de retención de logs. En algunos casos, las intrusiones se descubren cuando los atacantes llevan mucho tiempo dentro de la red, por lo que disponer de la mayor cantidad de logs posible ayuda a identificar el origen de la infección y a reconstruir las acciones de los atacantes desde entonces. Es tarea del equipo de seguridad de la organización hacer una revisión permanente de esos logs para detectar anomalías.*
    - *Este primer paso exige por parte de la organización una comunicación interna fluida con personal TIC. Puede ocurrir que, para el despliegue de herramientas específicas o acceso a los logs necesarios de los equipos concretos, el equipo de respuesta a incidentes que investiga el incidente necesite el apoyo del personal TIC de la organización víctima. Para ello, y con el objetivo de no dilatar los plazos de tiempo, la organización en cuestión ha de prevenir a estos equipos de esta situación y comunicarles la necesidad de remitir la información solicitada y necesaria para llevar a cabo la investigación a la mayor brevedad posible.*
    - *Será imprescindible disponer de los esquemas y diagramas de red que permitirán descubrir nuevos indicios según avanza la investigación. Se ha de ser tener en cuenta que el análisis de la red para ver movimientos extraños de información entre ordenadores lleva mucho tiempo. Asimismo, será necesario instalar herramientas específicas.*

Si bien se recomienda actuar con prontitud, el principal fallo de una organización ante esta situación sería intentar mitigar la situación con demasiada rapidez. El atacante debe sentirse seguro para actuar con normalidad. Solo así se podrán conseguir evidencias y saber hasta dónde tiene acceso a la red, así como dónde tiene desplegadas puertas traseras u otros mecanismos para reengancharse a la red.

- *En distintas situaciones de este tipo, el CCN-CERT ha comprobado la criticidad de este aspecto. Si el atacante es consciente de que ha sido descubierto puede optar por cesar su actividad temporalmente o por hacer uso de otros medios de acceso desconocidos por el equipo de respuesta al incidente, lo que complica sobremanera la investigación. El cambio de credenciales de acceso al correo no es suficiente para solucionar un incidente de este tipo, por ejemplo.*

- *Ello deriva en una situación compleja: por un lado, se necesita tiempo para conocer hasta dónde tiene el atacante el control de la red; por otro, el representante del organismo u organización quiere corregir la brecha de seguridad lo antes posible.*

- *En este punto es primordial gestionar los tiempos para que se pueda investigar a fondo hasta dónde ha llegado el atacante, su conocimiento de la red y sus diferentes planes para permanecer dentro. Es necesario instalar herramientas de monitorización y disponer de tiempo para estudiar la situación.*

Conocido el alcance, se realiza un detallado plan de mitigación, que debe ser aprobado por la Dirección.

- *En este punto, se debe tener en cuenta que una mitigación muy temprana sin tiempo de investigación suficiente conlleva que no se pueda realizar la limpieza necesaria ante los diferentes planes del atacante.*

- *El plan de mitigación debe ser lo más radical posible y se debe ejecutar en fin de semana para intentar no afectar al normal funcionamiento de la organización. De esta forma, y en general, no se ven afectados los sistemas y para los empleados no hay ninguna variación sobre su actividad: no hay servicios caídos ni sistemas bloqueados.*

- *No obstante, una vez que se decide ejecutar el plan de mitigación los empleados tendrán que cambiar sus credenciales de acceso, después de que se haya actuado.*

- *Puede ocurrir que la dirección no apruebe el plan de mitigación y se decidan tomar unas medidas insuficientes, que podrían provocar un nuevo ataque en el futuro o incluso que el atacante siga activo y con acceso a la red atacada.*

Aprendizajes

Aprendizajes

- *Las organizaciones deben mantener actualizados de forma constante los esquemas y diagramas de red del organismo.*
- *No es suficiente disponer de grandes medidas de seguridad en una organización. Se deben dedicar recursos y personal a monitorizar la actividad sospechosa de un modo continuado.*
- *Es importante que la organización cree un equipo para supervisión de la red que se convierta en un equipo de seguridad de la información, con herramientas y presupuesto permanentes.*
- *Concienciación en ciberseguridad. Es fundamental que la organización conozca la amenaza en general, el posible impacto sobre el servicio y el grado de preparación y, por lo tanto, sus carencias.*
- *La inversión en ciberseguridad debe ser una prioridad para las organizaciones. A pesar de la dificultad en calcular su retorno financiero exacto (como en toda inversión en seguridad, sea del tipo que sea), dada la cada vez mayor frecuencia de los ciberataques y el gran impacto que tienen tanto en afectación al servicio prestado como en salvaguarda de la información y reputación de la propia organización, no debe existir ninguna duda en llevarla a cabo.*

Anexo 2.
Caso de estudio Ransomware

El ransomware ha sido el tipo de código dañino más destructivo en la última década. De afectar a equipos personales, ha pasado a ser una de las grandes amenazas para empresas y para infraestructuras críticas (hospitales, infraestructuras energéticas, etc.).

En los últimos años, las capacidades de este malware han evolucionado, pasando de cifrar únicamente equipos de usuario a bloquear redes complejas con tecnologías heterogéneas, que son las que están presentes en grandes empresas y estructuras de un país.

La popularidad de este tipo de malware, así como el crecimiento de variantes, se debe en parte a lo que se conoce como *Ransomware as a Service*, servicio por el que los criminales facilitan la creación de este código dañino a cualquiera que lo solicite a cambio de un porcentaje de las ganancias que la campaña obtenga.

Sectores como el farmacéutico, el financiero, o el del comercio han sido las víctimas predilectas de los grupos ciber-criminales durante los últimos años, en los que, además de realizar el robo y exfiltración de información, también han provocado la disrupción de actividad infectando con ransomware la red. Además, los atacantes emplean técnicas de extorsión tras la infección de la red para monetizar el ataque, pidiendo un rescate económico para no publicar la información sustraída y/o para descifrar los ficheros afectados por este código dañino.

En este sentido, es importante resaltar que realizar el pago a un grupo criminal NO garantiza a la víctima que sus datos acaben publicados o vendidos en el mercado negro.

¿Qué suele suceder en este tipo de crisis?

Tradicionalmente este tipo de ciberdelitos eran muy ruidosos; se buscaba un beneficio económico a corto plazo. Sin embargo, en estos momentos, los grandes grupos de cibercrimen actúan siguiendo un *modus operandi* más sofisticado, tratando de colonizar la red en primera instancia, localizando los activos vitales de la víctima, exfiltrando la información valiosa para una posterior extorsión y, finalmente, desplegando el ransomware que imposibilite el acceso a la información.

Detección de este tipo de ataques

En la mayoría de los casos, la víctima es consciente de que ha sufrido un ataque relacionado con ransomware debido a la imposibilidad de acceder a múltiples ficheros desde varios equipos o a la inutilización de varios de sus servicios esenciales.

Objetivo

El principal objetivo del cibercrimen es rentabilizar económicamente una infección por varias vías:

- Extorsión directa hacia la víctima amenazando con la publicación de la información sensible sustraída.
- Disrupción en la disponibilidad de la información y de la prestación de servicios vitales para el afectado, ofreciendo el atacante la clave de descifrado de la información para poder restablecer el funcionamiento del organismo.

Qué debe hacer una organización en este tipo de situaciones

Medidas de prevención para evitar este tipo de ataques:

Para prevenir este tipo de infecciones se suele recomendar el seguimiento de políticas de seguridad a nivel de dominio que, por ejemplo, deshabiliten la ejecución de macros en documentos ofimáticos (principal vía de infección de Emotet) y de Powershell en todos aquellos equipos que no lo precisen (limitando así parcialmente la ejecución por parte del atacante de multitud de herramientas)[19].

Asimismo, se recomienda también establecer políticas a nivel de red que permitan controlar granularmente las conexiones que se puedan establecer entre los distintos puntos y equipos de la red, otorgando de esta manera al equipo de seguridad de mayor visibilidad y trazabilidad de todos los eventos generados, detectando en un tiempo oportuno actividad anómala que pudiera denotar un mal funcionamiento o una posible intrusión en la red.

Del mismo modo, la concienciación y sensibilización previa del personal de un organismo u organización es vital para evitar el éxito de este tipo de ataques.

Recomendaciones en la fase inicial de la gestión de la crisis:

Recomendaciones

- *Actuar con prontitud. La rápida notificación de un ciberataque al CERT de referencia se muestra como un paso fundamental para la resolución del incidente y la minimización de sus impactos. El establecimiento urgente de un canal de comunicación con el CERT es clave para comenzar a gestionar el incidente de seguridad.*
- *Se debe mantener una reunión con los responsables de seguridad de la información.*
- *Es necesario avisar a la Dirección de la empresa, así como mantenerla informada con las novedades de la investigación.*
- *Reunir al comité de crisis de la organización que deberá gestionar la situación y aplicar los planes dispuestos previamente. Será este grupo el que decida las acciones a llevar a cabo y si se requiere la formación de un equipo exclusivo para esta situación.*

19 Para tener información más detallada al respecto se recomienda la lectura de los Informes: CCN-CERT BP/04 Ransomware y CCN-CERT IA-11/18 Medidas de seguridad contra ransomware (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html?limit=25&limitstart=25)

Recomendaciones

- *Hay que realizar una primera valoración del estado de la red, equipos, activos y servicios que componen la red.*
- *Suele ser de gran utilidad plasmar en un diagrama la arquitectura de los sistemas informáticos para conocer la situación en el momento de comenzar la investigación. Asimismo, se inventariarían todos aquellos equipos afectados, para tener claro qué información y servicios críticos se encuentran comprometidos.*
- *Elaborar el Mapa de stakeholders y definir claramente a quién hay que notificar este incidente. En este caso, y de manera inmediata para evitar el peligro de infecciones colaterales, se deberá comunicar tanto a los empleados como a todas las conectividades externas de la organización (clientes, proveedores, usuarios, etc). Dependiendo del ámbito de actuación del afectado, tanto si se trata de un organismo público como de una empresa privada que ofrece servicios de IT a terceros, por ejemplo, será necesario contemplar escenarios en los que, tras la pertinente comunicación con los afectados, se proceda a bloquear el acceso que conecta a la víctima con el resto de entidades.*

Es posible imaginar el caso de un Ayuntamiento que presta servicios de cara al ciudadano, como el acceso a datos de carácter municipal (padrón, gestiones telemáticas, etc.), y que tras ser víctima de una infección de ransomware ha de revisar recursos que sean accesibles públicamente y que puedan contener código dañino susceptible de extender la infección.

Asimismo, ciertos organismos públicos delegan algunas tareas como la gestión de nóminas o personal en terceras empresas, con las que comparten recursos en red, accesos por escritorio remoto, túneles VPN, etc. Y es imprescindible tanto bloquear los accesos para evitar la propagación del malware como el alertar al tercero de cara a prevenir o mitigar en una fase temprana cualquier contagio colateral que hubieran podido sufrir.

En el caso de los MSP (*"Managed IT Services Provider"*, por sus siglas en inglés) o empresas proveedoras de servicios IT es aún más crítica la necesidad imperiosa de contactar con todos sus clientes y empresas asociadas de cara a evitar un colapso total que pudiera magnificar el impacto final de la infección.

Actuaciones que se realizan en la gestión de este tipo de crisis:

Actuaciones

Contención de la amenaza

Es necesario contener la propagación del código dañino por la red (cifrado de carpetas compartidas, movimiento lateral a equipos con visibilidad, etc.) para evitar que un potencial atacante remoto con acceso a los sistemas pueda continuar con su actividad (exfiltración de información, despliegue de puertas traseras adicionales, eliminación o destrucción de evidencias, etc.). Para ello, dependiendo del volumen de equipos afectados en la red y su naturaleza, se procederá a bloquear las conectividades de forma física (desconectando el cable de red) o lógica (bloqueando a nivel de Firewall).

Si el Firewall de la organización víctima no realiza una segmentación efectiva de las distintas subredes ubicadas en el parque, un atacante que obtuviera acceso a un sistema de la organización podría tener visibilidad de todos los equipos. Para solucionarlo, se rediseña la

segmentación de la red junto con los administradores de sistemas de la organización, fortificando las políticas existentes en el Firewall del que dispongan, y añadiendo otro cortafuegos adicional para incrementar el nivel de seguridad.

La velocidad con la que se actúa para frenar la infección y evitar un impacto más severo es clave en la resolución del incidente. De la misma forma, la implicación a todos los niveles dentro de la compañía afectada, desde el equipo técnico hasta la alta Dirección, permitirá obtener resultados desde el primer momento.

Detección de la amenaza

Tras la fase de contención, se procede a determinar qué equipos han sido afectados por el código dañino, porque el atacante los hubiera utilizado para pivotar por la red o para cifrar y/o eliminar su contenido.

En este momento, en los casos en los que colabora el CCN-CERT en la resolución del incidente, se procede a instalar el Sistema de Alerta Temprana (SAT) en la salida a Internet del organismo para identificar si, en base a los patrones conocidos por el CCN-CERT, existe tráfico categorizado como dañino en la red, de manera que se pueda actuar de forma oportuna para localizar y neutralizar posteriormente la amenaza.

En paralelo, mientras se realiza el análisis forense de los equipos afectados, los ejemplares de código dañino encontrados se remiten a los especialistas en ingeniería inversa, encargados de averiguar cuál es la funcionalidad de cada muestra de malware. Este punto es fundamental para caracterizar la amenaza, saber qué capacidades tiene, qué puntos de persistencia establece en los sistemas, si se trata de malware o herramientas avistadas en otros incidentes, etc.

Mitigación de la amenaza

Además de rediseñar la red segmentando los distintos entornos y de restaurar los equipos afectados (servicio de correo, Controlador de Dominio, servidor de bases de datos, equipos cliente, etc.) se procede a actualizar todo el equipamiento del parque, poniendo el foco en aquellos servicios expuestos de cara a Internet, que son los más susceptibles de ser vulnerados.

En este tipo de ataques, la herramienta Mimikatz es comúnmente empleada durante la intrusión en una red para obtener las credenciales locales y de dominio cacheadas en el equipo infectado. Si las credenciales cacheadas en el equipo infectado son las mismas en el resto del dominio se da por hecho que todos los equipos han sido potencialmente comprometidos. La solución pasa por resetear las credenciales del dominio, una vez reconstruido el Controlador de Dominio junto con el Directorio Activo (AD). Asimismo, se recomienda revisar y proceder con la eliminación de aquellos usuarios con privilegios de administración que pudieran haber sido creados por el atacante.

Por tanto, para mitigar con eficacia la amenaza, y de cara a prevenir futuros casos de infección similares, se sugiere cambiar todas las credenciales en el dominio, tanto en la infraestructura expuesta por la compañía u organismo en la nube (webmails, accesos por VPN, etc.), como a nivel interno (Directorio Activo, administradores locales, etc.). Asimismo, en esta fase, en la que se está acometiendo la tarea de revisión y limpieza del parque de equipos, y de

cara a llevar un control adecuado de los activos que aún no se han revisado, de aquellos que están infectados, y de aquellos que ya se han limpiado, es importante introducir el concepto de red limpia.

Esta red lógica se creará en un direccionamiento interno diferente del que posee la red principal, de la cual se aislará utilizando un firewall, por ejemplo, y su función será ir albergando progresivamente todos y cada uno de los equipos que han sido revisados y limpiados de la red principal. De esta forma se produce una separación idónea que permitirá reconstruir la red sin peligro a sufrir reinfecciones.

Actuaciones

Recuperación de la información y servicios

Tras un incidente de seguridad que ha implicado el cifrado y borrado de activos es fundamental establecer el alcance del impacto sufrido, evaluando qué información se puede recuperar y qué servicios se han visto afectados.

En algunos casos es posible recuperar gran parte de la información que ha sido cifrada, usando copias de seguridad aisladas que no se hayan visto afectadas y a través de la labor forense. Además de ello, es necesario reconstruir los servicios esenciales de la organización que hayan podido quedar dañados, aprovechando en este punto para realizar una instalación limpia y segura que permita una monitorización y trazabilidad más clara de cara al equipo de seguridad.

Aprendizajes

Aprendizajes

Este tipo de incidentes ponen de manifiesto que invertir en seguridad es una necesidad. Lamentablemente, en muchas ocasiones, solo cuando tienen lugar incidentes de esta relevancia se comienza a prestar atención desde la alta dirección a las peticiones que requerían más personal dedicado a la labor de seguridad, que pudiera realizar la labor de monitorización y mantenimiento de los sistemas y redes. Es necesario apostar por un equipo de seguridad preparado, con los medios materiales adecuados, que realice de forma proactiva auditorías en la red y que conciencie a todos los usuarios que hacen uso de los recursos técnicos.

Es imprescindible dotar materialmente al organismo de sistemas de seguridad como Firewalls, SIEM, EDR, etc. para poder llevar a cabo de forma más ágil la labor de velar por la seguridad.

No obstante, no basta solo con disponer de personas dedicadas a la seguridad informática o medios físicos para poder implementar las medidas correctas, sino que se precisa una concienciación profunda de la alta dirección para que, ante situaciones extraordinarias como por ejemplo la del teletrabajo, se establezcan los procedimientos oportunos que aseguren que el trabajo se lleva a cabo con garantías de seguridad equivalentes a las que se tienen cuando se trabaja desde el puesto de trabajo diario.

En general, la experiencia de los últimos años pone de manifiesto que no se tiene una cultura de seguridad que involucre a la alta dirección de los organismos y empresas.

Aprendizajes

- *Hay que adelantarse a lo inevitable, y es que en el mundo de la seguridad informática si bien es casi imposible prevenir una intrusión (ya sea por el desconocimiento de todas las vulnerabilidades que no son públicas, o por el hecho de que el usuario es el eslabón más débil de la cadena) se debe disponer de los medios y personas que permitan detectar con la mayor celeridad posible que un ataque está teniendo lugar, de forma que se puede atajar en una fase temprana un potencial incidente crítico.*
- *Intentar solventar un incidente en una empresa u organismo que dispone de un parque de equipos grande de manera demasiado rápida puede dar lugar a la precipitación en algunas decisiones técnicas. Es importante no pasar por alto posibles puertas traseras adicionales desplegadas por el atacante que le permitan volver a infectar la red en un corto espacio de tiempo.*
- *Trabajar in-situ desde el primer momento con el organismo afectado y disponer de un equipo de personas que tienen claro cuáles son los pasos que hay que seguir para atajar el incidente es el punto fundamental para determinar el éxito en la resolución del incidente.*
- *La coordinación entre todos los implicados es vital para poder explicar de manera sencilla y oportuna en el tiempo los avances de la investigación.*
- *Estos incidentes ponen de manifiesto la necesidad de revisar el diseño de la red, las políticas de seguridad y el método de teletrabajo que se está realizando.*
- *Todas las compañías, y en concreto las que pertenecen al ámbito de infraestructuras críticas o servicios esenciales, tienen que seguir madurando en el ámbito de la seguridad informática para evitar incidentes de seguridad que en última instancia puedan afectar gravemente al servicio que prestan a la ciudadanía.*

Anexo 3.
Caso de estudio Intento de Sustracción de fondos

El grupo atacante conocido como "Carbanak/Cobalt Gang" recibe este nombre por el nombre del código dañino que empleaba en sus ataques: el conocido como Carbanak hasta 2014 y Cobalt Strike Beacon[20] a partir de 2015. Este grupo está activo desde al menos 2014[21] y se estima que hasta el año 2019 ha robado al menos 1000 millones de euros de entidades bancarias en todo el mundo. Inicialmente, su actividad se centró en bancos rusos y ucranianos, pero dada la rentabilidad de sus ataques, pronto expandió sus actividades ilícitas al resto del sector bancario internacional.

20 https://www.cobaltstrike.com
21 Kaspersky Labs – "Carbanak APT, the great bank robbery".

¿Qué suele suceder en este tipo de crisis?

Desde hace unos años, existen grupos cibercriminales con grandes conocimientos técnicos que realizan ataques dirigidos. Una vez han penetrado en la red y obtenido el control de sus sistemas, los atacantes realizan transferencias de fondos a cuentas controladas por ellos mismos en otras entidades.

Para ello, utilizan tácticas, técnicas y procedimientos (TTP) más propios de actores patrocinados por Estados que se dedican al ciberespionaje (los conocidos como grupos APT). Aunque la motivación del ataque no sea la obtención de información sino el lucro económico, los cibercriminales realizan acciones similares a los grupos APT en las redes atacadas: labores de reconocimiento minuciosas para identificar los activos de su interés y labores de aprendizaje para saber cómo los operan los trabajadores de la entidad. Así, pueden replicar sus acciones pasando desapercibidos.

Qué debe hacer una organización en este tipo de situaciones

Medidas de prevención para evitar este tipo de ataques:

Medidas

- *Concienciación del personal: muchos ataques se evitan si el personal que trabaja con medios informáticos es consciente de los riesgos que ello supone y de las amenazas que afectan a la organización.*
- *Creación de un equipo exclusivo para manejar la situación.*

Recomendaciones en la fase inicial de la gestión de la crisis:

Recomendaciones

- *Actuar con prontitud. La rápida notificación de un ciberataque al CERT de referencia se muestra como un paso fundamental para la resolución del incidente y la minimización de sus impactos. El establecimiento urgente de un canal de comunicación con el CERT es clave para comenzar a gestionar el incidente de seguridad.*
- *Es fundamental priorizar todas las tareas relacionadas con la investigación con el apoyo de la Dirección, actuar con prontitud y crear un equipo exclusivo para manejar la situación, que es crucial ante ataques como este. La colaboración total y sincera de la víctima es crucial en compromisos así, ya que es su personal quien conoce la red, qué sistemas la conforman, etc.*
- *Asimismo, suele ser positivo la creación de una célula de crisis a nivel corporativo en la que se involucre el personal mínimo e imprescindible. Esto es importante ya que así se evitan las fugas de información cuando empiezan a correr los rumores. La célula debe informar en tiempo real a la Dirección sobre el estado de la investigación y las medidas que se van tomando. Este punto es crucial, ya que el apoyo de la Dirección es imprescindible para que la información fluya y la investigación llegue a buen puerto, más aún en este tipo de investigaciones en la que una entidad externa solicita información muy sensible sobre la red.*

Actuaciones que se realizan en la gestión de este tipo de crisis:

En primer lugar, se identifican las máquinas que están realizando o han realizado conexiones hacia los servidores de mando y control, para llevar a cabo un análisis forense y así conocer las herramientas y TTP que estarían empleando los atacantes. Estos análisis permiten descubrir que este tipo de ataque empleaba como vector de infección un correo electrónico dañino dirigido (*spear phishing*).

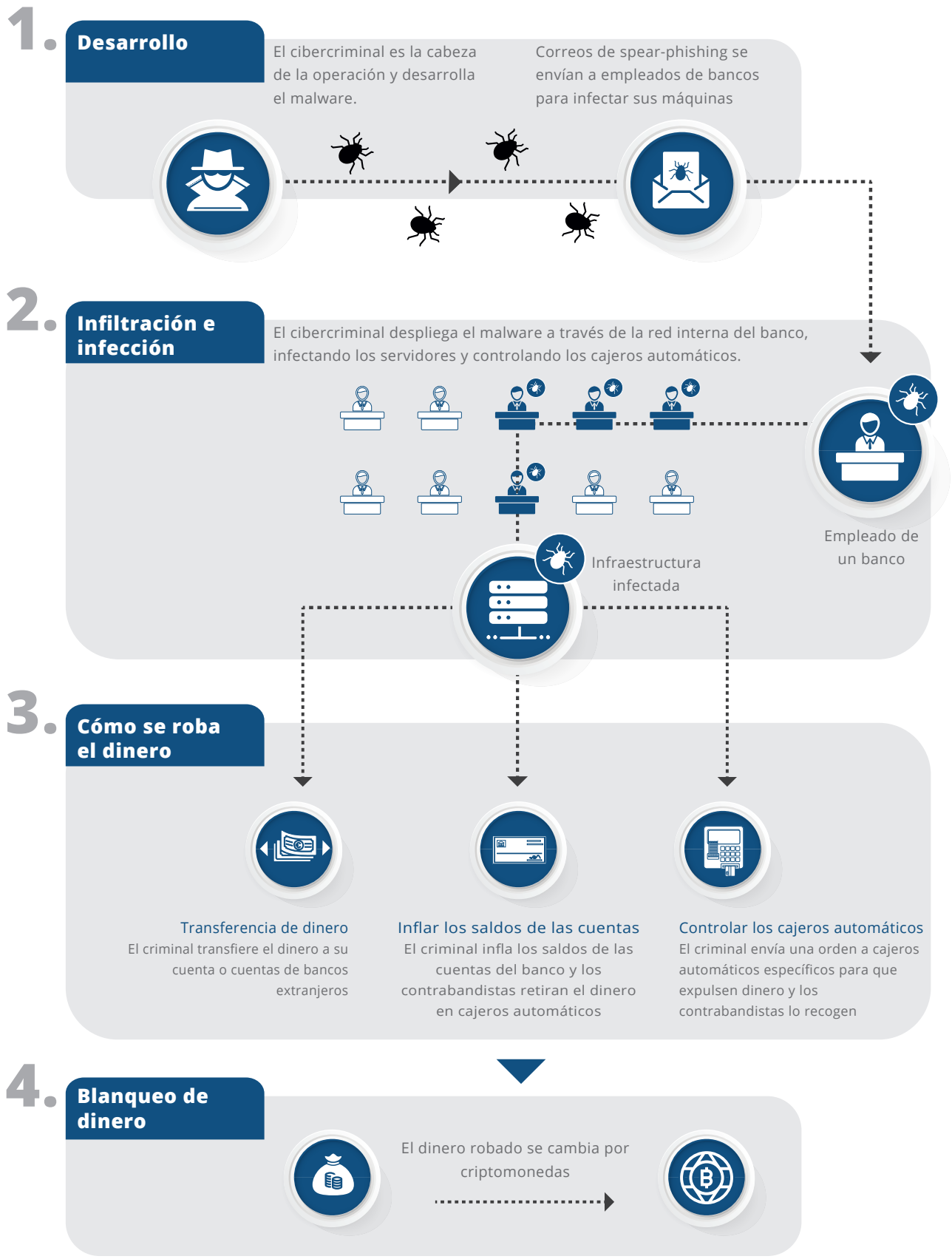
En la mayoría de casos, el correo dañino contiene un fichero adjunto de Word que, una vez abierto, explotaría varias vulnerabilidades de Microsoft Office e infectaría el equipo del usuario con el *malware* que da a los atacantes control sobre dicha máquina.

La instalación del malware da acceso completo y control sobre la máquina a los atacantes. Con el acceso a la red conseguido, los atacantes progresan rápidamente por ella y obtienen en muy corto espacio de tiempo credenciales de usuarios con permisos de administrador de la red, lo que les permite moverse con total libertad e instalar sus herramientas sin problemas.

El ataque seguiría el esquema reflejado en el siguiente gráfico de Europol:

Carbanak / Cobalt

Cómo funciona



Una vez definido el alcance total del incidente, se da paso a la fase de contención y mitigación, en la que se toman las siguientes medidas:

Medidas

- *Desconexión de los servidores principales, lo que paraliza la actividad de la organización durante unas horas. Este punto es importante ya que las medidas se tienen que tomar sin que el atacante tenga acceso a la red.*
- *Reinstalación y plataformado de todos los equipos afectados no críticos. En algunos servidores esto no es posible y se procede a una limpieza manual, eliminando el código dañino y modificando la configuración para securizarlos adecuadamente.*

Aprendizajes

Las lecciones aprendidas a nivel técnico son:

Aprendizajes

- *Necesidad de disponer de un equipo dedicado de seguridad: para evitar este tipo de ataques es imprescindible mantener una monitorización y vigilancia constantes. La seguridad debe afrontarse de forma proactiva, no reactiva. Si la organización no dispone de dicho equipo, no se podrá detectar la intrusión en sus primeras etapas.*
- *Aumentar la capacidad de retención de logs: en algunos casos, las intrusiones se descubren cuando los atacantes llevan mucho tiempo dentro de la red, por lo que disponer de la mayor cantidad de logs posible ayuda a identificar el origen de la infección y a reconstruir las acciones de los atacantes desde entonces. Es tarea del equipo de seguridad mencionado hacer una revisión permanente de esos logs para detectar anomalías.*
- *Segmentación de redes: de esta manera se puede limitar el acceso de los atacantes si éstos consiguen infectar a un usuario que realiza una tarea no esencial.*
- *Aplicación del principio de mínimo privilegio: los usuarios deberán disponer de los permisos estrictamente necesarios para llevar a cabo sus funciones.*
- *Concienciación del personal: muchos ataques se evitan si el personal que trabaja con medios informáticos es consciente de los riesgos que ello supone y de las amenazas que afectan a la organización.*

Aprendizajes

Las lecciones aprendidas para la gestión de la crisis son:

- *Informar lo antes posible, de forma clara, con la máxima transparencia e información disponible a la Dirección. Su apoyo es imprescindible para poder tomar las decisiones y ejecutar las acciones que se requieran.*
- *Formalización de la célula/estructura de gestión de crisis: es imprescindible saber "a quién hay que llamar" en cada momento.*
- *Mantener el control de la información, establecer canales seguros para tratar el incidente en curso de forma que el atacante no sepa que ha sido descubierto hasta que se esté en condiciones de evitar su acceso a la red.*
- *En la mayoría de las ocasiones, las entidades tienen una falsa sensación de seguridad. Disponen de un gran número de productos de seguridad, pero no tienen el personal adecuado para administrarlos ni explotarlos, por lo que apenas les sacan partido.*

Anexo 4.

Orientación sobre niveles y criterios de evaluación y clasificación de cibercrisis

Establecido / Origen	Tipología de impactos	Atributo	Nivel 1 BAJO
CCN-STIC 817	Externo	Afectación a la seguridad nacional	---
	Externo	Afectación a la seguridad ciudadana	---
	Interno	Afectación a infraestructuras críticas/servicio esencial	---
	Interno	Afectación a sistemas	Afecta a los sistemas de la organización
	Interno	Interrupción del servicio	Interrupción de la prestación de un servicio
	Interno	Recursos en jornadas personas	El ciberincidente precisa para resolverse menos de 1 jornadas-persona
	Interno	Impacto económico	Entre 0,0001 % y 0,002 % del PIB actual
	Externo	Afectación geográfica	Superior a 1 CCAA
	Externo	Impacto reputacional	Puntual, sin eco mediático
OTROS ATRIBUTOS DE GESTIÓN DE CRISIS	Interno / actividad / operaciones	Afectación a los procesos críticos	Sin afectación en procesos críticos
	Social	Afectación a las relaciones con los grupos de interés	Las expectativas y la confianza de los grupos de interés no se ven afectadas
	Social	Alarma social	Sin alarma
	Económico	Daños a terceros / entorno	Sin daños a terceros / entorno
	Económico	Pérdidas económicas (estimación)	Sin pérdidas o pérdidas insignificantes. Coste dentro de parámetros presupuestarios aceptables
	Legal	Implicaciones legales	Sin implicaciones
	De gestión	Declaración de crisis	No

Nivel 2 MEDIO	Nivel 3 ALTO*	Nivel 4 MUY ALTO*	Nivel 5 CRÍTICO*
---	---	Afecta apreciablemente a actividades oficiales o misiones en el extranjero	Afecta apreciablemente a la seguridad nacional
---	---	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas
---	---	Afecta a un servicio esencial	Afecta a una infraestructura crítica
Afecta a más del 20 % de los sistemas de la organización	Afecta a más del 50 % de los sistemas de la organización	Afecta a sistemas clasificados RESERVADO	Afecta a sistemas clasificados SECRETO
		Afecta a más del 75 % de los sistemas de la organización	Afecta a más del 90 % de los sistemas de la organización
Interrupción en la prestación del servicio superior al 5 % de usuarios	Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios	Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios	Interrupción en la prestación del servicio superior a 8 horas y superior al 50 % de los usuarios
El ciberincidente precisa para resolverse entre 1 y 5 jornadas-persona	El ciberincidente precisa para resolverse entre 5 y 50 jornadas-persona	El ciberincidente precisa para resolverse entre 50 y 100 Jornadas-Persona	El ciberincidente precisa para resolverse más de 100 Jornadas-Persona
Entre el 0,001 y 0,05 % del PIB actual	Entre el 0,05 % y el 0,07 % del PIB actual	Entre el 0,07 % y el 0,1 % del PIB actual	Superior al 0,1 % del PIB actual
Superior a 2 CCAA	Superior a 3 CCAA	Superior a 4 CCAA	Extensión geográfica supranacional
Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación)	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros	Daños reputacionales a la imagen del país (marca España) y cobertura continua en medios de comunicación nacionales	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales
Con afectación a procesos críticos y recuperación de la actividad interrumpida dentro de su RTO	Recuperación de una actividad interrumpida ligeramente por encima de su RTO (%)	Recuperación de una actividad interrumpida por encima de su RTO (%)	Recuperación de una actividad interrumpida o desconocida o muy por encima de su RTO (%)
Las expectativas y la confianza de los grupos de interés no se ven afectadas	Las expectativas y la confianza de los grupos de interés se verán mínimamente afectadas	Las expectativas y la confianza de los grupos de interés se verán afectadas de manera considerable	Las expectativas y la confianza de los grupos de interés y la relación con estos se verán fuertemente afectadas durante un largo periodo de tiempo
Sin alarma	Principio de alarma en población con/sin causa justificada	Alarma en población con/sin causa justificada	Pánico en población con/sin causa justificada
Daños materiales leves (valoración €?)	Daños moderados (valoración €?)	Daños graves (valoración €?)	Daños muy graves (valoración €?)
Pérdidas por valor hasta coste de reposición	Pérdidas por valor hasta coste de reposición	Pérdidas por valor hasta coste de reposición	Pérdidas por valor hasta coste de reposición
Sin implicaciones	Sin implicaciones	Reclamaciones aisladas de terceros y/o indicios de delito	Reclamaciones masivas de terceros y/o materialización de delito
No	**Opcional**	**Sí, de nivel MUY ALTO**	**Sí, de nivel CRÍTICO**

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

CCN
centro criptológico nacional