

CCN-CERT BP/29

Gestión de crisis para ciberincidentes en entidades locales



CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VAIES-528001551, ou=CENTRO
CRYPTOLOGICO NACIONAL, o=CENTRO
CRYPTOLOGICO NACIONAL, c=ES
2023.03.23 01:37:38 +01'00'

Fecha de Edición: Enero 2023

Institut Cerdà ha participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	4
2. ALCANCE DE LA GUÍA	6
I. ORGANIZACIÓN PARA LA GESTIÓN DE LA CRISIS: MODELO BÁSICO	10
3. ¿QUÉ ENTENDEMOS POR CRISIS? ¿Y POR CIBERCRISIS?	13
4. RESPONSABLES PÚBLICOS EN LA GESTIÓN DE CRISIS POR CIBERINCIDENTE	16
II. PROTOCOLO DE ACTUACIÓN: MODELO BÁSICO	23
5. DE LA GESTIÓN DE INCIDENTES A LA GESTIÓN DE CRISIS	24
6. FASE 1. IDENTIFICACIÓN, CLASIFICACIÓN Y EVALUACIÓN DEL INCIDENTE	27
7. FASE 2. ACTIVACIÓN DEL COMITÉ DE CRISIS	34
8. FASE 3. GESTIÓN Y SEGUIMIENTO DE LA CIBERCRISIS	36
9. FASE 4. CIERRE DE LA CRISIS Y DESACTIVACIÓN DEL COMITÉ DE CRISIS	43
ANEXO 1. PROTOCOLO DE DATOS A APORTAR POR PARTE DEL ORGANISMO AFECTADO POR RANSOMWARE	48
ANEXO 2. PLAYBOOKS DE REFERENCIA PARA RESPUESTA A CIBERINCIDENTES	50

1. INTRODUCCIÓN



Vivimos en un mundo cada vez más complejo y globalizado, más digitalizado y tecnológicamente dependiente, en el que los **ciberataques han ido en aumento**. Hemos de ser conscientes del reto al que nos enfrentamos y de que las entidades locales no pueden quedarse al margen.

En los últimos años los Ayuntamientos, las Diputaciones Provinciales, los Cabildos Insulares, etc., han implementado medidas para que cada vez más **servicios públicos estén disponibles digitalmente**, se depende de internet para las interacciones y transacciones cotidianas, se dispone de un mayor número de elementos tecnológicos, desde aplicaciones móviles y servicios en la nube, así como de una gran diversidad de dispositivos electrónicos, el personal desarrolla una buena parte de sus actividades telemáticamente...

El incremento del uso de los medios electrónicos por parte de nuestras entidades locales hace imprescindible garantizar la protección de sus capacidades tecnológicas, la información tratada y los servicios prestados, los cuales, por su proximidad a la ciudadanía, es imprescindible que mantengan su plena operatividad.

Las entidades locales **son susceptibles de sufrir un ciberataque**, no es cuestión de preguntarse si ocurrirá, sino de cuándo y de si, para entonces, estaremos suficientemente preparados para responder adecuada y organizadamente. No podemos confiarnos: los atacantes seguirán intentando romper las barreras de seguridad para sustraer datos, dañar los sistemas y/o bloquear la gestión administrativa y la prestación de los servicios a la ciudadanía.

Últimamente se ha avanzado mucho en el ámbito de la ciberseguridad, el Esquema Nacional de Seguridad (ENS) ha definido principios y requisitos, se han elaborado Guías para ayudar en la implantación, la seguridad, la gestión de incidentes (la Serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad), sin embargo, **se ha trabajado menos en preparar a los responsables de las entidades locales para el “durante”**. El modelo de gestión de crisis que se presenta en esta Guía se incardina en lo perseguido por el Esquema Nacional de Seguridad (ENS), para su aplicación en las entidades locales¹.

La ciberseguridad es imprescindible, pero la **adecuada gestión de una ciber crisis es también vital para que la ciudadanía confíe en sus ayuntamientos**: todos deben revisar, actualizar y reforzar continuamente su ciberseguridad, pero también deben desarrollar sus capacidades para gestionar una ciber crisis.

Este documento va dirigido especialmente a los cargos y órganos directivos de las entidades locales, ya sean cargos electos o de función pública (Alcalde/sa, Presidente/a de Diputación, Tenientes de Alcalde/sa, Junta de Gobierno Local, Concejales/as, Responsable de comunicación, Secretarios/as, Interventores/as y Tesoreros/as).

Con esta Guía se espera contribuir a mejorar las capacidades de las entidades locales para responder ante un incidente de ciberseguridad relevante y de alto impacto, para gestionar una ciber crisis y volver a la normalidad con las menores consecuencias para las entidades locales, la ciudadanía y sus otros grupos de interés.

¹ El Esquema Nacional de Seguridad (ENS) determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos por parte de las entidades del sector público (y de aquellas organizaciones del sector privado que les presten servicios), estando constituido por los principios básicos y los requisitos mínimos para una protección adecuada de la información tratada y los servicios prestados, de obligatoria observancia por las entidades de su ámbito subjetivo de aplicación, para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Esta **preparación** ha de llevarse a cabo a fin de **generar confianza** y proporcionar garantías de que, en caso de ciber crisis, se está preparado para tomar decisiones, coordinarse con todos los agentes que van a participar en la respuesta y comunicar adecuadamente. Se ha tenido en cuenta, que en las entidades locales el marco de referencia a seguir para organizar las responsabilidades generales en la gestión de la seguridad de la información se debería articular mediante la definición de tres bloques, que se adapta a cualquier entidad independientemente de sus necesidades y limitaciones, en el organigrama:

1. **Bloque de Gobierno:** roles y órganos que conocen la misión del organismo, establecen y especifican los objetivos y requisitos en materia de seguridad de la información y proporcionan los recursos adecuados y necesarios para alcanzarlos.
2. **Bloque de Supervisión:** rol o roles que comprenden las funciones del organismo, contribuyen a la coordinación de todos sus departamentos para alcanzar los objetivos, y supervisan su ejecución.
3. **Bloque de operación:** rol o roles que se centran en el desarrollo, operación y mantenimiento del sistema de información para que se ajuste a los requisitos de seguridad marcados.

En definitiva, se persigue que sea leído y tomado en consideración por todos aquellos que, desde los niveles altos de gobierno de una entidad local, sustentan la responsabilidad de hacer más segura y confiable la administración pública y **más eficiente y eficaz la respuesta en caso de posibles ciberataques**.

2.

ALCANCE DE LA GUÍA

El objetivo de toda entidad local debe ser avanzar hacia la resiliencia, entendiendo ésta por la capacidad de anticiparse, adaptarse y responder para recuperar el estado inicial cuando ha cesado la perturbación a la que se había estado sometido.

Esta Guía se centra en uno de los pilares de la resiliencia: en la necesidad de diseñar, desarrollar e implantar un modelo de gestión de crisis, el cual complementa las capacidades que haya desarrollado la entidad local en prevención de riesgos, en seguridad y en la continuidad de los servicios (ver **Figura 1**).



Figura 1. Los pilares de la resiliencia

Por otra parte, una entidad local resiliente debe contemplar todo el ciclo: prevención, preparación, detección, **respuesta**, recuperación y aprendizaje. Esta Guía muestra **un método** para la gestión de las crisis **cuando éstas ocurren**, es decir, se centra en la respuesta, en el durante (ver **Figura 2**), y para ello se centra en los elementos clave que deben prepararse con antelación y que configuran las capacidades para responder adecuadamente a un incidente de alto impacto.

La Guía tiene **dos (2) partes**:

La primera parte propone un **MODELO BÁSICO de ORGANIZACIÓN** para gestionar ciber crisis y sus elementos clave:

- **Comité de Crisis**: quiénes han de formar parte y de qué se han de ocupar.
- Funciones de los distintos responsables: del/la Alcalde/sa/sa, Presidente/a de Diputación, Tenientes de Alcalde/sa, Junta de Gobierno Local, Concejales/as, Responsable de comunicación, Secretario/a, Interventor/a y Tesorero/a.

La segunda parte propone un **MODELO de PROTOCOLO de ACTUACIÓN** en caso de incidente que puede derivar en crisis:

- **Criterios** de evaluación.
- **Acciones** durante las diferentes **fases** del gobierno de la crisis.

Finalmente, los contenidos de esta Guía se complementan con ejemplos, lecciones aprendidas y buenas prácticas en gestión de crisis, fruto del trabajo de análisis de más de 100 casos reales a nivel nacional e internacional² y fruto de las **lecciones compartidas por entidades locales que han vivido** recientemente un ciberataque de nivel MUY ALTO o CRÍTICO.

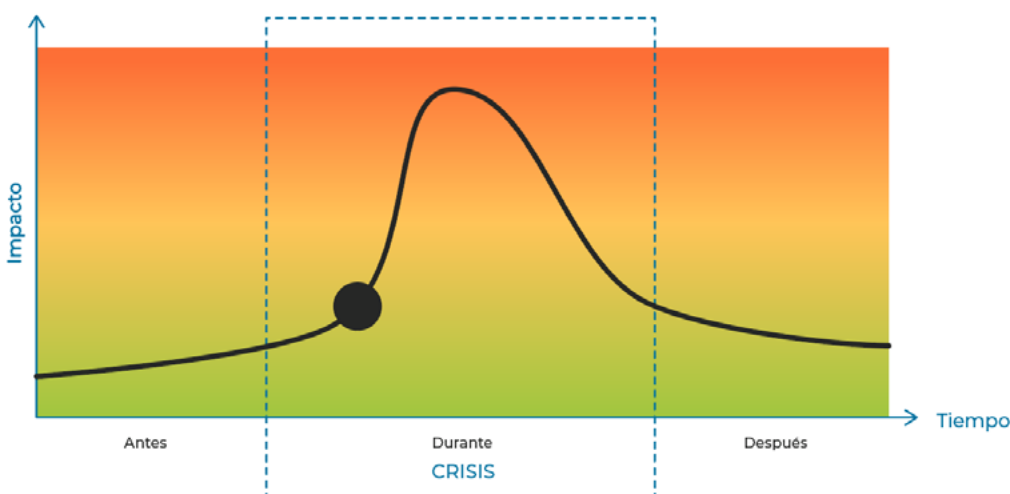


Figura 2 Ciclo temporal de un incidente que deviene una crisis

² Más información en el informe CCN-CERT BP/20 Buenas Prácticas en la Gestión de Ciber crisis

Recursos para la implantación del Esquema Nacional de Seguridad, Serie 800 del CCN e informes:

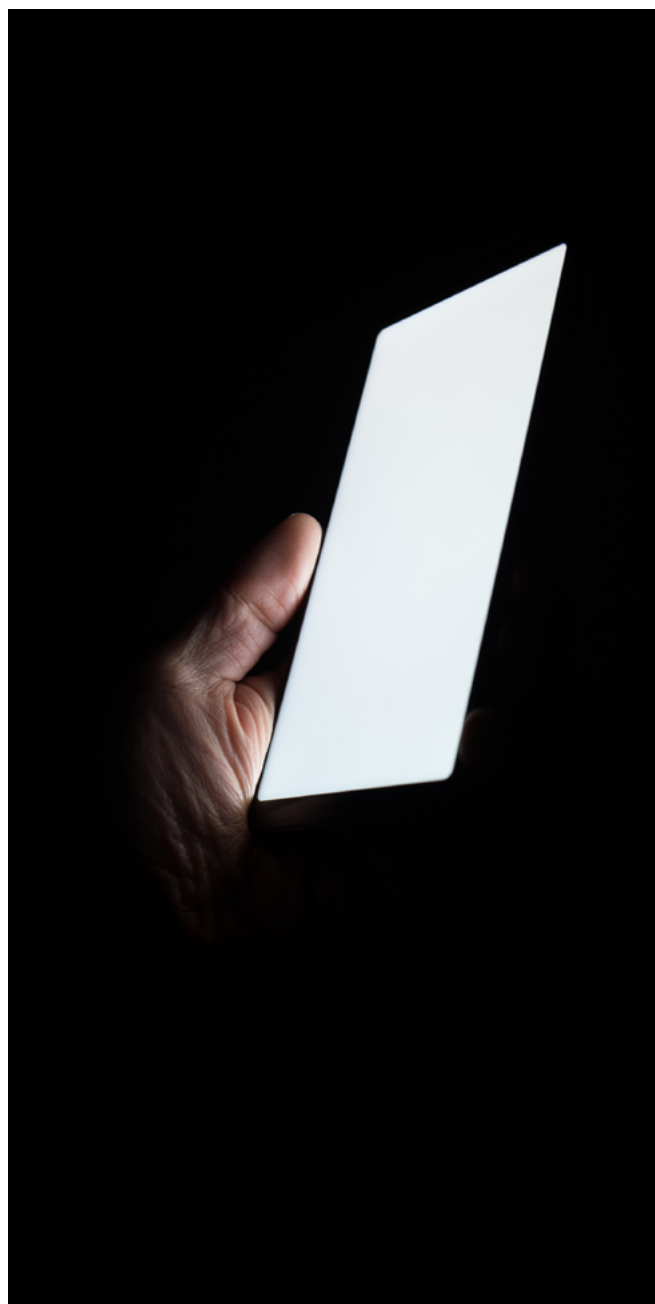
- Aproximación al Marco de Gobernanza de la Ciberseguridad (CCN).
- Prontuario de Ciberseguridad para Entidades Locales del Centro Criptológico Nacional (CCN) y la Federación Española de Municipios y Provincias (FEMP).
- CCN-STIC 800 Glosario de términos y abreviaturas del ENS.
- CCN-STIC-801 Responsabilidades y Funciones en el ENS.
- CCN-STIC-802 Auditoría del ENS.
- CCN-STIC-803 Valoración de Sistemas en el ENS.
- CCN-STIC-804 ENS. Guía de implantación.
- CCN-STIC-805 Política de Seguridad de la Información.
- CCN-STIC-806 Plan de Adecuación al ENS.
- CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS.
- CCN-STIC-809 Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento.
- CCN-STIC-815 Indicadores y métricas en el ENS.
- CCN-STIC-821 Normas de Seguridad en el ENS.
- CCN-STIC-822 Procedimientos de Seguridad.
- CCN-STIC-882 Guía de Análisis de Riesgos para Entidades Locales.
- CCN-STIC-883 Guía de implantación del ENS para Entidades Locales.
- CCN-STIC 890 Adecuación al ENS conforme Requisitos Esenciales Seguridad según μ CeENS

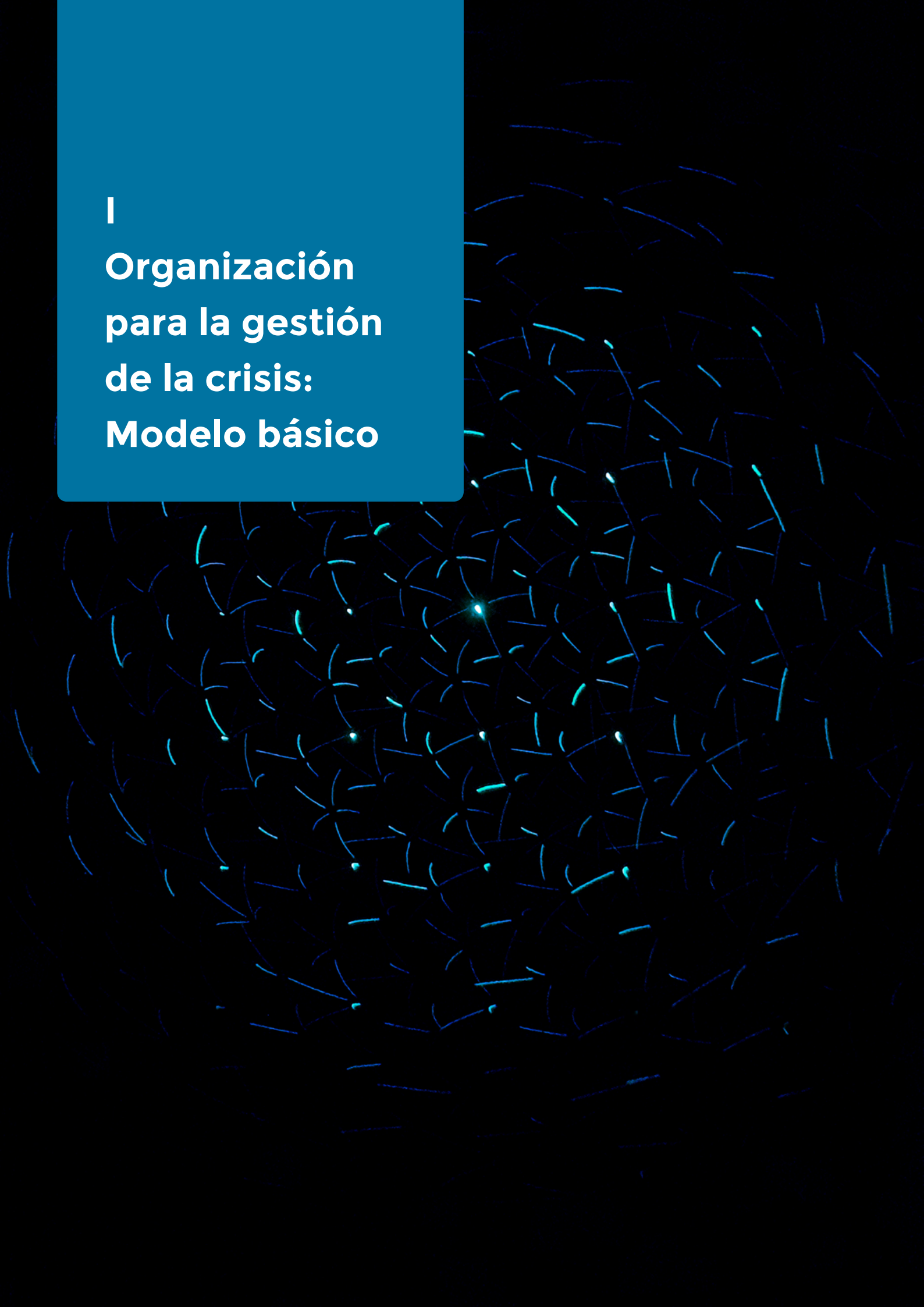
Recursos para la gestión de Incidentes:

- Guía Nacional de Notificación y Gestión de Ciberincidentes aprobado por el Consejo Nacional de Ciberseguridad.
- CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciberincidentes.

Recursos para la gestión de crisis:

- CCN-CERT BP/ 20 Buenas Prácticas en la Gestión de Cibercrisis.
- CCN-CERT BP/29 Gestión de Crisis por Ciberincidente en Entidades Locales.





I

Organización para la gestión de la crisis: Modelo básico

3. ¿QUÉ ENTENDEMOS POR CRISIS? ¿Y POR CIBERCRISIS?

De un modo general definiremos **una crisis** como una situación de **baja probabilidad** que cuando sucede genera un **gran impacto** y cuyos efectos **perduran** en el tiempo. Estos efectos producen un impacto:

- sobre la dinámica de la entidad local o sobre las actividades que realiza y servicios que presta,
- sobre la reputación e imagen de la entidad local, y
- sobre la ciudadanía en general o sobre algún colectivo en particular en función de dónde se haya producido el ataque.

Además, las crisis provocadas por ciberincidentes (**cibercrisis**), **deliberados o no, tienen una característica: la entidad local** está siendo **atacada**, hay unos “malos” que de forma intencionada y desde su posición ventajosa buscan perjudicar a la entidad y sacar provecho.

Toda crisis implica una **toma de decisiones bajo mucha presión**, en poco **tiempo** y probablemente con **información incompleta**, en diversos **frentes en paralelo** y con muchos grupos y personas interviniendo.

En concreto, las crisis por ciberincidente se caracterizan porque requieren tiempo y especialistas para el análisis y la recuperación, y a menudo se hace **difícil conciliar prioridades** entre la investigación del incidente y la necesidad de recuperación de los servicios que presta la entidad.

Así mismo, en este tipo de crisis a menudo es difícil conciliar los diferentes lenguajes y romper la cultura de silos que habitualmente hay entre equipos.

Por todo ello, es necesario tener pensado previamente un esquema de cómo será la respuesta y quién participará en ella.

MODELO BÁSICO DE ORGANIZACIÓN: COMITÉ DE CRISIS, EQUIPO TÉCNICO Y EQUIPO DE COMUNICACIÓN

Con independencia del origen que cause la crisis, de la definición previa se hace patente la **componente de gestión** que su resolución implica. Por lo tanto, en toda crisis se identifican **dos (2) esferas de actuación** distintas (ver **Figura 3**):

1. Organizativa y estratégica en la medida en que su impacto afecta a diferentes ámbitos de la entidad local (servicios, atención a la ciudadanía, imagen y reputación, relación con grupos de interés, presencia en redes sociales, etc.) y requiere de una respuesta coordinada a alto nivel.

2. 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. Gestión que recae sobre un **Equipo Respuesta a Incidentes (ERI)**.

Las actuaciones contempladas en la esfera organizativa y estratégica han de ser asumidas principalmente por **la Junta de Gobierno**, la cual pasa a constituir el núcleo principal del **Comité de Crisis (CdC) constituido** específicamente para cada crisis.

Adicionalmente, a estas dos esferas (la técnica y la de gestión-coordinación) hay que añadir y darle importancia a la gestión de la comunicación. Las crisis provocadas por un ciberincidente suelen tener repercusión en los medios de forma muy rápida, es decir: suelen tener una componente mediática que demanda una actuación coordinada entre la comunicación interna y la externa.

En definitiva, la gestión de una cibercrisis ha de estar **liderada por la Junta de Gobierno, en su calidad de Comité de Crisis**, el cual se **apoya en dos (2) equipos** más técnicos y especializados y que deben estar muy bien coordinados y alineados:

- el de respuesta al Ciberincidente, que liderará y tomará la iniciativa de las acciones.

- el de comunicación que, conociendo el alcance de la situación y las acciones tomadas, desarrollará su actividad comunicacional.

Este sistema de comités y equipos es un MODELO BÁSICO cuya aplicación dependerá sin lugar a duda **del tamaño de la entidad local de que se trate** y de sus capacidades o recursos, pero que puede ser trasladado a cualquier entidad, pues en todas existe un **equipo de gobierno cuyo Alcalde/sa-President/a o Presidente/a y Junta de Gobierno Local puede constituirse en Comité de Crisis en caso de necesidad**. Nadie mejor que ellos para liderar al Ayuntamiento, a la Diputación o al Cabildo en estos momentos de incertidumbre y transmitir confianza a la ciudadanía conforme se está actuando de forma adecuada, proporcionada y coordinada.

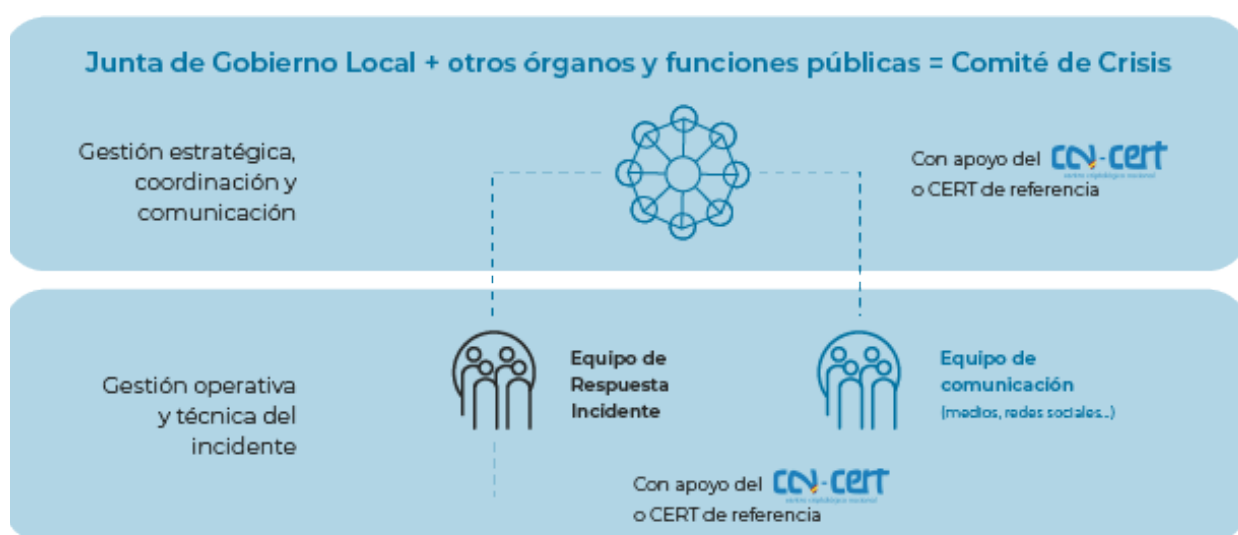


Figura 3. Modelo básico de organización

Cuando la entidad local es grande, su tamaño y su complejidad justifican que exista el Comité de Crisis y los distintos equipos, mientras que en municipios pequeños o medianos se podrá disponer de un único Equipo o Comité de Crisis o, simplemente, definiendo un protocolo de actuación liderado por Alcalde/sa.



3.1. El Comité de Crisis

El Comité de Crisis para ciberincidentes debe tener sus **miembros bien definidos** y éstos deben tener asignado un rol o responsabilidad en el ejercicio de sus funciones dentro del Comité de Crisis.

Para ello se debe haber pensado y definido previamente qué responsables se necesitan para cubrir todos los frentes que requieren la gestión de este tipo de crisis, que, en algunos casos, puede llegar a paralizarlo todo durante semanas o meses.

Estas funciones o roles **han de asignarse a concejales/as, diputados/as o altos cargos** del organigrama de la institución, los cuales, a su vez, estarán cubiertos por cargos electos o de libre designación, cuya adscripción puede cambiar.

Pese a que su composición puede ser **variable** en función de la naturaleza del incidente o de la situación, algunos roles es **preferible que sean permanentes**, como la presidencia del Comité, la coordinación del Comité y los responsables a nivel operativo, de comunicación y jurídico.

Se recomienda crear una **tabla con la correspondencia** entre los roles dentro del Comité de Crisis y los cargos que asumirán ese rol en caso de convocarse el comité. En la tabla deben figurar los datos de contacto de las personas que ocupan esa posición, tanto titulares como suplentes, y debe estar permanentemente actualizada. En entidades medianas o pequeñas, algunas funciones o roles pueden ser asumidos por una misma persona.

Es importante que **se haya definido y compartido** con sus miembros las funciones del Comité en general y la de los miembros que lo componen en particular, el objetivo es alinear el enfoque y facilitar el funcionamiento entre ellos. En concreto, es clave que el presidente del Comité -probablemente lo sea el propio Alcalde/sa o Presidente/a- tenga bien asumido su rol, pues de él dependerá en gran medida la conducción del equipo y por consiguiente el éxito de la gestión.

La composición del Comité de Crisis puede ser de geometría variable de modo que las funciones permanentes sean siempre convocadas, mientras que el resto dependan de las características concretas de la crisis de que se trate.

La organización adecuada para hacer frente a una crisis no se improvisa cuando esta surge, y por tanto es **imprescindible desarrollarla con antelación** para disponer de la preparación necesaria en ese momento. En este sentido, es fundamental que todo ello esté predefinido en un Plan o Procedimiento y que éste se mantenga al día periódicamente (Plan de Respuesta a Incidentes, Plan de Gestión de Crisis general o específico de ciberincidentes...).

Todo **lo que no se prevea es prácticamente imposible improvisarlo durante la emergencia**, por lo que una de las claves para una gestión efectiva de la crisis viene determinada por la capacidad de anticipación e identificación de los ámbitos que pueden llegar a transformarse en situaciones críticas. Se requiere un constante ejercicio de prospectiva que ayude a ser conscientes de las debilidades de las entidades locales y de esta forma, poder prepararse y anticiparse.

Buena práctica:

Tener los planes y protocolos previamente definidos

En resumen, la capacidad de gestionar una situación de crisis depende en gran medida de los comités que se hayan establecido, de su organización y funciones, antes de que ocurra el desastre causado por ese suceso ciber de “baja probabilidad y alto impacto”.

En la figura 4, se muestran los roles y funciones principales que deberían quedar cubiertas en un Comité de Cibercrisis³.



Figura 4. Composición del Comité de Crisis del MODELO BÁSICO

³ Los cargos que se mencionan son, mutatis mutandis, igualmente predicables a las Diputaciones Provinciales, Cabildos Insulares, etc.

3.2. Funciones del Comité de Crisis

En el MODELO BÁSICO propuesto en esta Guía, tomando como base, total o parcialmente, la Junta de Gobierno, **constituye el núcleo principal del Comité de Crisis** para la resolución de los incidentes que hayan sido calificados como crisis.

Efectivamente, la Junta de Gobierno es el órgano en el que se construye la gestión de la crisis a alto nivel dentro de la entidad local, que aporta mayor capacidad de visión 360° y estratégica, a la vez que dispone de una mayor capacidad de interlocución y de movilizar recursos extraordinarios, en caso necesario.

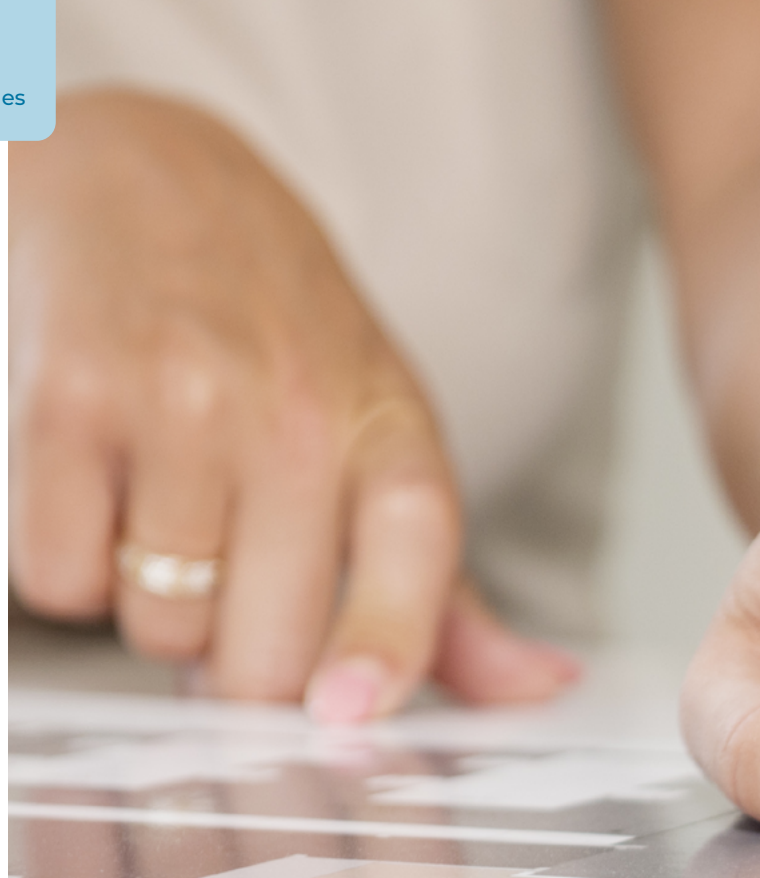
Es el órgano encargado de **tomar las decisiones y coordinar** las acciones necesarias para la resolución de los incidentes que hayan sido calificados como crisis, en todos los frentes de gestión:

· **Asumiendo la responsabilidad de interlocución y comunicación con todas las partes afectadas e interesadas (ciudadanía, medios de comunicación, el propio Ayuntamiento en Pleno...).**

Las principales funciones y responsabilidades del Comité de Crisis, principalmente formado por los miembros de la Junta de Gobierno, son:

· **Comprender el estado de situación y realizar una previsión de escenarios:**

- evaluar toda la información recibida sobre el incidente, realizar una valoración inicial de su impacto (real o potencial) y de las consecuencias sobre la entidad local afectada, sus servicios y las partes interesadas,
- mantener una previsión del impacto potencial y las consecuencias para la organización, considerando los riesgos emergentes y los escenarios hacia donde puede evolucionar para poder acometer medidas de anticipación.



· **Coordinar y priorizar las acciones de resolución y vuelta a la normalidad:**

- Determinar y/o validar y supervisar las estrategias y las medidas implementadas previamente y/o propuestas por el Equipo de Respuesta a Incidentes ERI (para el análisis, contención, mitigación y recuperación de equipos, servicios, información...).
- Determinar las prioridades para recuperar las actividades y servicios en el menor tiempo posible, minimizando los impactos sobre las partes interesadas.
- Dar apoyo al equipo técnico de respuesta, sometido a mucho estrés y probablemente con pocos momentos para el descanso.
- Activar la movilización de recursos extraordinarios cuando sea preciso.
- Hacer un seguimiento de los puntos abiertos, por ejemplo, mediante un documento de "Diario del Ciberataque" que relacione la información relevante respecto a la gestión diaria, medidas adoptadas y estado de situación (con hora y fecha), y las tareas del Plan de Acción (con responsables y plazo establecido).
- Actuar como centro de referencia de información durante la respuesta al incidente y su posterior recuperación, tanto ante los agentes internos como externos, involucrados o concernidos por el incidente.



· Definir el posicionamiento y dirigir la comunicación interna y externa:

- Definir la estrategia de comunicación interna y externa: teniendo en cuenta la función de servicio de la entidad local, los valores del equipo de gobierno elegido y la necesidad de velar por salvaguardar la confianza, la reputación y la imagen, así como la seguridad.
- Asumir la responsabilidad de la comunicación y asegurar las relaciones y la interlocución con todas las partes afectadas e interesadas (ciudadanía, medios de comunicación, el Ayuntamiento en Pleno...).
- Designar el/la portavoz y prepararle para las muchas ocasiones en que será complejo atender las peticiones de información...
- Asegurar que se llevan a cabo, por parte del Equipo de Comunicación, las medidas de comunicación previamente diseñadas, ya sea en medios, redes sociales, marcos asociativos, etc.

· Coordinar las acciones de análisis posterior al incidente:

- Extraer lecciones aprendidas y puntos de mejora.
- Asegurar que se lleva a cabo el Plan de Acción resultante.

4. RESPONSABLES PÚBLICOS EN LA GESTIÓN DE CRISIS POR CIBERINCIDENTE

En este MODELO BÁSICO que se ha propuesto, cabe destacar las funciones de los principales responsables públicos.

4.1. Órganos necesarios

Lo primero que hay que señalar es que, tratándose de Ayuntamientos, el **Gobierno y la administración municipal**, salvo en aquellos municipios que legalmente funcionen en régimen de Concejo Abierto, **corresponde al Ayuntamiento**, integrado por el/la **Alcalde/sa y los Concejales/as del Equipo de Gobierno**.



Alcalde/sa



Tenientes de alcalde/sa



El Pleno



La Junta de Gobierno Local

En los municipios con población de derecho superior a 5.000 habitantes, así como, en los que menos, cuando así lo disponga su Reglamento orgánico o lo acuerde el Pleno de su Ayuntamiento.

4.1.1. El/la Alcalde/sa

El/la Alcalde/sa es el/la presidente/a de la Corporación y, entre otras atribuciones y, por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las **siguientes funciones y responsabilidades**:

- Dirigir el gobierno y la administración municipal y, en el marco del Reglamento orgánico, la organización de los servicios administrativos de la Corporación, lo que también comprende el gobierno de la seguridad de la información y de las crisis provocadas, en este caso, por un ciberincidente.

- Convocar y presidir las sesiones de la Junta de Gobierno Local, cuya estructura constituirá la base, total o parcial, del Comité de Crisis:

- activar y desactivar el Comité de Crisis.

- designar otros miembros ajenos a la Junta de Gobierno Local que han de incorporarse al Comité de Crisis (ya sea personal propio del ayuntamiento, miembros del Comité de Seguridad de la Información, responsables de la Información, de los Servicios, del Sistema o la Seguridad, según dispone el Esquema Nacional de Seguridad, o bien ya sean otros cargos electos o de organismos externos necesarios para la resolución del ciberincidente).

- dirigir la dinámica del Comité de Crisis.

- Asumir la interlocución a alto nivel y **representar al Ayuntamiento**, también ante las entidades públicas competentes en materia de ciberseguridad (como, por ejemplo, a la hora de ordenar la notificación de un incidente de seguridad con impacto significativo) o ante las entidades privadas (por ejemplo, alentando, desde su posición de máximo representante de la institución, de que los técnicos responsables de la entidad se aseguren de que los sistemas de información de los proveedores que prestan servicios a la entidad local sean conformes con lo dispuesto en el Esquema Nacional de Seguridad).

- Convocar y presidir las sesiones del Pleno y de cualesquiera otros órganos municipales a los que deba mantener debidamente informados de la situación y de las principales acciones que se estén llevando a cabo.

- La **aprobación de medidas, proyectos y servicios extraordinarios** (cuando sea competente para su contratación o concesión) necesarios y urgentes para la pronta resolución del incidente.

- Velar por los datos como responsable último del Registro de Tratamientos que establece la AEPD.

Conviene recordar que el/la Alcalde/sa puede efectuar delegaciones en favor de la Junta de Gobierno Local (cuando constituya el Comité de Crisis), como órgano colegiado, de forma que los acuerdos adoptados por esta en relación con las materias delegadas tendrán el mismo valor que las resoluciones que dicte el/la Alcalde/sa en ejercicio de las atribuciones que no haya delegado, sin perjuicio de su adopción conforme a las reglas de funcionamiento de la Junta de Gobierno.

El/la Alcalde/sa podrá realizar las denominadas delegaciones genéricas en las materias que considere necesarias para la resolución del incidente (por ejemplo, aquellas relativas a la seguridad de los sistemas de información de la entidad) y podrá efectuar delegaciones especiales en cualquier concejal/a.

4.1.2. Teniente de alcalde/sa

Los tenientes de alcalde/sa, que habrán sido nombrados por el/la Alcalde/sa, **sustituyen al Alcalde/sa**, por el orden de su nombramiento y en los casos de vacante, ausencia o enfermedad, siendo libremente designados y removidos por este de entre los miembros de la Junta de Gobierno Local y, donde esta no exista, de entre los/ las concejales/as:

- **Sustituir en sus funciones** al Alcalde/sa en su función de presidir la Junta de Gobierno -Comité de Crisis- durante la crisis.

El/la Alcalde/sa puede delegar el ejercicio de determinadas atribuciones en los miembros de la Junta de Gobierno Local (cuando constituye el Comité de Crisis), y, donde esta no exista, en los tenientes de alcalde/sa, sin perjuicio de las delegaciones especiales que, para cometidos específicos, pueda realizar en favor de cualesquiera concejales/as.

4.1.3. El Pleno

El Pleno está integrado por todos los/las Concejales/as (equipo de gobierno y concejales/as de la oposición) y es presidido por el/la Alcalde/sa.

Del Pleno, entre otras atribuciones y por lo que puede resultar de aplicación a la gestión de crisis por ciberincidente se pueden destacar las siguientes funciones y responsabilidades:

- **Velar por ser debidamente informado** apelando al **sentido de la responsabilidad** que un ciberataque requiere, especialmente si ha provocado daños en las actividades y servicios que presta el Ayuntamiento, o si se ha producido una violación de datos personales, etc.

Durante los días o semanas que dure la gestión y resolución de un ciberataque es deseable que el Pleno confíe en el/la Alcalde/sa y en la Junta de Gobierno Local, en su condición Comité de Crisis, alentando que la Junta de Gobierno Local determine los recursos extraordinarios que fueren precisos, con las particularidades que se correspondan con la normativa aplicable a municipios de gran tamaño.



4.1.4. Junta de Gobierno Local

Aunque las decisiones y competencias varían según el régimen del municipio (de gran tamaño o no), para la mayoría de ellos la Junta de Gobierno Local está integrada por el/la Alcalde/sa, que la preside, y un número de concejales/as nombrados libremente por él como miembros de la misma, que no podrá superar al tercio del número legal de miembros de la Corporación.

La Junta de Gobierno debe **ser informada de todas las decisiones del/la Alcalde/sa**, previamente a la adopción de la decisión, siempre que la importancia del asunto así lo requiera, y por ello es especialmente necesario que formen parte como miembros permanentes del Comité de Crisis y que se reúnan. Cuando hay crisis, toca reunirse.

Así pues, en el MODELO BÁSICO propuesto en esta Guía la **Junta de Gobierno constituye el núcleo esencial vertebrador del Comité de Crisis** para la resolución de los incidentes que hayan sido calificados como crisis, siendo el órgano encargado de la gestión de la crisis a alto nivel dentro del Ayuntamiento que aporta una visión estratégica y 360°, a la vez que dispone de una mayor capacidad de interlocución y de movilizar recursos extraordinarios, en caso necesario (ver apartado Comité de Crisis).

La Junta de Gobierno Local tiene las siguientes funciones y responsabilidades:

- Son miembros permanentes del Comité de Crisis y, por tanto, las principales funciones y responsabilidades de la Junta de Gobierno son las propias del Comité de Crisis.
- La **asistencia permanente al Alcalde/sa** en el ejercicio de sus atribuciones y, por consiguiente, en calidad de presidente/a del Comité de Crisis.
- Otras atribuciones que el/la Alcalde/sa o el Pleno le delegue o le atribuyan las leyes.

4.2. Órganos complementarios

En función de la población del municipio existen otros órganos complementarios cuya responsabilidad cabe destacar mientras dura un ciberataque: los/as concejales/as.



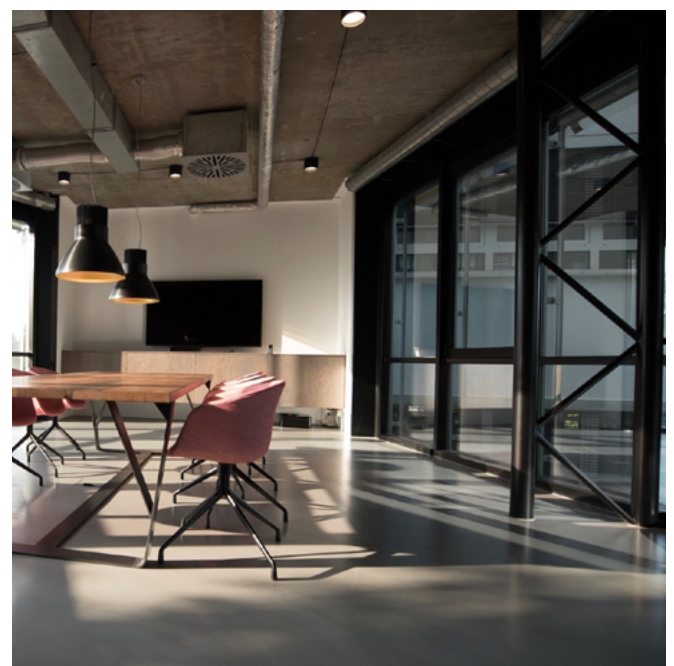
Concejales/as

4.2.1. Concejales/as

Los/as concejales/as en calidad de responsables de áreas concretas o departamentos son los principales responsables de la continuidad de las actividades y servicios que presta el Ayuntamiento o la entidad local de que se trate.

Así pues, durante un ciberataque sus principales funciones y responsabilidades son:

- Aportar **información y análisis de las áreas afectadas** y de la repercusión sobre activos, servicios, ciudadanía, ...
- **Coordinar las acciones**, equipos y los planes de respuesta de las actividades interrumpidas, planes de continuidad en caso de que los haya, ...
- Identificar, **movilizar y organizar los recursos necesarios** para intentar mantener las actividades y la prestación de los servicios, aunque sea en un modo más reducido mientras el Equipo de Respuesta a Incidentes está trabajando para la recuperación completa de los sistemas y/o información, es decir, mientras duran los trabajos de vuelta a la normalidad.



4.3. Funciones públicas de los habilitados nacionales: secretarios/as e interventores/as

Son funciones públicas necesarias en todas las corporaciones locales, cuya responsabilidad administrativa está reservada a funcionarios de Administración Local con habilitación de carácter nacional:



Secretaría



Intervención

4.3.1. Los/as Secretarios/as

En todas las entidades locales existe un puesto de trabajo denominado Secretaría que sustenta la responsabilidad administrativa de las funciones de fe pública y asesoramiento legal preceptivo con el alcance y contenido previsto en el ordenamiento jurídico.

De las atribuciones comprendidas en la función pública de la Secretaría y por lo que puede resultar de aplicación a la seguridad de la información y los servicios prestados por la entidad en caso de una crisis causada por un ciberincidente, se pueden destacar las siguientes funciones y responsabilidades:

En cuanto a la fe pública:

- Preparar los asuntos que hayan de ser incluidos en el **orden del día de las sesiones** que celebren el Pleno, la Junta de Gobierno y el Comité de Crisis.
- Asistir y levantar **acta** de las sesiones.
- Recopilar la **información y decisiones tomadas**: transcribir al libro de **resoluciones** las relativas al incidente y también las derivadas el análisis post incidente/crisis y su consecuente plan de mejoras.
- Actuar como fedatario en la formalización de contratos, convenios y documentos análogos en que intervenga la entidad local, como aquellos suscritos con terceros proveedores -públicos o privados- de servicios dirigidos a garantizar la resolución del incidente que afecta a la entidad local.

· Disponer que se **publiquen**, cuando sea preceptivo y en la medida en que el ciberataque lo permita, los actos y acuerdo de la entidad local en los medios oficiales de publicidad, tablón de anuncios y en la sede electrónica.

· Dirigir el **registro y archivo** de la entidad local, incluyendo en las circunstancias que el ciberataque lo permita, velar por la garantía de disponibilidad de los archivos electrónicos y la confidencialidad, integridad, trazabilidad y autenticidad de la información contenida en ellos.

En cuanto al asesoramiento legal:

· La emisión de informes previos en aquellos supuestos en que así lo ordene el/la Presidente/a o Alcalde/sa de la Corporación o cuando lo solicite un tercio de miembros de la misma. Tales informes deberán señalar la legislación en cada caso aplicable y la adecuación a la misma de los acuerdos en proyecto. Este sería el caso, por ejemplo, de aquellos informes relativos a acciones o iniciativas en relación con la seguridad de la información de la entidad.

· La emisión de informes previos siempre que un precepto legal o reglamentario así lo establezca o la emisión de informe previo siempre que se trate de asuntos para cuya aprobación se exija la mayoría absoluta del número legal de miembros de la Corporación o cualquier otra mayoría cualificada.

· Emitir informes cuando así se establezca en la legislación sectorial.

· Informar en las sesiones de los órganos colegiados a las que asista y cuando medie requerimiento expreso de quien presida, acerca de los aspectos legales del asunto que se discuta, con objeto de colaborar en la corrección jurídica de las decisiones que hayan de adoptarse durante la gestión y resolución del ciberincidente.

4.3.2. Los/as Interventores/as

En las Entidades Locales cuya Secretaría esté clasificada en clase primera o segunda, existirá un puesto de trabajo denominado Intervención.

El control interno de la gestión económico-financiera y presupuestaria comprende durante la gestión y la resolución teniendo en cuenta que puede requerir la dedicación extraordinaria de recursos económicos no previstos.

Teniendo en cuenta las condiciones de excepcionalidad que provoca una ciber crisis y teniendo en cuenta que puede necesitarse recursos económicos-financieros con premura, las funciones y responsabilidad son:

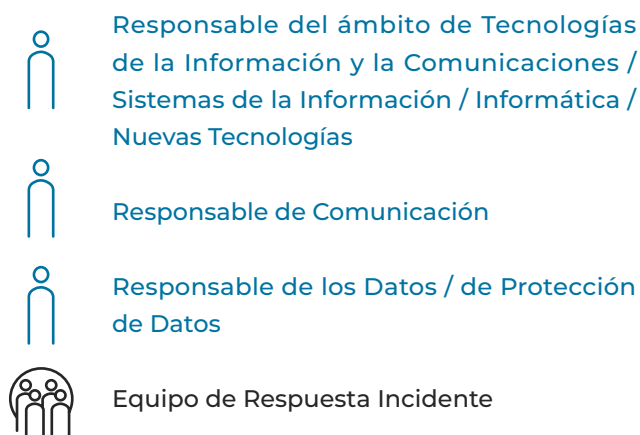
- La función **interventora**.
- El **control financiero** (control permanente y auditoría pública, incluyéndose en ambas el control de eficacia), incluirá las actuaciones de control atribuidas en el ordenamiento jurídico al órgano interventor requeridas para la gestión y resolución del ciberincidente.
- La emisión de informes, dictámenes y propuestas que en materia económico-financiera o presupuestaria sean requeridas durante la gestión del incidente.

Por su parte, la función de contabilidad comprende, entre otras:

- **Organizar** un adecuado sistema de archivo y conservación de toda la **documentación e información contable del ciberincidente** que permita realizar un análisis económico:
 - tanto del impacto como del coste de la crisis, y
 - en la medida de lo posible extraer lecciones aprendidas sobre el beneficio de invertir en seguridad o el impacto de las “medidas aplazadas”.

4.4. Otras figuras a integrar en el Comité de Crisis

El MODELO BÁSICO propuesto en esta Guía propone integrar otras funciones de la entidad local para una respuesta ágil y eficaz durante la crisis:



4.4.1. Responsable del ámbito de Tecnologías de la Información y la Comunicación, Sistemas de la Información

Todos los incidentes de ciberseguridad deben tener asignado un responsable o gestor del incidente y esta responsabilidad puede recaer en diferentes cargos según sea el tamaño y la organización de la entidad local de que se trate. Este rol es asumido generalmente por el Responsable del ámbito de Tecnologías de la Información y la Comunicación, o de Sistemas de la Información, de Informática, de Nuevas Tecnologías o, en terminología del Esquema Nacional de Seguridad: el Responsable del Sistema.

En todo caso, es necesario que se defina un responsable operativo o gestor del incidente, el cual asumirá las funciones relacionadas con la gestión técnica propiamente de seguridad de la información, de Ciberseguridad, de los Sistemas y Tecnologías.

En concreto, sus funciones serán:

- Definir, establecer y hacer seguimiento del Plan de Acción para la contención, erradicación y recuperación de redes, equipos y/o sistemas vulnerados.
- Ser **el enlace entre el Comité de Crisis y el Equipo Técnico** de respuesta a incidente, desempeñando una función clave, la de **intérprete** entre las dos esferas del Ayuntamiento o entidad local. Es la persona en la cual se apoyará el/la Alcalde/sa y su equipo para comprender lo que está pasando.
- Coordinar el Equipo de Respuesta a Incidentes para el desarrollo de las actividades que sean necesarias para la contención, erradicación y recuperación del ciberincidente.
- Preparar y canalizar la información sobre el estado de situación y el Plan de Acción en curso y previsto.
- Asegurar la validez legal de las evidencias.



4.4.2. Responsable de Comunicación

Teniendo en cuenta que la comunicación es uno de los ejes de la gestión que la entidad local debe asumir, en este MODELO BÁSICO organizativo hay que añadir la necesidad de coordinar todo lo relativo a la comunicación a través de **un responsable que puede apoyarse en un equipo específico** de Comunicación.

Sus principales funciones y responsabilidades son:

- Definir el Plan de Comunicación externa e interna y con las partes interesadas.
- Gestionar relación con los medios, los canales, las redes sociales, etc.
- Coordinar al Equipo de Comunicación.
- Definir los mensajes de comunicación externos e internos.
- Realizar seguimiento de la información disponible en medios, los canales y las redes sociales y que puedan tener impacto en la entidad.
- Ayudar a preparar al portavoz.
- Asegurar la comunicación interna: Instrucciones.
- Velar por la proactividad en relación a las partes interesadas, teniendo en cuenta el contexto y sus expectativas (ciudadanía, usuarios de servicios, proveedores, etc.)
- Asegurar que lo que se comunica al personal de la entidad local esté perfectamente alineado con los mensajes y las explicaciones hacia el exterior.

4.4.3. Delegado de Protección de Datos (DPD)

Otra de las figuras clave durante la gestión de un ciberincidente que ha llegado a provocar una crisis en el ayuntamiento es el Delegado de Protección de Datos (DPD). La legislación vigente establece como obligatoria la presencia de un DPD. En ciertos casos, esta figura puede estar delegada en alguna entidad supramunicipal, desde donde se presta el servicio de DPD (externamente) o, incluso en una entidad privada.

Las funciones esenciales del DPD serán

- Cuando se trata de un ciberincidente que afecta a datos personales, deberá iniciar el expediente de incidente a la Autoridad de Control dentro de las 72 horas tras el incidente y responsabilizarse del mismo hasta su finalización.
- Informar y asesorar al Responsable (Comité de Crisis) o al Encargado del Tratamiento y al personal que se ocupe del tratamiento de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en la normativa vigente en materia de Protección de Datos y de las políticas del Responsable o del Encargado del Tratamiento, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la autoridad de control (AEPD o Agencias Autonómicas de Protección de Datos).
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

4.4.4. Equipo de Respuesta a Incidentes

El Equipo de Respuesta a Incidentes es el equipo operativo y representa el nivel táctico de la gestión de los ciberincidentes. Es el órgano encargado de **prevenir, gestionar y responder** eficazmente a los incidentes de seguridad de las tecnologías de información y realizar las **acciones orientadas a la contención, erradicación y recuperación** de redes, equipos y/o sistemas vulnerados.

Estos equipos suelen estar liderados por el Responsable del Sistema y conformados por un grupo de expertos que actúan según procedimientos y políticas predefinidas; expertos tanto en medidas preventivas como en medidas de respuesta frente a sucesos/incidentes que afecten a TI, pudiendo ser parte de la entidad local o un equipo subcontratado de una empresa de ciberseguridad.

El Equipo de Respuesta a Incidentes será el encargado de identificar y clasificar el nivel al que se adscribirá el incidente, a través de los criterios de clasificación mostrados anteriormente, y responder de forma rápida mediante la implementación de medidas de mitigación, contención, erradicación y recuperación de la normalidad.

Es recomendable disponer de un sistema de reporting o informes (que se habrá construido dentro de las acciones preventivas) para informar desde las capas más operativas a la alta dirección del ayuntamiento o entidad local (a la Junta de Gobierno), de cualquier incidente con cierto impacto (potencial o real), de forma que se asegure que el equipo directivo es conocedor de hechos significativos y, por tanto, puede activar medidas adicionales a las ya realizadas por la capa operativa.

En el marco de esta Guía cabe destacar las tres (3) funciones siguientes:

- Comunicar y coordinarse con el Centro Criptológico Nacional o el CERT de referencia respecto de los incidentes de seguridad considerados de nivel ALTO, MUY ALTO o CRÍTICO.
- Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Criptológico Nacional o CERT de referencia en caso de ciberincidente.
- Coordinar y colaborar a través del Centro Criptológico Nacional o CERT de referencia con otros Equipos de Respuestas ante Incidentes, si procede.

Un elemento clave en la gestión de incidentes es someter los planes, procedimientos y configuraciones preestablecidas a permanente prueba y verificación, lo que permitirá la evaluación de la superficie de exposición de las entidades, identificando las vulnerabilidades, brechas de seguridad y deficiencias de configuración asociadas a sus servicios y aplicaciones.

Buena práctica:

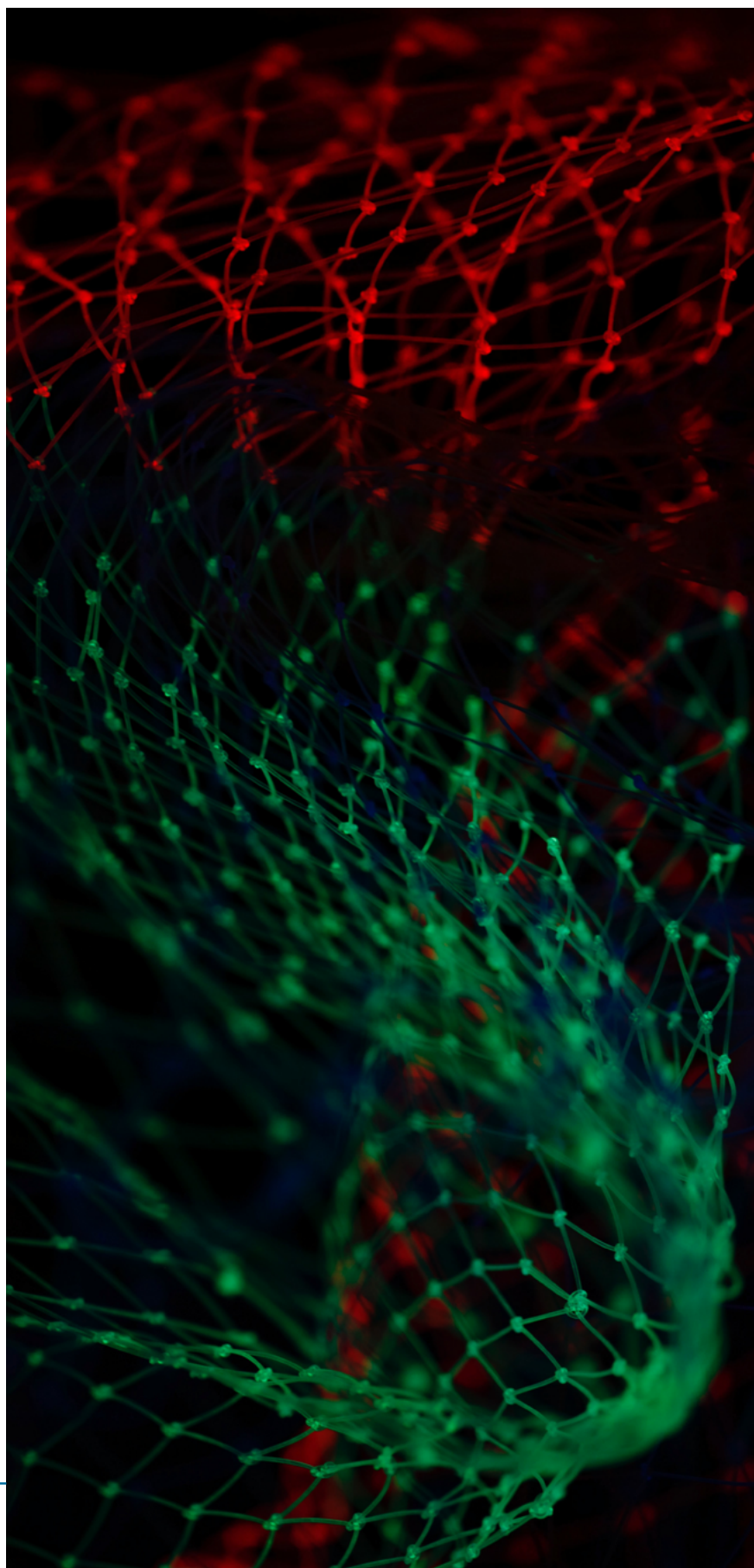
Mantener controlada la superficie de exposición mediante diagnósticos de seguridad



II

Protocolo de actuación: Modelo Básico

5. DE LA GESTIÓN DE INCIDENTES A LA GESTIÓN DE CRISIS



La gestión de las crisis originadas por ciberincidentes debe tener muy en cuenta las características específicas de este tipo de eventos:

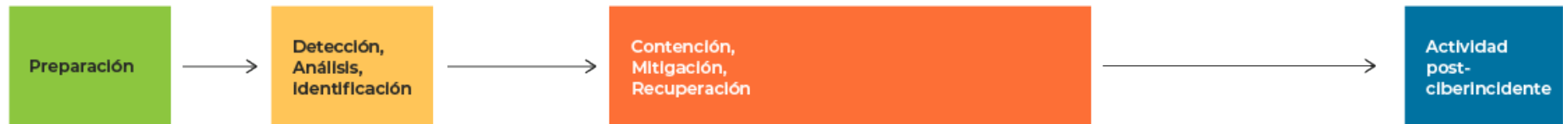
a) La amenaza puede ir mucho más allá del ayuntamiento o entidad local.

b) La existencia de normativa de obligado cumplimiento a seguir en estas circunstancias, como por ejemplo la relativa a protección de datos.

c) La implicación de organismos públicos especializados en la materia -el CCN-CERT, en el caso de las entidades del sector público- que ejercen una vigilancia constante y brindan apoyo técnico y operativo, tanto en las etapas de detección, como en la de reacción, contención, mitigación y recuperación. En relación con las entidades locales, pueden aportar soluciones técnicas o, incluso personal técnico especializado para que se integre en el Equipo de Respuesta a Incidente y/o asesore al Comité de Crisis.

Teniendo en cuenta estas condiciones de contexto, la presente Guía plantea una secuencia en cuatro (4) etapas o fases (**Figura 5**) con el objetivo de asegurar que determinados incidentes **se escalen internamente de forma rápida** y lleguen al ámbito de decisión donde habrán de ser evaluados, a fin de determinar si conviene elevarlos al Comité de Crisis para que éste tome el control de la situación.

Guía de Seguridad de las TIC.
CCN-STIC 817.
Esquema Nacional de **Gestión de ciberincidentes**



Guía de Gestión de Crisis por Ciberincidente para **Entidades Locales**

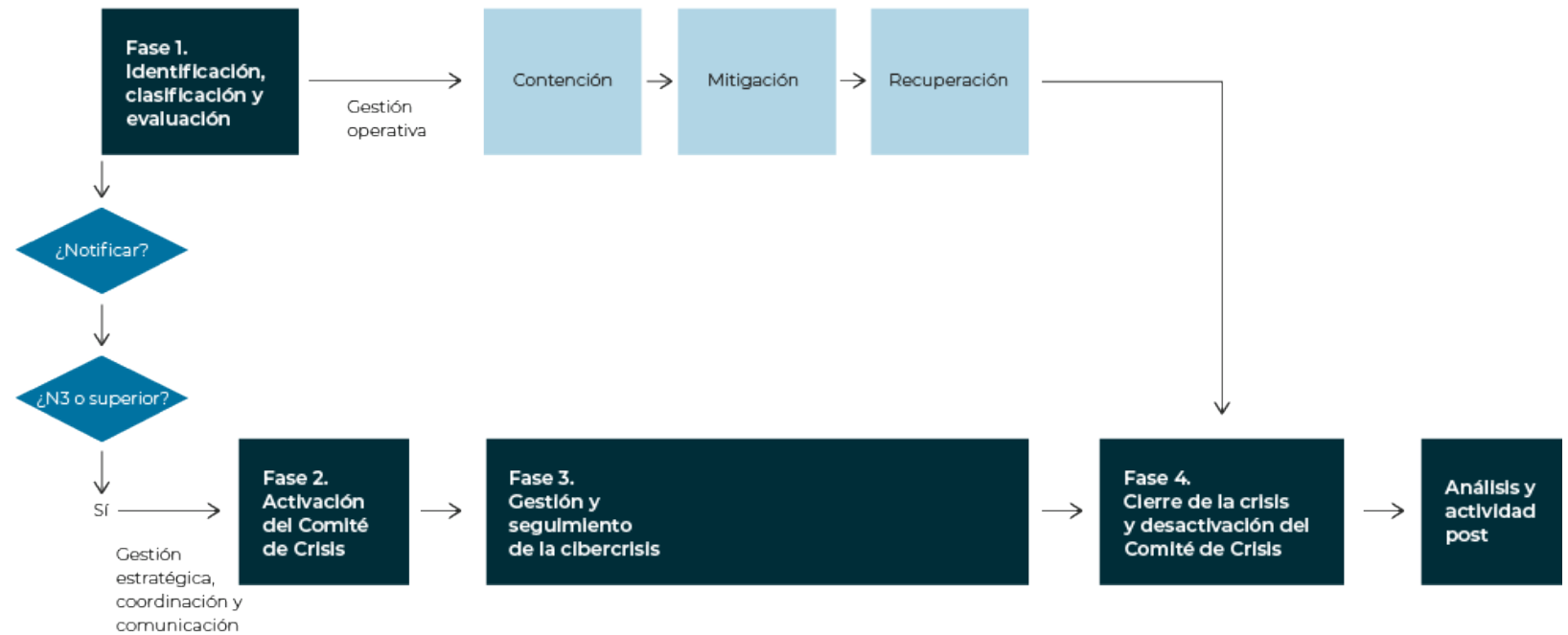


Figura 5. Fases de la gestión del incidente en caso de que se pueda clasificar como crisis

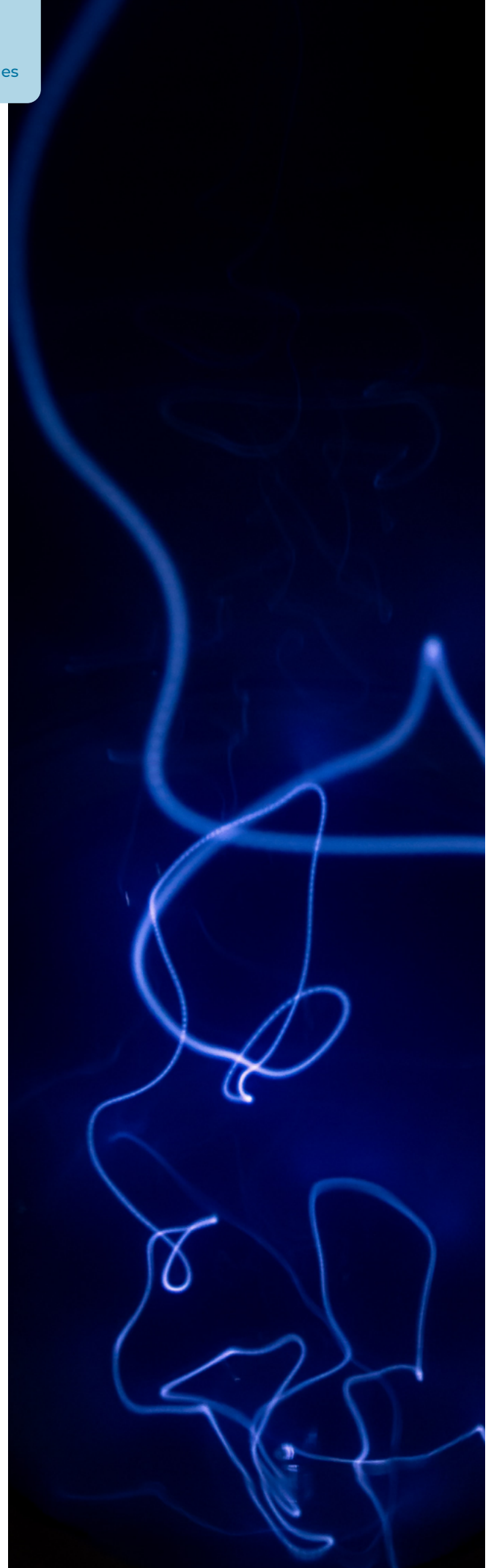
El orden cronológico y natural de la gestión de una crisis, en virtud de las fases anteriores, ha de permitir:

1. Abordar una **amplia gama de ciberincidentes** que pueden ser detectados mediante diferentes mecanismos internos y externos a la entidad local, y que deben ser escalados y notificados rápidamente a quien se determine.
2. Realizar la evaluación mediante los criterios definidos y clasificar el incidente en un determinado nivel de peligrosidad e impacto.
3. **Activar el Comité de Crisis**, al objeto de asegurar la adecuada toma de decisiones de alto nivel y visión global en la entidad local para la coordinación de todas las acciones técnicas (para la resolución y vuelta a la normalidad), de comunicación y de atención a las partes interesadas, etc.
4. Asegurar que se **activan los planes operativos existentes** (de seguridad de la información, de comunicación, continuidad de las actividades, etc.) o bien que se diseñan ad-hoc en función de la tipología del ciberincidente.

Tal como muestra la Figura 5, el primer paso ante un ciberincidente es la realización de una clasificación y evaluación inicial rápida que permita determinar su naturaleza y posible magnitud al objeto de orientar correctamente la estrategia a seguir.

En este sentido, es conveniente cómo, a partir de la detección de un ciberincidente, considerar lo establecido en la Guía Nacional de Notificación y Gestión de Ciberincidentes y en la Guía de Seguridad de las TIC CCN-STIC 817. Así mismo, se han de poder aplicar criterios propios de la entidad local para valorar también el nivel de la emergencia y la conveniencia de activar el Comité de Crisis, a fin de que sea éste el que lidere la respuesta en todos sus frentes, coordinando todos los responsables/equipos implicados, entre los cuales estará el de respuesta al incidente, propiamente dicho.

A continuación, se desarrolla cada una de las fases de la gestión del incidente aportando directrices generales y recursos básicos para que cada entidad local pueda adaptarlo a sus circunstancias.



6. FASE 1. IDENTIFICACIÓN, CLASIFICACIÓN Y EVALUACIÓN DEL INCIDENTE

El ciberataque encuentra a la entidad local centrada en sus obligaciones cotidianas y, sin embargo, debe **transitar rápidamente** de sus prioridades habituales a la situación de crisis, sin una pérdida de tiempo que otorgue ventaja a los atacantes, al no asegurar la rápida intervención del CERT de referencia.

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 entidad local sea proactiva y no reactiva, que tome sus decisiones con rapidez y que se posicione para liderar la gestión de la crisis.

Buena práctica:

Tener iniciativa y ser proactivos en base a mecanismos de prevención establecidos

Cuando se detecta un incidente de ciberseguridad no hay tiempo que perder, pero dada la presión y el estrés que genera un ciberataque conviene **no improvisar** y, por lo tanto, todo lo que se haya podido pautar con anterioridad facilita la imprescindible rapidez de actuación.

En este sentido, es **indispensable haber diseñado un procedimiento detallado a seguir** si se produce un incidente. A efectos de esta Guía se presupone que el personal de la entidad local, cuando tenga conocimiento del incidente, sabrá cómo escalarlo a la persona o personas que se haya determinado internamente, proporcionando la información del incidente necesaria para su análisis, clasificación y notificación hacia el CERT de referencia, si procede.

En este sentido, es fundamental haber definido previamente un protocolo de escalado una vez se ha detectado y un esquema de clasificación de los incidentes en base a las guías de los CERT de referencia.

Este esquema debe **incluir niveles** de peligrosidad potencial e impacto, y, por consiguiente, debe incluir los **criterios de clasificación** de la peligrosidad **y de evaluación** del impacto para ubicar el incidente en un determinado nivel, facilitando así la rápida toma de decisiones en las primeras etapas a la vez que ayuda a discernir si es una crisis y, por consiguiente, si será conveniente activar el correspondiente Comité de Crisis.



La Guía de Gestión de incidentes CCN-STIC 817 y la Guía Nacional de Notificación y Gestión de Ciberincidentes (ver **Figura 6**) proporcionan una taxonomía y unos niveles de peligrosidad que sirven, en primer lugar, para clarificar la obligatoriedad de la notificación, pero también pueden servir para orientar si conviene o no activar el Comité de Crisis:

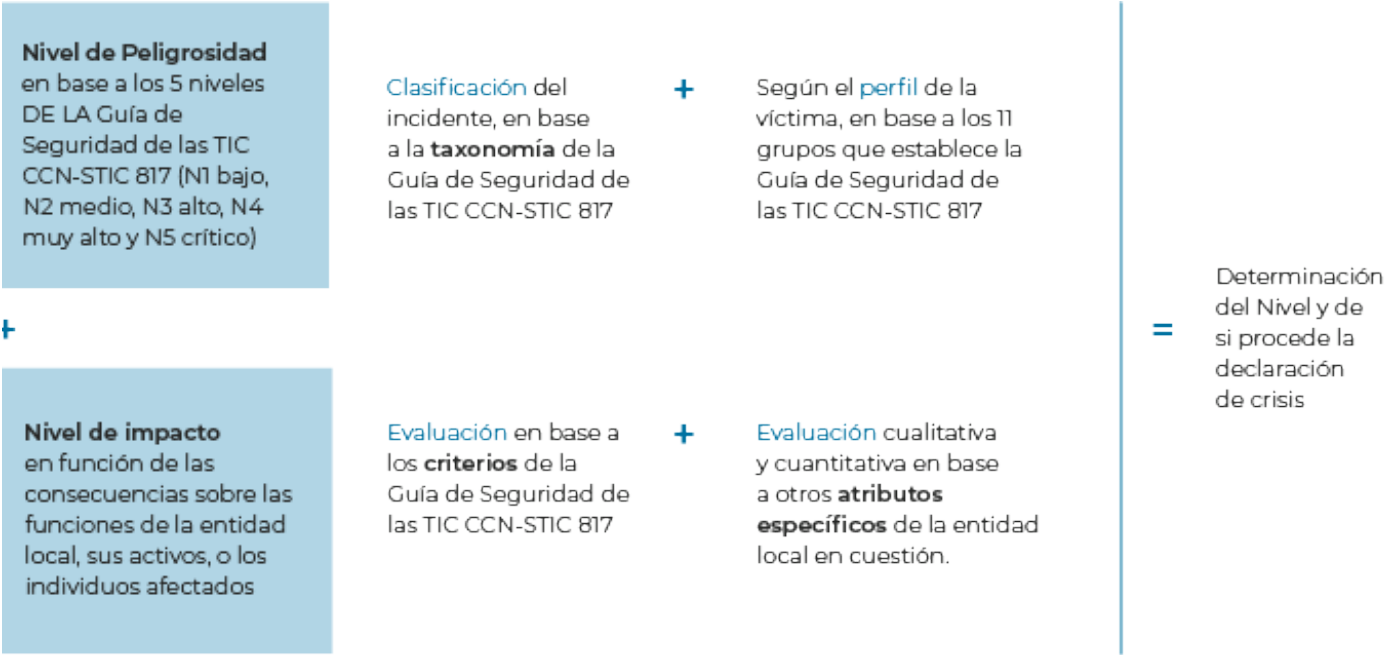


Figura 6. Pautas para determinar el nivel del incidente y la declaración de crisis

Cada entidad debe **desarrollar su propia tabla** e introducir los conceptos o atributos específicos con el objetivo de facilitar la pronta clasificación de los incidentes. Cuantos más se incluyan, mejor puede ser el escalado obtenido, pero, a la vez, más difícil será conseguirlo. La tabla pretende ser una herramienta facilitadora, pero hay que evitar que un afán perfeccionista en su definición la convierta en una limitación que impida avanzar.

A continuación, se muestran los criterios de evaluación que puede servir de **referencia**, tomando como punto de partida los establecidos en la Guía de Seguridad de las TIC CCN-STIC 817 a los cuales se añaden, a modo de sugerencia, otros posibles conceptos a considerar por las entidades locales (ver **Tabla 1**).

Fuente	Atributo / criterio
CCN-STIC 817	Afectación a la seguridad nacional
	Afectación a la seguridad ciudadana
	Afectación a infraestructura crítica/servicio esencial
	Afectación a sistemas
	Interrupción del servicio
	Recursos en jornadas personas
	Impacto económico
	Afectación geográfica
	Impacto reputacional
Otros atributos que puede considerar la entidad local	Afectación a sistemas, procesos o servicios críticos, por ejemplo, si son críticos por imperativo legal
	Afectación a determinados colectivos, por ejemplo, si es un colectivo vulnerable, ...
	Posible alarma social
	Afectación a la seguridad ciudadana (por ejemplo, si ha habido robo de información sensible...)
	Afectación a las relaciones y a la confianza con grupos de interés
	Daños a terceros / entorno
	Implicaciones legales y contractuales
	Criterio de oportunidad: en función del día o época del año en que ha ocurrido el incidente, por ejemplo, si es el período de una campaña especial como pago de impuestos, matriculación escolar, elecciones,
	Otros...

Tabla 1. Criterios de evaluación y clasificación del ciberincidente

La evaluación y clasificación la realizarán personas que posean una visión transversal y tengan la capacidad de valorar desde diferentes ópticas el alcance y la gravedad de la situación, apoyándose en los criterios asumidos por la entidad local. Así pues, el responsable de la clasificación de un incidente puede ser una persona o una pequeña comisión con conocimientos tanto de aspectos de ciberseguridad como de la propia organización y del impacto potencial que sobre ella puede tener el ciberataque. A estos efectos, puede ser útil que la persona o personas encargadas de la valoración del incidente y de su impacto sean las mismas a las que se atribuyeron la Responsabilidad de la Información y de los Servicios, en terminología del Esquema Nacional de Seguridad.

Un caso: el Ayuntamiento de Castellón (I)

El Ayuntamiento de Castellón detectó un ciberincidente el día 30 de marzo de 2021 que dejó inoperativos sus sistemas informáticos, notificándolo a la dirección del Ayuntamiento, y realizando una fase de diagnóstico por parte del Departamento de Modernización determinando que se trataba de un ransomware.

Se creó un plan de trabajo para restablecer la normalidad en el Departamento de Informática y se notificó al CCN y al CSIRT-CV, que **se desplazó** a Castellón para tratar el ataque y mitigar la infección.

6.1. La importancia de la notificación

Teniendo en cuenta que las crisis no las constituyen solo los hechos que estén sucediendo sino también **la forma en que se gestionan**, y teniendo en cuenta que las primeras etapas suelen ser determinantes, es conveniente recordar ahora lo que establece la Guía Nacional de Notificación y Gestión de Ciberincidentes y la Guía de Seguridad de las TIC CCN-STIC 817 del Esquema Nacional de Seguridad en relación con las notificaciones.

Posteriormente a la determinación del nivel de peligrosidad e impacto del ciberincidente, se deberá notificar el incidente a la autoridad competente a través del CERT de referencia para establecer una comunicación directa. En el caso de las entidades del sector público, se deberán notificar los ciberincidentes al CCN-CERT, en caso de que el nivel determinado sea ALTO (Nivel 3), MUY ALTO (Nivel 4) o CRÍTICO (Nivel 5).

Esta notificación se podrá realizar o a través del correo electrónico "incidentes@ccn-cert.cni.es", incluyendo una descripción detallada del incidente, o, mejor, a través de la herramienta LUCIA (ver CCN-STIC- 845 – Manual del Usuario), conteniendo:

- Recopilación de toda la información relevante referente al incidente.
- Documentar el incidente y las acciones llevadas a cabo hasta el momento por parte del Equipo de Respuesta a Incidentes.

En el **Anexo 1** se amplía un Protocolo tipo de los datos a aportar por parte del organismo afectado.

El proceder obligado para operadores de servicios esenciales **es asimismo muy recomendable para las entidades locales** dado que garantiza una rápida reacción, la disponibilidad inmediata de recursos de actuación especializados y la pronta advertencia a otras organizaciones susceptibles de ser también afectadas. En concreto, los operadores de servicios esenciales han de notificar a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos significativos en dichos servicios y es obligatorio **informar sobre el incidente, como mínimo, en tres (3) ocasiones** (ver **Tabla 2**).

Los operadores han de realizar una primera notificación sin dilación indebida tan pronto como dispongan de información suficiente en un plazo máximo de 48 horas desde el momento en que tengan conocimiento del suceso. Se realizarán, además, las notificaciones intermedias que sean precisas para actualizar el incidente y su evolución mientras no esté resuelto, y se realizará una notificación final tras su resolución, informando del detalle de la evolución del suceso, la valoración de la probabilidad de su repetición y las medidas correctoras previstas.

Nivel de peligrosidad	Notificación Inicial	Notificación Intermedia	Notificación Final
CRÍTICA	Inmediata	24/48 horas	20 días
MUY ALTA	Inmediata	72 horas	40 días
ALTA	Inmediata	-	-
MEDIA	-	-	-
BAJA	-	-	-

Tabla 2. Criterios notificación incidentes según la Guía de Seguridad de las TIC CCN-STIC 817

El CCN-CERT, en colaboración con el INCIBE-CERT y el ESPDEF-CERT, pone a disposición de todos los actores involucrados la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes**. Esta plataforma, basada en la herramienta LUCÍA (Listado Unificado de Coordinación de Incidentes y Amenazas) permite el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y CSIRT de referencia de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal.

6.2. Protocolo de actuación: la gestión y el diálogo con el atacante

Este es un punto clave a considerar durante la gestión del ciberincidente, por ejemplo, en caso de un ransomware.

Como norma general:

- la víctima no debe dialogar con el atacante.
- se recomienda a la víctima que ponga una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional, Guardia Civil o policías autonómicas).
- actuaciones de las autoridades competentes:
 - FCSE (Policía Nacional, Guardia Civil u otras): si se hubiera puesto en conocimiento de las FCSE, actuarán con su criterio informando a la entidad también en caso de diálogo con el atacante.
 - CCN-CERT o CSIRT de referencia: actuará en función de su criterio y práctica, informando a la entidad en caso de diálogo con el atacante, y en su caso compartir hallazgos con otros posibles actores en la investigación.
- Si de las actuaciones citadas de las autoridades competentes se derivara algún perjuicio para la víctima la autoridad en cuestión desplegaría las acciones necesarias para restaurar o solventar el problema causado.

6.3. Soporte de respuesta a incidentes

La determinación de las actuaciones a adelantar para la gestión de crisis ante un ciberincidente contempla el **servicio de soporte de respuesta a incidentes** basado en la identificación e implementación de una estrategia y medidas para la gestión, contención y desarrollo de actividades de mejora continua a través del **uso de tareas automatizadas (playbooks) de referencia como apoyo** a la entidad local afectada.

Buena práctica:

Uso de playbooks para el desarrollo de actividades de planificación, detección y respuesta de ciberincidentes con el objetivo de minimizar su impacto.



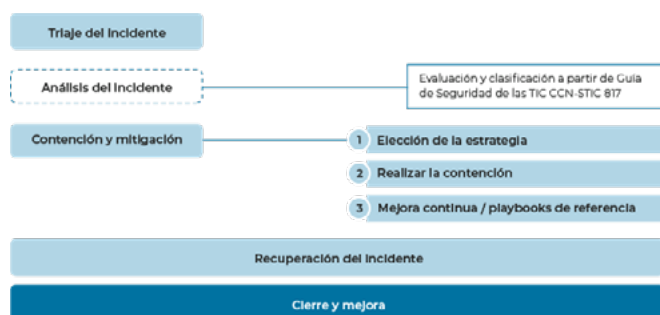


Figura 7 Actividades del servicio de soporte de respuesta a incidentes

Tal como muestra la figura 7., **el triaje** y el **análisis del incidente** son las primeras actividades que debe realizar la entidad local para determinar el estado de la situación del ciberincidente e identificar su criticidad. Respecto a la actividad de contención y mitigación, el **servicio de soporte a la respuesta debe contemplar el desarrollo de tres (3) actuaciones**:

1. Elección de la estrategia y selección del playbook aplicable

en base al análisis y características del incidente. En caso de no contar con un playbook asociado a la gestión y contención del incidente, se deben identificar y preparar las medidas para contener y mitigar la afectación.

2. Realizar la contención de acuerdo al playbook aplicable o en caso de no tenerlo, mediante las medidas identificadas en la anterior actividad, incluyendo la recolección de evidencias, documentación de las actividades realizadas y resultados obtenidos, con el fin de cerrar el incidente o para compartir hallazgos con otros posibles actores en la investigación.

3. Mejora continua de las actividades de contención mediante la actualización y elaboración de playbooks de referencia en base a la experiencia y resultados obtenidos durante la respuesta al incidente.

El **servicio de respuesta** implicará entonces, que los playbooks sean actualizados periódicamente por un equipo multidisciplinar en la entidad para reflejar los cambios en el contexto de la organización en cuanto a controles implementados, servicios y tecnologías utilizadas e integración de roles y responsabilidades para el manejo de incidentes, entre otros.

Buena práctica:

Los playbooks deben actualizarse periódicamente para reflejar los cambios en el contexto de la entidad local.



Tal como se muestra en la figura 8., la elaboración de **playbooks** debe contemplar **tres (3) etapas**: **Planificación, Detección y Respuesta** para la determinación de actividades específicas que conduzcan al análisis efectivo del incidente, su detección y respuesta.

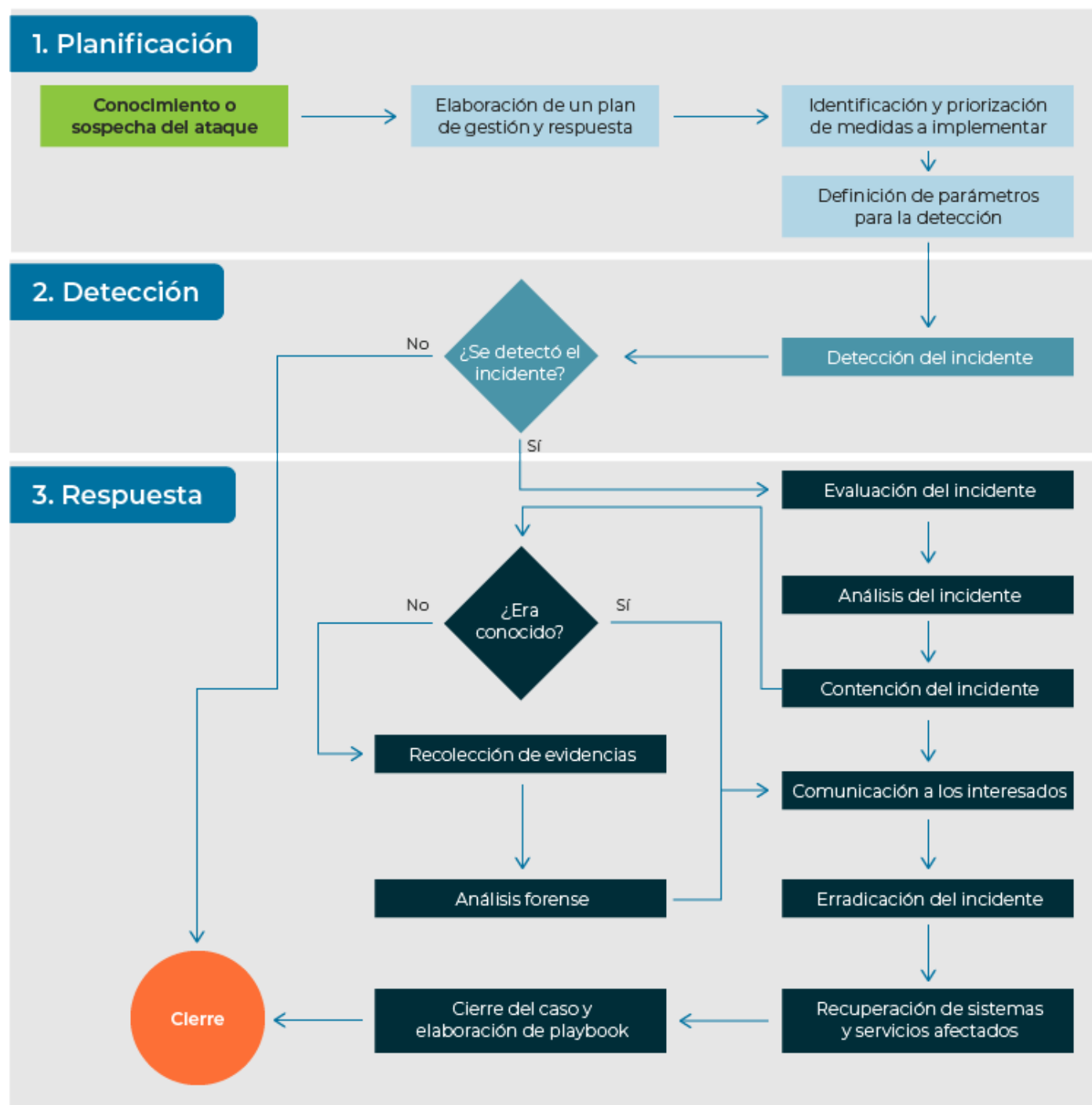


Figura 8 Etapas y actividades para la elaboración de playbooks

Teniendo en cuenta las tres (3) etapas para la elaboración de playbooks se propone tomar como base para la gestión de ciberincidentes relacionados con la **filtración de datos, denegación de servicio, malware y ataques internos (insiders)** los playbooks anexos a esta Guía.

7. FASE 2. ACTIVACIÓN DEL COMITÉ DE CRISIS

Siguiendo con el flujo general del acontecimiento, una vez detectado el incidente y realizada la primera valoración, la indispensable notificación inicial y la consulta de los criterios definidos en la tabla de clasificación y evaluación, los cuales también sirven como criterios de escalado, se pondrán en marcha los mecanismos de gestión de la propia crisis.

La decisión de activar el Comité de Crisis de la entidad local puede ser difícil cuando se está en las primeras etapas del incidente, el nivel de estrés y de incertidumbre sobre el propio incidente hacen que no siempre sea evidente si hay que escalarlo hasta el equipo de gobierno. La experiencia demuestra que pueden ser varias las razones:

- Las personas tienden a evitar transmitir malas noticias, que parezcan catastrofistas.
- A menudo hay un exceso de voluntarismo pensando que se podrá resolver antes de comunicarlo a instancias superiores.
- Se tiende a pensar que dichas instancias superiores pueden ser una injerencia en la resolución y que no se necesita su implicación...
- Etc.

Por ello es conveniente que la entidad local tenga establecido el protocolo de escalado del incidente y el nivel a partir del cual se activa el Comité de Crisis. En este sentido, la determinación del Nivel de Peligrosidad e Impacto es clave para deducir si es conveniente la declaración de crisis y, por consiguiente, de si es conveniente activar el Comité de Crisis:

1. En principio, los incidentes de Nivel 1 BAJO y Nivel 2 MEDIO no deberían requerir la convocatoria del Comité de Crisis como tal. Será la organización, bajo la responsabilidad directa del Responsable de Seguridad de la Información, y el Equipo de Respuesta a Incidentes los competentes para solucionar el problema desde un punto de vista operativo: sea porque tienen conocimiento técnico suficiente o sea con la ayuda de los equipos del CSIRT de referencia.
2. Si el incidente es de Nivel 3 ALTO sería opcional.
3. Si el incidente es de Nivel 4 MUY ALTO o de Nivel 5 CRÍTICO si se considera adecuado la declaración de crisis y por consiguiente se activaría el Comité de Crisis.



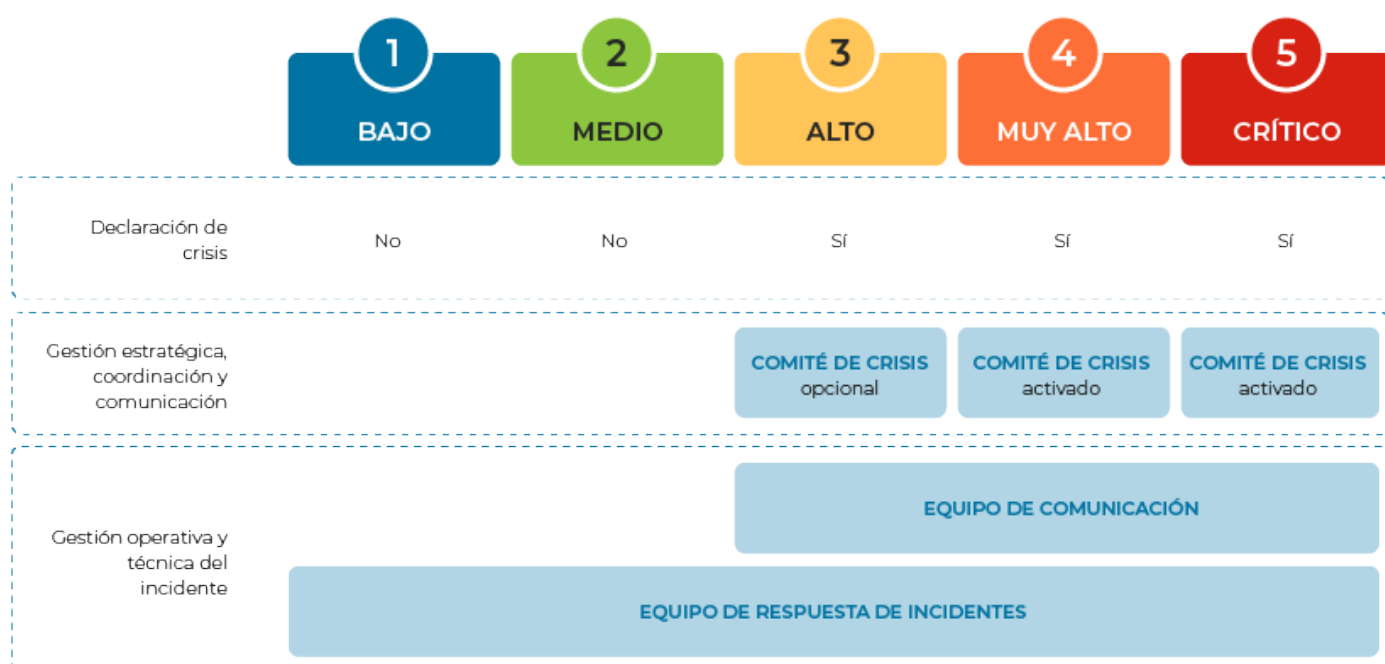


Figura 9. Comité y equipos según el Nivel

Decidir sobre qué nivel del ayuntamiento y sobre qué comité o equipo ha de recaer la gestión es también un elemento a considerar para decidir el nivel del incidente/ crisis.

Esta configuración de comités (ver **Figura 9**) 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 Nivel ALTO o MUY ALTO la cúpula de la entidad local será quien tome las decisiones finales dentro del Comité de Crisis, según las aportaciones del Equipo de Respuesta a Incidentes, el Equipo de Comunicación y los equipos compuestos por representantes de las áreas funcionales.

Es importante tener bien definido el **procedimiento formal de activación del Comité de Crisis**, incorporando aspectos tales como:

- 1) Qué **miembros tienen la potestad** de activarlo, además del/la Alcalde/sa. En caso de que, como se ha comentado anteriormente, haya una persona o comisión encargada de evaluar los incidentes, puede ser a propuesta de esta.
- 2) Qué canales se utilizarán para activar el Comité y convocar la primera reunión: correo electrónico, llamada telefónica, grupo en red social, aplicación de

comunicación masiva con el grupo predeterminado, teniendo en cuenta que las herramientas de la red corporativa pueden no estar operativas.

- 3) El modo en que se desarrollarán las reuniones: presenciales, por videoconferencia, llamada múltiple, híbridas.
- 4) Qué información ha de contener el comunicado de activación: tipo de incidente, primera clasificación, impactos conocidos...

Es importante liderar, tomar y mantener la iniciativa durante un incidente y, si ésta se pierde, buscar las oportunidades que permitan recuperarla. Tomar medidas razonables es casi siempre mejor que no hacer nada, partiendo de una preparación y un plan previamente acordado.

Buena práctica:

Tomar el liderazgo, velar por los valores propios y mantener el control

8. FASE 3. GESTIÓN Y SEGUIMIENTO DE LA CIBERCRISIS

Seguido de la convocatoria y activación del Comité, la primera medida a adoptar por parte del Comité de Crisis es **reunirse**.

Hay una cierta tendencia a dejar pasar un tiempo inicial precioso a la espera de más información (que raramente llega) o de que el incidente se desactive por sí solo (nunca sucede). Este tiempo inicial es imprescindible para **tomar decisiones con anticipación** y hacer un **primer diagnóstico** que influirá de un modo fundamental sobre el trabajo posterior, así como dedicar tiempo a los posibles escenarios de evolución.

La gestión de la crisis requiere abordar varios frentes a la vez como se muestra en la Figura 10 que, de forma simplificada, se desarrollarán a lo largo de este documento.



Figura 10. Ámbitos de actuación a cubrir en una crisis

En esta fase de gestión es donde se aplican los mecanismos y procedimientos que se hayan definido con antelación. Desde el punto de vista técnico:

1) Estos mecanismos deben contemplar la **rápida coordinación con el CERT de referencia** de modo que se forme un equipo capacitado que pueda actuar con celeridad y cuyas tareas sean asumidas como prioritarias por la organización. De estos trabajos saldrán más evidencias y más información para evaluar mejor la situación en el Comité de Crisis.

2) Cuando la situación esté controlada por esos equipos técnicos, se deberá elaborar un **Plan de Mitigación** que deberá ser aprobado por el Comité de Crisis. Ese plan deberá ser muy detallado y estudiado por todas las partes, incluyendo a sus ejecutores, antes de llevarse a cabo, asegurando una ejecución metódica, paso por paso, con dos (2) objetivos:

i) Disminuir su tiempo de ejecución, puesto que, muy probablemente su ejecución conllevará la indisponibilidad temporal de la red de la organización.

ii) No dejar resquicios al atacante para poder mantenerse dentro de la red, una vez se ejecute el plan.

Un caso: el Ayuntamiento de Castellón (II)

Un día después de la detección del incidente, el día 31 de marzo, se determinaron tres (3) líneas de actuación:

Contención:

El objetivo fue eliminar el malware e iniciar el proceso de desinfección de los puestos de trabajo. En esta línea de actuación se identificó la tipología de ataque para poder determinar las actuaciones a realizar.

Además, se realizó la comunicación a la Agencia Española de Protección de Datos y se denunció el ataque a la Policía Nacional.

Mitigación:

Se rediseño la red, actualizando los equipos, limpiando los discos duros, cambiando las credenciales de todo el dominio y actualizando las reglas de antispam y de firewalls para poder mitigar el impacto del incidente.

En esta línea de actuación se recuperó, también, las copias de seguridad, catalogándolas y asegurando unos entornos estables y seguros.

Recuperación de los servicios:

Se recuperan las bases de datos, copias de seguridad y servidores de ficheros. De hecho, el día 5 de abril se recuperan los servicios, recobrando gran parte de las herramientas de trabajo, y servicios del Ayuntamiento, entre ellos:

- Recuperación de la Sede electrónica.
- Recuperación de los servicios sin toda la capacidad operativa

Buena práctica:

Asegurar la coordinación entre los diferentes departamentos implicados es básica para la gestión del ciberataque.

La coordinación entre todos los implicados y participantes es una de las claves para la buena resolución de un ciberincidente, y para ello es necesario a menudo reconocer que la situación sobrepasa las propias capacidades y que se necesita ayuda externa.

8.1. Dinámica de las reuniones del Comité de Crisis

El objetivo de la primera reunión es asumir las funciones encomendadas, tomar el control de la situación y emprender el proceso formal de toma de decisiones para la gestión de la ciber crisis. La reunión debe realizarse con la mayor brevedad posible (con sus miembros titulares o suplentes) y puede ser de tipología diversa (presencial, videoconferencia, etc.).

Es útil tener prevista la dinámica del Comité de Crisis tanto en la primera reunión como entre reuniones durante el desarrollo de la propia crisis. Para ello se recomienda incluir en el Plan o Manual de Crisis una agenda tipo y una lista de control o checklist de temas a tratar, con el objetivo de facilitar la dinámica y el proceso de toma de decisiones, asegurando que se tratan los puntos clave.

Buena práctica

Recordar las principales funciones que tienen asignadas los miembros del Comité de Crisis

A modo de orientación **la agenda** puede contener los siguientes puntos:

- a) Establecer una estimación de la duración de la reunión.
- b) Revisar hechos y pedir información actualizada del incidente.
- c) Comprobar la lista de control (checklist).
- d) Recordar rápidamente el rol de cada miembro: repasar sus funciones y las acciones prefijadas que debe realizar en los primeros momentos.
- e) Asignar responsabilidades derivadas del Plan de Acción y primeras acciones acordadas.
- f) Verificar que las acciones son asumidas por los responsables, clarificando las cuestiones de coordinación entre ellos.

g) Fijar la próxima reunión y frecuencia de las siguientes reuniones del Comité y de los puntos de control (éstos, con un doble objetivo: informativo y de revisión en caso de que se hayan producido cambios).

h) Concretar aspectos a incluir en la siguiente reunión.

i) Validar que se han tratado todos los puntos de la lista de control (checklist).

La lista de control o checklist debe ser confeccionada con anterioridad, con el objetivo de que sirva de soporte al Comité de Crisis para asegurarse de que se tratan de forma ordenada y sistemática todos los temas que se deben abordar en una ciber crisis y evitar que las prisas o la urgencia de la situación provoquen el olvido de alguno de ellos. Como cabe deducir, es importante que tenga una vocación de exhaustividad en los aspectos que incluye.

El primer paso en la gestión y posterior resolución de un incidente es llevar a cabo un diagnóstico de lo que está sucediendo. A pesar de que, en los primeros momentos de un incidente, 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).

Buena práctica:

Realizar un diagnóstico inicial y escenarios posibles

Es importante registrar de un modo continuo las decisiones que vaya tomando el Comité de Crisis en un documento de "Diario del Ciberataque" que relacione la información relevante respecto a la gestión diaria, medidas adoptadas y estado de situación (con hora y fecha), y las tareas del Plan de Acción (con responsables y plazo establecido).

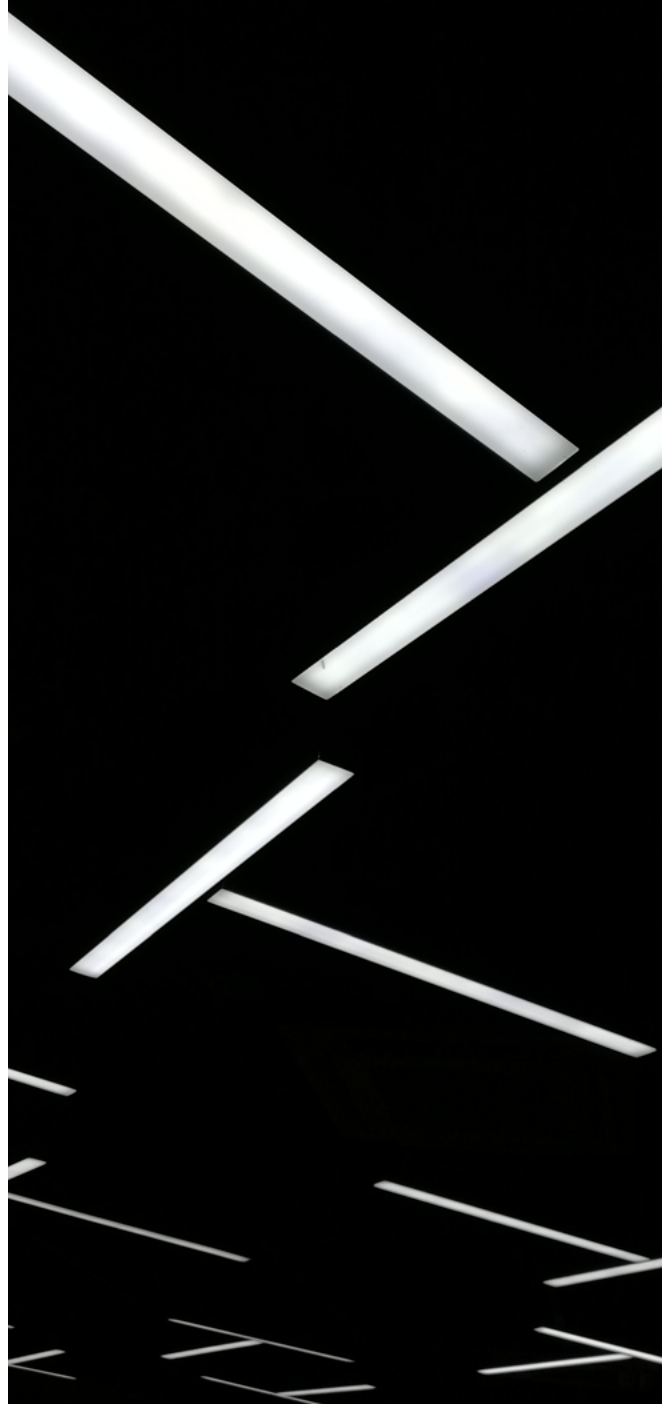
8.2. El Comité de Crisis entre reuniones

El Comité de Crisis debe realizar el seguimiento continuo de la situación, lo que implica mantener una dinámica de reuniones adecuada que asegure la revisión periódica y sistemática de la situación, así como de los resultados y de la estrategia de la respuesta adoptada.

Por lo tanto, hay que contemplar que mientras el Comité esté activado se utilizará un **proceso de reunión-pausa-reunión-pausa**, a fin de que sus miembros puedan llevar a cabo las acciones encomendadas y tengan tiempo para coordinar a su equipo e implementar las acciones de su ámbito.

A continuación, se recuerdan las principales tareas a realizar entre reuniones por parte de los miembros del Comité de Crisis.

- 1) Llevar a cabo las tareas del Plan de Acción acordadas en la anterior reunión.
- 2) Asignar o emprender acciones individuales.
- 3) Supervisar el desarrollo de la estrategia.
- 4) Recopilar nueva información que deberá ser proporcionada en tiempo real al Coordinador del Comité quien, a su vez, tiene la responsabilidad de que se comparta y llegue al resto de miembros del Comité cuando no están reunidos.



Un caso: el Ayuntamiento de Castellón (III)

La Alcaldesa convocó una reunión con el Centro de Coordinación Operativa Municipal (CECOPAL) para abordar el ataque, con el objetivo de neutralizarlo. Entre los asistentes al CECOPAL participaron:

- La Alcaldesa,
- El portavoz del equipo de Gobierno,
- La concejala de Administración Electrónica e Innovación Digital,
- Representantes de la parte técnica municipal,
- Representantes de la administración y del pleno, del servicio jurídico, urbano y de emergencias,
- Técnicos del equipo técnico del Departamento de Modernización.

En total se realizaron 13 reuniones del CECOPAL y 4 juntas de portavoces de carácter técnico, en las que participaron:

- El director del servicio
- La concejala del Ayuntamiento de Castellón
- El jefe de Sección

8.3. La comunicación durante la crisis

La gestión de la comunicación en una situación de crisis requiere, igual que con los otros ámbitos, de una **planificación** y de una aplicación férrea del Plan de Comunicación que se haya definido previamente, dado que el ruido interno y externo que se produce en estas situaciones pone en riesgo el éxito de esa gestión y puede situar a la entidad local a remolque de la situación.

En el momento actual, cualquier situación de crisis es retransmitida en directo por las redes sociales, que a su vez actúan como fuente de información para los medios de comunicación tradicionales, que se hacen eco de las mismas. Ese circuito es aprovechado por múltiples interlocutores que ejercen de portavoces o bien de “presuntos expertos”, dimensionando inapropiadamente la situación de crisis, **“si no dices lo que haces, otros dirán lo que no haces”**.

Ante esa situación, la única opción es la proactividad, en el sentido de tomar las riendas del incidente, **estableciendo un ritmo propio** que no suponga quedar a merced de la presión interna o externa. Lo deseable siempre en una crisis es que la principal fuente de información sea la propia organización. Para que esto sea así, es imprescindible ser proactivos y llevar la iniciativa, 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**.

Buena práctica:

Ser proactivos, tener un discurso unificado y ser la fuente oficial de información

Para ello se requieren algunas condiciones esenciales: la primera es **disponer de un plan o protocolo** previo de comunicación de crisis que haya “pensado” en este tipo de escenarios, que determine los circuitos de información, los argumentarios necesarios y recurrentes, los canales, los portavoces, todos los interlocutores involucrados y las acciones a desarrollar.

El tiempo de respuesta en las crisis actuales es nulo y por ello es necesario contar con los **liderazgos** y con la capacidad de decisión adecuada para tomar las riendas de la situación. Tal como se ha mencionado anteriormente, la entidad local deberá **decidir quién, a nivel comunicativo, es el responsable** de gestionar la situación en todas su dimensión interna y externa.

En este sentido, la proactividad y el discurso unificado son componentes muy importantes de la política comunicativa que debe tener en cuenta no sólo la información externa (medios de comunicación, página web, redes sociales, etc.) sino también que esa unicidad de mensaje se practique internamente, hacia el propio personal, proveedores y/o clientes.

Efectivamente, la **comunicación interna es tan importante como la externa** y empieza por atender las **necesidades de información de los propios colaboradores**, los cuales, en una sociedad donde imperan las redes sociales, pueden ejercer a su vez de canales de comunicación, es decir, cualquier colaborador puede actuar -voluntaria o involuntariamente- como fuente de información sobre lo que está sucediendo.

Se recomienda actuar con celeridad y **elaborar la información a transmitir internamente** a todo el personal, no solo en relación con lo que deben hacer técnicamente, sino también aportando esa información que les ayude a hacer frente a preguntas de sus círculos familiares y de amistad.

8.3.1. Reflexiones sobre la transparencia, la empatía y las responsabilidades

La desinformación, 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 entidad **debe evitarse la incertidumbre**. Esta actitud es también relevante en la rápida notificación al CERT de referencia, ya que ello redundará en un beneficio global.

En general, una sociedad madura acepta que en una organización las cosas no siempre funcionan 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 lo hagan de forma inadecuada.

Sin embargo, mantener la transparencia durante un escenario ciber 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 entidad local.

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.

Como se ha comentado anteriormente, también el modo de gestionar una crisis se asienta en los valores de la organización. Desde este punto de vista, el asumir responsabilidades cuando las haya es una muestra de que dichos valores existen y se respetan. Más allá de ello, en general, no asumir las responsabilidades se vuelve en contra de la entidad y de su equipo de gobierno, cuando se hace patente que negándolas pretendía eludir las consecuencias de sus actuaciones.

Buena práctica:

Tener empatía y asumir responsabilidades

Por consiguiente, es importante cuidar de un modo especial, el **equilibrio entre lo que puede decirse** (un exceso de comunicación 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 la necesidad de atender las expectativas de información de las partes interesadas, como, por ejemplo, del pleno del ayuntamiento o los representantes de la oposición.

8.3.2. Acciones de comunicación durante la crisis

Al igual que en la gestión técnica del incidente y la gestión de la crisis, la gestión de la comunicación es un proceso que debe empezar mucho antes de la misma y **debe finalizar mucho después**, pero desde el momento en que se detecta el incidente y éste deriva en la declaración de crisis, es importante recordar los siguientes puntos:

- Recopilar toda la información y comprender la situación.
- Actualizar y generar los argumentarios y mensajes: elaborar la información más adecuada teniendo en cuenta tiempo/prioridad y grupo de interés.
- Designar el portavoz y prepararlo.
- Identificar los interlocutores vinculados y posibles nuevos interlocutores.
- Editar contenidos multiplataforma para los mensajes.
- Gestionar, atender y seguir los medios y canales de comunicación.
- Definir un cronograma y agenda propia con las acciones de comunicación para ser presentado al Comité de Crisis.

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, todavía no hay resultados que se puedan presentar a la opinión pública y grupos de interés.

En un contexto como el descrito más arriba de proactividad y transparencia por parte de la entidad local, cuando haya comparecencia del portavoz o comunicados periódicos, es un buen momento para poner en valor las medidas tomadas por la entidad y su equipo de gobierno, tanto las preventivas en materia de ciberseguridad (inversiones, coordinación con el CERT de referencia, elaboración de planes, cambios tecnológicos,...) como las correctivas (personas trabajando en el incidente, colaboradores coordinados, etc.).

Buena práctica:

Poner en valor de las acciones adoptadas y los recursos utilizados

Cualquier crisis representa una oportunidad para demostrar a la opinión pública la capacidad de su administración más cercana -el Ayuntamiento, la Diputación, el Cabildo, etc.- para solventar (en solitario o coordinadamente con otros agentes implicados) una situación compleja, demostrando que la gestión de la adversidad ha sido manejada adecuadamente.

8.4. La gestión de las partes interesadas

La gestión de las partes interesadas, afectadas o no, es uno de los pilares de la gestión de los ciberincidentes, que ha de ser incorporada por el Comité de Crisis entre sus funciones, pues todos los concejales/as y equipos, todas las áreas de la entidad, tienen sus propios colectivos a los que prestar atención.

En función del tipo de incidente y del escenario ocasionado, habrá que revisar todos los grupos de interés, sus expectativas y la estrategia a seguir con cada uno de ellos, y lo que es muy importante, asegurar que se conoce el interlocutor principal.

Por esta razón se aconseja desarrollar el denominado **"Mapa de partes interesadas"** donde las diferentes áreas de la entidad local deben identificar aquellos a los que puede estar afectando la situación y que requieren información a la vez que soluciones o medidas alternativas en caso de que la situación se alargue en el tiempo. A continuación, se apunta una relación de grupos de interés a modo orientativo, sin ánimo de exhaustividad:

- Ciudadanía en general y las entidades / asociaciones vecinales a través de los/as concejales/as de distrito / barrio.
- El Pleno municipal donde están representadas todas las fuerzas políticas.

- Entidades (culturales, deportivas, sociales, recreativas, etc.).
- Sector económico del municipio (industria, comercio) a través de sus asociaciones y su concejal/a asignado.
- Organismos autónomos de la corporación.
- Los sindicatos y entidades representativas de los trabajadores.
- Sector educativo y sanitario.
- Organismos supramunicipales (Diputación, consejo comarcal).
- Proveedores de bienes y servicios.
- Otros...

Todas las partes deben hacer esfuerzos para entender cuál la situación, dónde está el umbral mínimo de responsabilidad que le corresponde a cada uno y comprometerse a asumirla, así como es disponer o crear ad-hoc los canales ágiles y claros de interlocución para pilotar la vuelta a la normalidad.



9. FASE 4. CIERRE DE LA CRISIS Y DESACTIVACIÓN DEL COMITÉ DE CRISIS

Las organizaciones tienden a cerrar rápidamente las carpetas de las crisis, pero es importante dedicar esfuerzos a cerrar bien las crisis pues sus efectos e impactos perduran en el tiempo y, especialmente, para evitar que queden cuestiones mal resueltas que puedan reproducirse en el futuro.

En esta fase se diferencian dos (2) partes: la desactivación del Comité de Crisis y la de análisis post crisis y adopción de lecciones aprendidas.

9.1. Desactivación del Comité de Crisis

Las crisis por ciberincidente suelen ser largas y probablemente los equipos y servicios se irán restituyendo de forma segura progresivamente, lo que conlleva trabajar un tiempo en precario/degradado. En ese caso, la vuelta a la normalidad puede alargarse en el tiempo y la desactivación del Comité de Crisis es tan solo una de las acciones necesarias, pero no la única: el cierre de las crisis requiere un trabajo programado y estructurado que sigue implicando a diferentes partes de la entidad local.

En este sentido, se recomienda incorporar criterios que **ayuden a decidir la desactivación** del Comité de Crisis, por ejemplo:

1) Si el Equipo de Respuesta a Incidentes puede continuar trabajando sin el apoyo del Comité.

2) Si ya no es necesaria la implicación / dirección del personal del Comité y lo que queda pendiente puede ser ejecutado por otras personas de sus respectivos equipos.

3) Si se dispone de un Plan de Acción que garantiza que todos los temas abiertos son tratados adecuadamente y se ha establecido un programa para actualizaciones periódicas.

Independientemente de que se haya desconvocado el Comité de Crisis, se designará alguien que vele por el correcto archivo de la información generada durante el episodio, prestando especial atención a la información que pueda ser de utilidad a los servicios jurídicos en los meses siguientes y velando por las medidas de seguridad de la información.

9.2. Gestión post crisis y adecuación al ENS

Una vez cerrada la crisis, es fundamental llevar a cabo un análisis y valoración de todo lo ocurrido a fin de identificar aquellas acciones (buenas prácticas) que contribuyeron a gestionarla adecuadamente e identificar puntos débiles, todo ello con el objetivo de diseñar medidas que contribuyan a mejorar la respuesta de la entidad local en el futuro, lo que han de constituir las lecciones aprendidas de cada crisis.

En muchos casos la presión del día a día hace que el incidente no se cierre del modo más adecuado. La mejor práctica de un cierre correcto está, sin duda, en dedicar tiempo y recursos a extraer lecciones aprendidas e implementarlas en la realidad de la organización, así como en comunicar dicho cierre, tanto a nivel interno como externo.

Buena práctica:

Realizar un cierre formal de una crisis

En consecuencia, la realización 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 ciber crisis y en muchas ocasiones se realizan solo a medias.

En esta fase final, las tareas a realizar a fin de **garantizar un cierre que proporcione valor** a la entidad local son:

1. Realizar **el informe post crisis**, con un análisis en profundidad del desarrollo de la crisis, de sus causas y las propuestas de medidas a implementar. Este informe tiene por objetivo aprender de la experiencia, tanto para prevenir otras posibles crisis como para mejorar su gestión cuando estas ocurran. Para ello es importante que haya **espíritu crítico** para generar buenas prácticas, lecciones aprendidas y definir las medidas a implementar (con plazo, coste y responsable).
2. Definir el **Plan de Adecuación al ENS** y la metodología de mejora continua (seguimiento de las medidas acordadas). La adecuación al ENS es clave porque ayuda a reducir la superficie de exposición, a adoptar una mejor posición de seguridad, a potenciar (sino definir) la figura del Responsable de Seguridad de la Información y del Comité de Crisis.
3. Realizar una **reunión del Comité de Crisis** para este análisis post crisis. El objetivo es revisar el episodio y el informe preliminar de valoración post crisis realizado por el responsable operativo o coordinador, repasar las decisiones tomadas reflexionando de un modo crítico para extraer lecciones aprendidas y determinar cómo se van a introducir en la organización. El/la Alcalde/sa o Presidente/a decidirá qué otros miembros de las áreas del ayuntamiento o entidad local deberán asistir a esta reunión para completar y aportar su visión.
4. Transmitir el agradecimiento al personal de la entidad local, a los colaboradores externos que han intervenido, a la ciudadanía en general, a los miembros del Pleno, a quien se crea conveniente y comunicarles, además, que la crisis se ha cerrado formalmente.
5. Si se determina que la crisis ha producido un daño a la reputación en la entidad local, se definirá un Plan de Comunicación y relaciones con las partes interesadas/ afectadas que aborde las causas y propicie recuperar la confianza de las partes.

Hay que **tratar un incidente como una fuente de aprendizaje**, obteniendo conclusiones de lo sucedido mediante el análisis en profundidad y ajustando dichos aprendizajes a los planes de acción e inversión futuros.

9.3. Plan de Adecuación al ENS y metodología de mejora continua

Para la efectiva adopción del Plan de Adecuación que permita dar cumplimiento de lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), se toman como referencia, treinta y cinco (35) Requisitos Esenciales de Seguridad que se muestran a continuación, en los ámbitos de Marco Organizativo, Marco Operacional y Medidas de Protección, cuya valoración de cumplimiento o estado de implantación en las organizaciones mediante la herramienta de gobernanza INES, proporcionada por el Centro Criptológico Nacional, permitirá identificar su estado de avance respecto a la adecuación al ENS y la identificación de posibles deficiencias y riesgos existentes, contribuyendo a la disminución de la superficie de exposición, la adopción de una mejor posición de seguridad de la entidad y el establecimiento o consolidación de un Comité de Crisis y figura del Responsable de Seguridad de la Información.

Buena práctica:

Adoptar las lecciones aprendidas

Marco Organizativo (4):		Medidas de protección (17):	
[org.1]	Política de seguridad	[mp.per]	Gestión del personal
[org.2]	Normativa de seguridad	[mp.per.2]	Deberes y obligaciones
[org.3]	Procedimientos de seguridad	[mp.per.3]	Concienciación
[org.4]	Proceso de autorización	[mp.per.4]	Formación
Marco Operacional (14):		[mp.eq]	Protección de los equipos
[op.pl]	Planificación	[mp.eq.1]	Puesto de trabajo despejado
[op.pl.1]	Análisis de riesgos	[mp.eq.3]	Protección de dispositivos portátiles
[op.pl.3]	Adquisición de nuevos componentes	[mp.eq.4]	Otros dispositivos conectados a la red
[op.acc]	Control de acceso	[mp.com]	Protección de las comunicaciones
[op.acc.1]	Identificación	[mp.com.1]	Perímetro seguro
[op. acc.2]	Requisitos de acceso	[mp.com.2]	Protección de la confidencialidad
[op. acc.4]	Proceso de gestión de derechos de acceso	[mp.si]	Protección de los soportes de información
[op. acc.6]	Mecanismo de autenticación (usuarios de la organización)	[mp.si.3]	Custodia
[op.exp]	Explotación	[mp.si.4]	Transporte
[op.exp.1]	Inventario de activos	[mp.si.5]	Borrado y destrucción
[op.exp.2]	Configuración de seguridad	[mp.info]	Protección de la información
[op.exp.4]	Mantenimiento y actualizaciones de seguridad	[mp.info.1]	Datos de carácter personal
[op.exp.6]	Protección frente a código dañino	[mp.info.3]	Firma electrónica
[op.exp.7]	Gestión de incidentes	[mp.info.5]	Limpieza de documentos
[op.exp.8]	Registro de la actividad	[mp.info.6]	Copias de seguridad (backup)
[op.exp.10]	Protección de claves criptográficas	[mp.s]	Protección de los servicios
[op.mom]	Monitorización del sistema	[mps.1]	Protección del correo electrónico
[op.mom.2]	Sistema de métricas	[mps.3]	Protección de la navegación web

Tabla 3. Requisitos Esenciales de Seguridad

Es así como para la implantación efectiva de un Plan de Adecuación al ENS, que entre otras, enmarca unos principios básicos y unos requisitos mínimos que buscan dar confianza, tanto a los ciudadanos, como a la administración pública en el uso de los medios electrónicos, utilizando medidas e indicadores para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, se propone el desarrollo de una hoja de ruta, cuyas actuaciones tendrían una duración máxima de seis (6) meses, distribuidas en la ejecución de dos (2) grupos de actividades que se realizan de manera consecutiva, con entregables asociados a cada una de ellas en los ámbitos de **(i) Modelo de Gobierno y Cumplimiento, y (ii) Herramientas de Seguridad**, complementadas con el desarrollo de un análisis técnico enfocado a obtener la Superficie de Exposición de la organización, identificando las posibles vulnerabilidades, brechas de seguridad, deficiencias de configuración y riesgos existentes.

Buena práctica:

Diagnóstico de cumplimiento e iniciar el Plan de Adecuación del ENS en su caso.



En la Figura 11 y Figura 12, se describen las actividades para cada ámbito y cronograma (estimación de tiempo) asociado a su ejecución:

· **(i) Modelo de Gobierno y Cumplimiento:** inicio de la aplicación del Modelo μ CeENS a partir del cual se diagnóstica si el nivel de riesgo de la organización es asumible y establece un Plan de Adecuación que contribuya a la mejora de la postura de seguridad. Adicionalmente, se identifican las necesidades y se estiman las actuaciones prioritarias a implementar, respecto al marco de Gobernanza, determinación de roles y responsabilidades, y cumplimiento para la efectiva protección de la información y gestión del dato.

· **(ii) Herramientas de Seguridad:** a partir de la validación del riesgo asumible y el análisis de la Superficie de Exposición, se determinan los servicios, sistemas y activos críticos para el desarrollo de auditorías técnicas en caja gris, pentesting o ejercicios de hacking ético, junto con la identificación del despliegue de medidas proactivas que, a partir de los diagnósticos de las actividades previas, contribuya a adoptar una mejor postura de seguridad adecuada a la potencial amenaza.



Figura 11. Actividades y entregables asociados a cada ámbito.

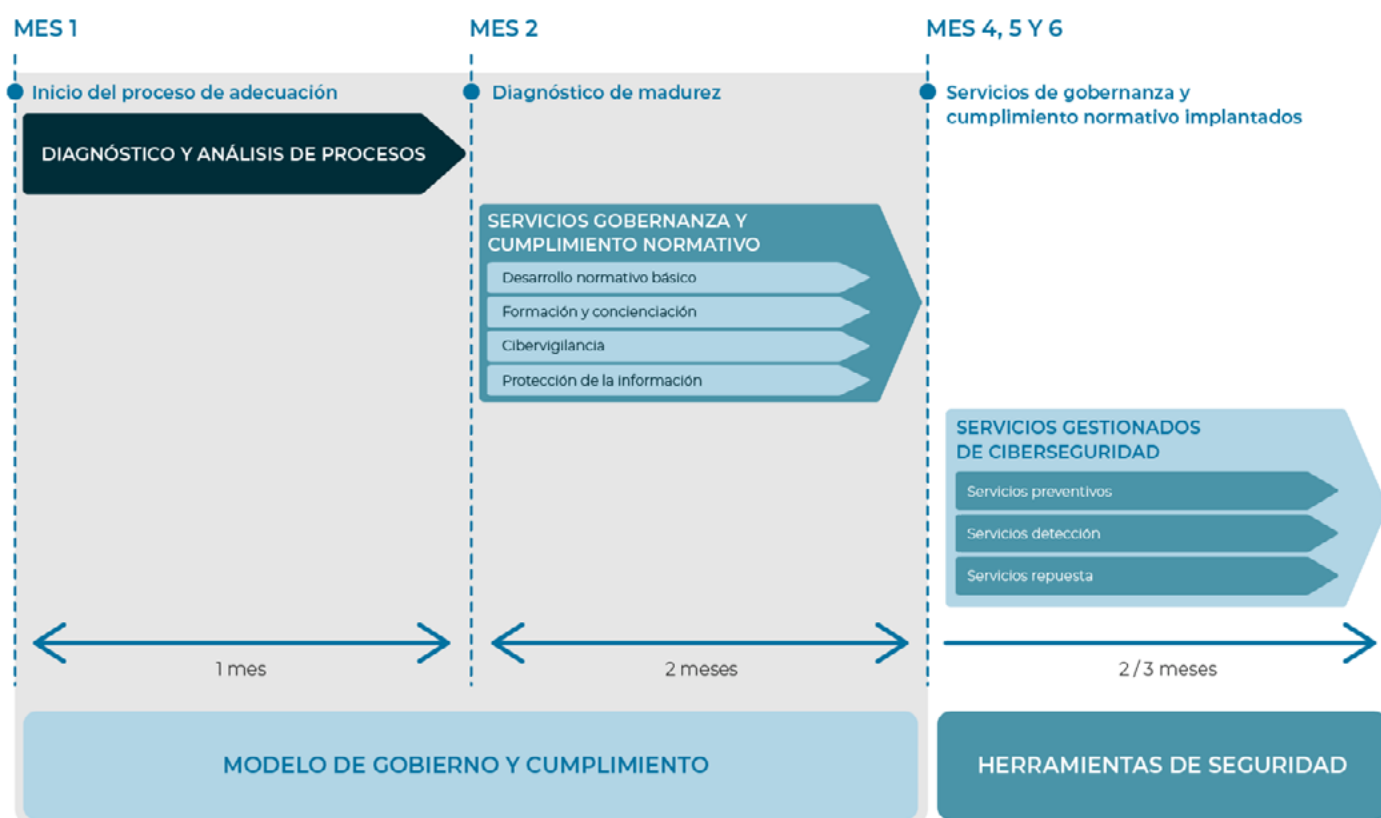


Figura 12 Cronograma establecido para el desarrollo de las actividades



El desarrollo de la hoja de ruta propuesta facilitará tanto la adecuación al ENS por parte de las entidades, así como a organizar y centrar los esfuerzos en torno a las siguientes actuaciones:

- **Análisis global del riesgo** mediante la gestión de la seguridad de los sistemas de información a partir de la información de los activos de la organización y la valoración del impacto que puede suponer la pérdida de estos.
- **Identificación de medidas a nivel técnico, normativo y procedimental** que permitan lograr una protección adecuada tanto de la información como de los sistemas críticos de las entidades para apoyar la efectiva prestación de servicios a la ciudadanía y avanzar en el plan de adecuación al ENS.
- **Apoyo a la gestión de la Prevención Proactiva** en base a las herramientas de gobernanza proporcionadas por el Centro Criptológico Nacional para la implantación del servicio de gobernanza y cumplimiento, de manera escalonada, de acuerdo con las necesidades de la entidad.

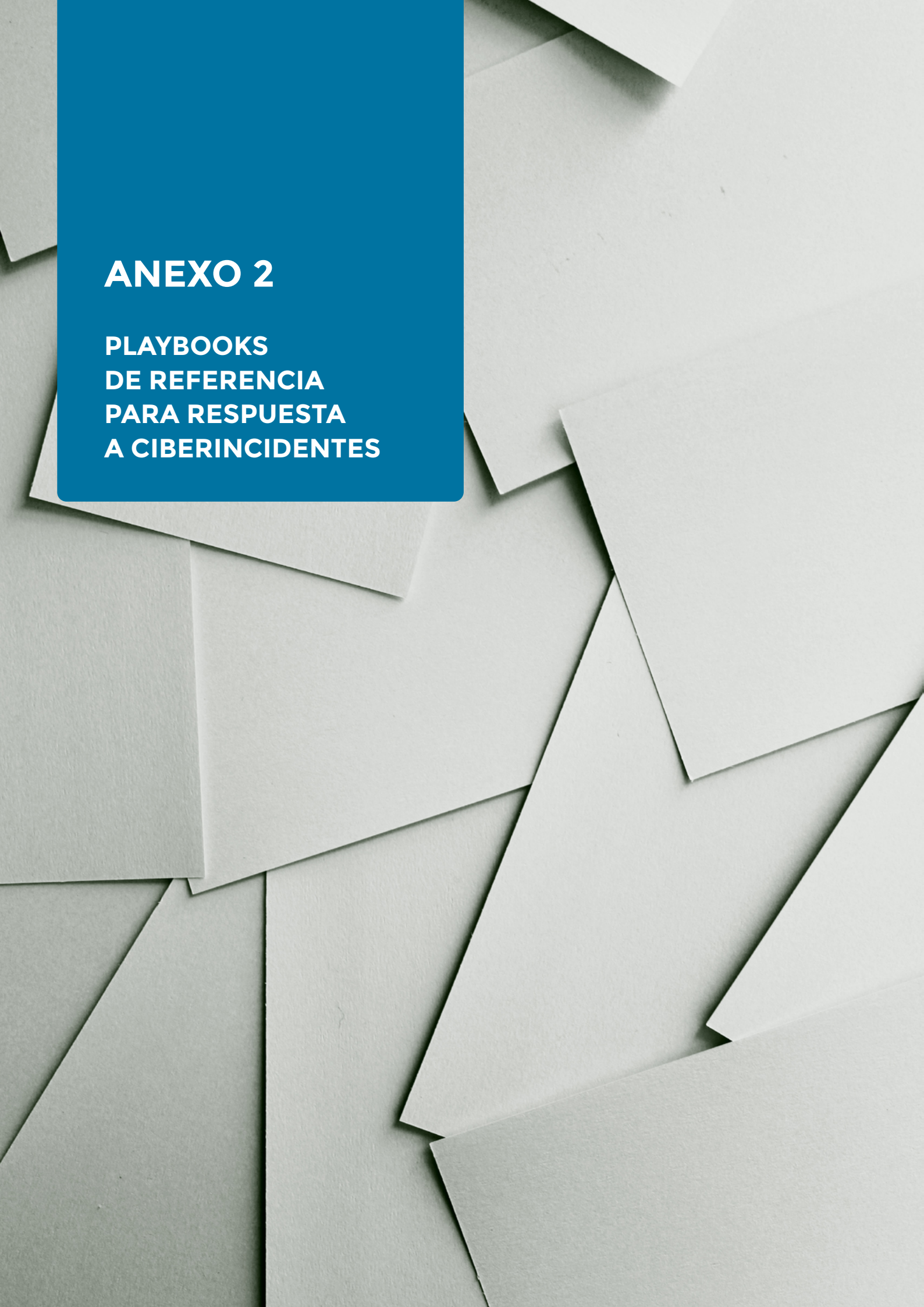
ANEXO 1

**PROTOCOLO DE
DATOS A APORTAR
POR PARTE DEL
ORGANISMO
AFECTADO POR
RANSOMWARE**



La entidad aportará la información siguiente:

- El **personal técnico** de la entidad que actúa **como POC** y canalizador de las peticiones sobre el incidente.
- El **teléfono** y correo del siguiente personal de la entidad:
 - Responsable de seguridad
 - Responsable de comunicaciones
 - Responsable de sistemas
 - Responsable del sistema de virtualización
- ¿Qué y cuándo se ha detectado?
- ¿Cuántos equipos afectados se cree que hay?
- ¿Los equipos afectados son servidores físicos o virtuales?
- En caso de que sean virtuales, ¿se ha cifrado a nivel de máquina (es decir, archivos dentro de la máquina virtual) o a nivel de hipervisor (todo el disco duro virtual)?
- Envío de la nota de rescate si se ha recibido y se dispone de ella
- ¿Se dispone de copia de seguridad (en especial de los datos cifrados) ?, en caso afirmativo, ¿fecha de la última?
- ¿Se conoce si los servidores de copia de seguridad han sido afectados?
- ¿Se han tomado acciones para la mitigación? ¿Cuáles?
- ¿Existe acceso remoto por VDI (tipo Citrix)?
- ¿Existe acceso remoto por VPN?
- ¿Todos los dispositivos son corporativos?
- Credenciales usadas o comprometidas. Protocolos. Directorio activo
- Comunicaciones. Monitorización de la red. Distribución de la red.
- ¿Hay un SOC desplegado?
- ¿Antivirus? ¿EDR?
- ¿Se dispone de doble factor en los accesos remotos a la entidad (tanto VPN como VDI)?
¿Qué fecha de logs tiene en este aspecto?
- Proporcionar un fichero cifrado
- Listado de servicios críticos de la entidad
- ¿Dispone la entidad de listas blancas?

The background of the page consists of several overlapping, light gray rectangular papers of various sizes and orientations, creating a layered, geometric effect. A solid blue rectangle is positioned in the upper left corner, containing the title text.

ANEXO 2

PLAYBOOKS DE REFERENCIA PARA RESPUESTA A CIBERINCIDENTES

Filtración de Datos

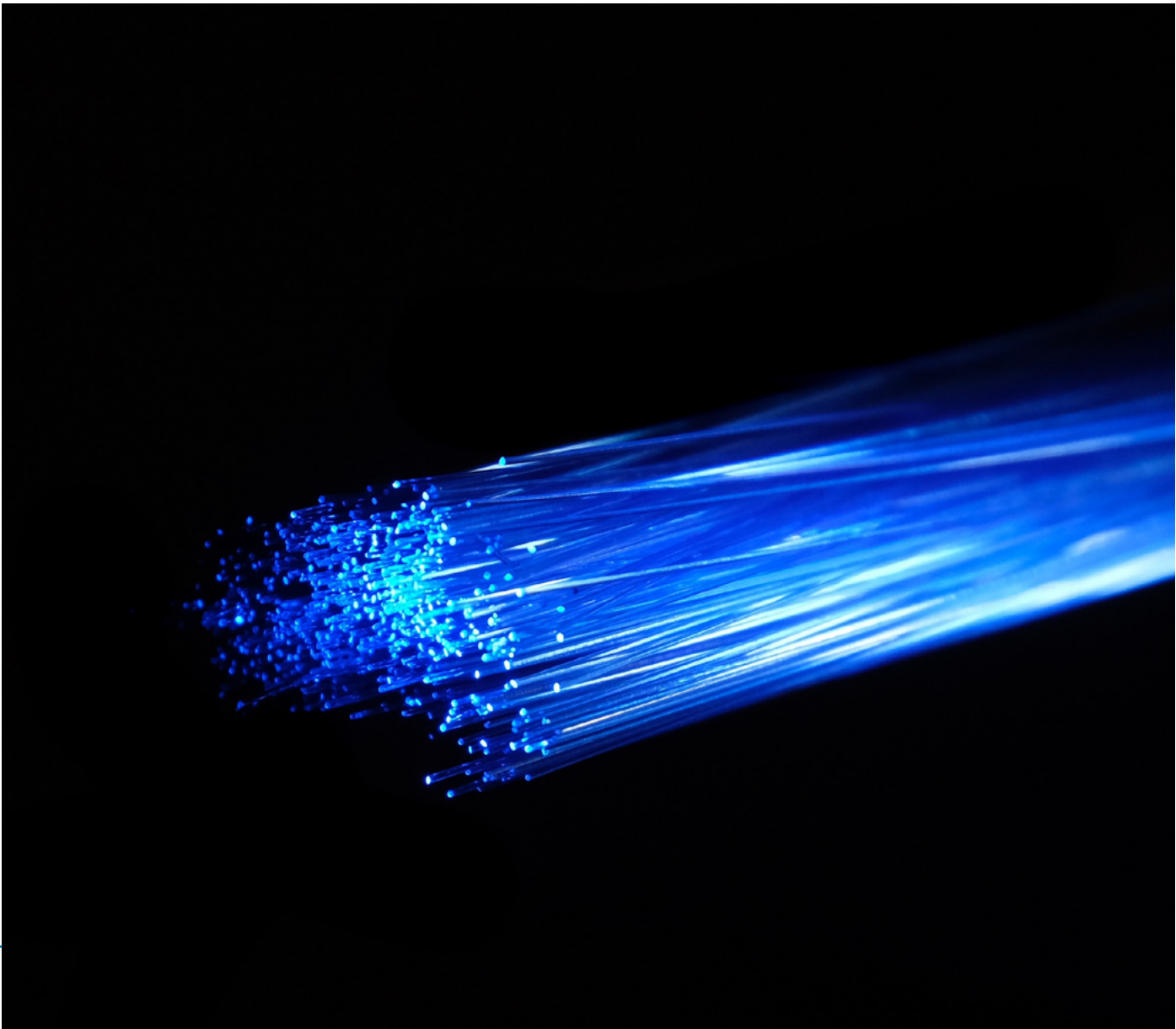
PLAYBOOK			
FILTRACIÓN DE DATOS	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Planificación	Elaboración de un Plan de Respuesta 1.1 Conformación de un equipo de respuesta identificando roles y responsabilidades para la planificación, detección y respuesta. 1.2 Elaboración de un plan de respuesta ante ciberincidentes de filtración de datos, teniendo en cuenta recursos disponibles y contemplando el riesgo y recuperación. 1.3 Revisión y aprobación del plan de respuesta ante ciberincidentes de filtración de datos. 1.4 Elaboración de un programa de comunicación interno y externo, incluyendo la concienciación respecto al incidente y definición del portavoz. 1.5 Inventario de activos relacionados con datos sensibles / críticos. Implementación de Medidas Preventivas 2.1 Uso de herramientas básicas y complementarias para prevenir la fuga de información (detección de accesos o usos no autorizados, uso de firewall entre redes para restringir tráfico, sistemas de prevención de intrusiones, etc...) 2.2 Documentación y análisis del incidente. Definición de parámetros de detección 3.1 Establecimiento de indicadores para la detección de filtración de datos	Elaboración de un Plan de Respuesta 1.1 Responsable de seguridad de la información 1.2 Responsable de seguridad de la información, responsable de sistemas, equipo legal y continuidad de negocio. 1.3 Alcalde, responsable de seguridad de la información, responsables de sistemas, equipo legal, continuidad de negocio y responsable de comunicaciones. 1.4 Responsable de comunicaciones y responsable de seguridad de la información. 1.5 Responsable de seguridad de la información y responsable de recursos humanos. Implementación de Medidas Preventivas 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información y responsable de sistemas. Definición de parámetros de detección 3.1 Responsable de seguridad de la información.
	Detección	Evaluación del incidente 1.1 Categorización del ciberincidente como ataque de filtración de datos y determinación del nivel de criticidad. Análisis del incidente 2.1 Verificación de la legitimidad de los datos / información filtrada. 2.2 Análisis de distintas fuentes de información para entender el objetivo del ataque. Contención del incidente 3.1 Implementación de medidas físicas y lógicas de cuarentena de los activos infectados, restringiendo y limitando su acceso a las redes. 3.2 Implementación de medidas adicionales para la navegación en internet, uso de dispositivos extraíbles y listas blancas.	Evaluación del incidente 1.1 Responsable de seguridad de la información. Análisis del incidente 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información y responsable de sistemas. Contención del incidente. 3.1 Responsable de seguridad de la información y encargado de la seguridad física. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información. 3.4 Responsable de seguridad de la información.

PLAYBOOK			
FILTRACIÓN DE DATOS	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Respuesta	Evaluación del incidente 1.1 Categorización del ciberincidente como ataque de filtración de datos y determinación del nivel de criticidad. Análisis del incidente 2.1 Verificación de la legitimidad de los datos / información filtrada. 2.2 Análisis de distintas fuentes de información para entender el objetivo del ataque. Contención del incidente 3.1 Implementación de medidas físicas y lógicas de cuarentena de los activos infectados, restringiendo y limitando su acceso a las redes. 3.2 Implementación de medidas adicionales para la navegación en internet, uso de dispositivos extraíbles y listas blancas. 3.3 Suspensión de las credenciales de inicio de sesión de las cuentas de los usuarios comprometidos y deshabilitación de servicios afectados en los servidores. 3.4 Verificación de firmas de antivirus y malware en los equipos. Documentación y control de evidencias 4.1 Elaboración de copias de los archivos (logs) de los elementos de seguridad perimetral y de los dispositivos afectados. 4.2 Identificación y análisis de paquetes de red para identificar direcciones IP, puertos, protocolos, agentes, etc. Análisis forense 5.1 Análisis forense de la amenaza para identificar la motivación del ataque y su objetivo, el método utilizado y posible actor involucrado, etc. 5.2 Comunicación del estado del incidente y su gestión ante los actores de interés. Erradicación del incidente 6.1 Instalación de parches de seguridad que mitiguen la explotación de la vulnerabilidad asociada con el ataque. 6.2 Implementación de configuraciones y controles personalizados de seguridad en los servidores, aplicaciones y segmentos de red. Recuperación de servicios afectados 7.1 Recuperación de la disponibilidad de los dispositivos y sistemas comprometidos. Cierre del incidente 8.1 Generación del informe e identificación de actividades de mejora.	Evaluación del incidente 1.1 Responsable de seguridad de la información. Análisis del incidente 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información y responsable de sistemas. Contención del incidente 3.1 Responsable de seguridad de la información y encargado de la seguridad física. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información. 3.4 Responsable de seguridad de la información. Documentación y control de evidencias 4.1 Responsable de seguridad de la información. 4.2 Responsable de seguridad de la información. Análisis forense 5.1 Responsable de seguridad de la información. 5.2 Responsable de seguridad de la información y responsable de comunicaciones. Erradicación del incidente 6.1 Responsable de seguridad de la información. 6.2 Responsable de seguridad de la información. Recuperación de servicios afectados 7.1 Responsable de seguridad de la información. Cierre del incidente 8.1 Responsable de seguridad de la información y responsable de sistemas.

Denegación de Servicio (DDoS)

PLAYBOOK			
DENEGACIÓN DE SERVICIO (DDoS)	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Planificación	Elaboración de un Plan de Respuesta 1.1 Conformación de un equipo de respuesta identificando roles y responsabilidades para la planificación, detección y respuesta. 1.2 Elaboración de un plan de respuesta, teniendo en cuenta recursos disponibles y contemplando el riesgo y recuperación. 1.3 Revisión y aprobación del plan de que incluya la verificación del cumplimiento y efectividad de las actividades, las responsabilidades y el flujo de escalamiento. 1.4 Elaboración de un programa de comunicación interno y externo, incluyendo la concienciación respecto al incidente y definición del portavoz. Implementación de Medidas Preventivas 2.1 Protección de los servicios publicados o expuestos en redes públicas, como el correo electrónico, el portal Web y servicios DNS entre otros. 2.2 Inclusión en la etapa de diseño de proyectos de cambios o nuevos servicios, las técnicas de mitigación de ataques de denegación de servicio (DDoS), 2.3 Fortalecimiento de la configuración de la infraestructura (red, servidores, aplicaciones y sistemas operativos) que podrían verse afectadas por un ataque de denegación de servicio (DDoS), 2.4 Documentación y análisis del incidente. Definición de parámetros de detección 3.1 Definición de indicadores para la detección de eventos anómalos relacionados al ataque de denegación de servicio (DDoS) en base al tráfico promedio y el límite máximo tolerable. 3.2 Definición de la estructura de registros (logs) que son necesarios habilitar en los elementos de infraestructura (servidores, routers, entre otros), protección perimetral (firewall, IPS, entre otros) y sondas de detección que permitan obtener visibilidad de las conexiones (dirección IP origen y destino, protocolo), volumen de tráfico, entre otros. 3.3 Configuración y análisis de los eventos anómalos que pasan a través del tráfico saliente, principalmente en los protocolos IRC, P2P y HTTPS.	Elaboración de un Plan de Respuesta 1.1 Alta dirección. 1.2 Responsable de seguridad de la información, responsable de sistemas, equipo legal y continuidad de negocio. 1.3 Alcalde, responsable de seguridad de la información, responsable de sistemas, equipo legal, continuidad de negocio y responsable de comunicaciones. 1.4 Responsable de comunicaciones y responsable de seguridad de la información. Implementación de Medidas Preventivas 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información. 2.3 Responsable de seguridad de la información y responsable de sistemas. 2.4 Responsable de seguridad de la información. Definición de parámetros de detección 3.1 Responsable de seguridad de la información. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información.

PLAYBOOK			
DENEGACIÓN DE SERVICIO (DDoS)	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Detección	Detección del incidente 1.1 Monitorización y detección oportuna de eventos anómalos en el tráfico de red (paquetes desconocidos o no identificados que vengan desde orígenes desconocidos, incremento en el volumen de los datos cifrados, incremento anómalo en el uso del ancho de banda, etc...). 1.2 Revisión y análisis de alertas de los componentes de seguridad perimetral (Firewall, IPS, Sistemas anti DDoS, etc...). 1.3 Revisión y análisis de las notificaciones provenientes de los proveedores. 1.4 Revisión y análisis en fuentes de ciberinteligencia de las nuevas tendencias en relación a los ataques de denegación de servicio (DDoS).	Detección del incidente 1.1 Responsable de seguridad de la información 1.2 Responsable de seguridad de la información 1.3 Responsable de seguridad de la información. 1.4 Responsable de seguridad de la información.



PLAYBOOK			PRINCIPALES ACTORES INVOLUCRADOS
DENEGACIÓN DE SERVICIO (DDoS)			
	Respuesta	Evaluación del incidente 1.1 Categorización del ciberincidente como ataque de denegación de servicio (DDoS) y determinación del nivel de criticidad. Análisis del incidente 2.1 Obtención y análisis de distintas fuentes de información / datos necesarios para poder comprender detalles del ciberataque. 2.2 Comunicar el análisis del incidente al CERT de referencia. 2.3 Ejecución del plan de respuesta / playbook de que se disponga. Contención del incidente 3.1 Identificación de qué tráfico descartar o permitir según el historial de origen del tráfico malicioso o legítimo. 3.2 Comunicación y solicitud de bloqueo de tráfico malicioso al proveedor de internet. 3.3 Si el nivel de criticidad del incidente lo requiere, recurrir al plan de continuidad de negocio y procedimiento de recuperación ante desastres para trasladar las operaciones de TI a sitios alternativos. Documentación y control de evidencias 4.1 Elaboración de copias de los archivos (logs) de los componentes de seguridad perimetral y de los dispositivos afectados. 4.2 Identificación y análisis de paquetes de red para identificar direcciones IP, puertos, protocolos, agentes, etc. Análisis forense 5.1 Análisis forense de la amenaza para identificar la motivación del ataque y su objetivo, el método utilizado y posible actor involucrado, etc. 5.2 Comunicación del estado del incidente y su gestión ante los actores de interés. Erradicación del incidente 6.1 Instalación de parches de seguridad que mitiguen la explotación de la vulnerabilidad asociada con el ataque. 6.2 Implementación de configuraciones y controles personalizados de seguridad en los servidores, aplicaciones y segmentos de red. Recuperación de servicios afectados 7.1 Recuperación de la disponibilidad de los dispositivos y sistemas comprometidos. Cierre del incidente 8.1 Generación del informe e identificación de actividades de mejora.	Evaluación del incidente 1.1 Responsable de seguridad de la información. Análisis del incidente 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información. 2.3 Responsable de seguridad de la información y responsable de sistemas. Contención del incidente 3.1 Responsable de seguridad de la información. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información. Documentación y control de evidencias 4.1 Responsable de seguridad de la información. 4.2 Responsable de seguridad de la información. Análisis forense 5.1 Responsable de seguridad de la información. 5.2 Responsable de seguridad de la información y responsable de comunicaciones. Erradicación del incidente 6.1 Responsable de seguridad de la información. 6.2 Responsable de seguridad de la información. Recuperación de servicios afectados 7.1 Responsable de seguridad de la información. Cierre del incidente 8.1 Responsable de seguridad de la información y responsable de sistemas.

Malware

PLAYBOOK			
MALWARE	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Planificación	Elaboración de un Plan de Respuesta 1.1 Conformación de un equipo de respuesta identificando roles y responsabilidades para la planificación, detección y respuesta. 1.2 Elaboración de un plan de respuesta, teniendo en cuenta recursos disponibles y contemplando el riesgo y recuperación. 1.3 Revisión y aprobación del plan de que incluya la verificación del cumplimiento y efectividad de las actividades, las responsabilidades y el flujo de escalado. 1.4 Elaboración de un programa de comunicación interno y externo, incluyendo la concienciación respecto al incidente y definición del portavoz. Implementación de Medidas Preventivas 2.1 Protección de todos sus dispositivos (equipos de escritorio, equipos portátiles y servidores) a través de un software antivirus y antimalware, 2.2 Implementación de herramientas de mitigación que detecten y detengan los ataques de malware. 2.3 Documentación y análisis del incidente. Definición de parámetros de detección 3.1 Definición de indicadores para la detección de eventos anómalos relacionados con el ataque de malware. 3.2 Habilitación en los componentes de infraestructura (servidores, routers, etc...) y de protección perimetral (firewall, IPS, etc...) los registros (Logs) para obtener visibilidad de los paquetes, volumen, origen, destino, protocolos, entre otros. 3.3 Análisis de los eventos anómalos que se generan por los servicios y aplicaciones desconocidos o inesperados.	Elaboración de un Plan de Respuesta 1.1 Alta dirección. 1.2 Responsable de seguridad de la información, responsable de sistemas, equipo legal, y continuidad de negocio. 1.3 Alcalde, responsable de seguridad de la información, responsable de sistemas, equipo legal, continuidad de negocio y responsable de comunicaciones. 1.4 Responsable de comunicaciones y responsable de seguridad de la información. Implementación de Medidas Preventivas 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información. 2.3 Responsable de seguridad de la información y responsable de sistemas. Definición de parámetros de detección 3.1 Responsable de seguridad de la información. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información.
	Detección	Detección del incidente 1.1 Monitorización y detección oportuna de eventos anómalos en el tráfico de red (paquetes desconocidos o no identificados que vengan desde orígenes desconocidos, incremento en el volumen de los datos cifrados, incremento anómalo en el uso del ancho de banda, etc...). 1.2 Revisión y análisis de las alertas de los elementos de seguridad perimetral (Firewall, IPS, Sistemas anti DDoS, entre otros) para identificar posibles ataques de malware, por ejemplo, ICMP virus, troyanos, spyware, RAT, ransomware, rogueware, malware periférico, entre otros. 1.3 Revisión y análisis de las notificaciones provenientes de los proveedores. 1.4 Revisión y análisis en fuentes de ciberinteligencia de las nuevas tendencias en relación a los ataques de malware.	Detección del incidente 1.1 Responsable de seguridad de la información 1.2 Responsable de seguridad de la información 1.3 Responsable de seguridad de la información. 1.4 Responsable de seguridad de la información.

PLAYBOOK			
MALWARE	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Respuesta	Evaluación del incidente 1.1 Categorización del ciberincidente como ataque de malware y determinación del nivel de criticidad. Análisis del incidente 2.1 Obtención y análisis de distintas fuentes de información y datos necesarios para poder comprender detalles del ciberataque. 2.2 Comunicar el análisis del incidente al CERT de referencia. 2.3 En caso de que el incidente se encuentre entre los niveles de criticidad MEDIA y BAJO, verificar si se cuenta con un plan de respuesta específico para este tipo de incidente (ataque de malware), y continúe con las actividades contención y erradicación. Contención del incidente 3.1 Inicio de cuarentena (física o lógica) de los activos infectados, restringir o limitar el acceso a las redes mediante los dispositivos de seguridad perimetral y a las instalaciones mediante controles físicos. 3.2 Finalización de las conexiones o servicios no deseados en los servidores. 3.3 Suspensión de credenciales de inicio de sesión de las cuentas de los usuarios comprometidos y deshabilitar los servicios afectados en los servidores. 3.4 Adecuación de las reglas de comportamiento en el SIEM, Firewall y software antivirus / antimalware, y continuar monitorizando la red para detectar cualquier nueva infección que pueda implicar su propagación en la red. 3.5 Verificación de que el antivirus / antimalware en todos los dispositivos cuenten con las últimas firmas disponibles. Documentación y control de evidencias 4.1 Elaboración de copias de los archivos (logs) de los componentes de seguridad perimetral y de los dispositivos afectados. 4.2 Identificación y análisis de paquetes de red para identificar direcciones IP, puertos, protocolos, agentes, etc. 4.3 Elaboración de copias de seguridad del Malware que afecta a los dispositivos, y realice la simulación en herramientas SandBox.	Evaluación del incidente 1.1 Responsable de seguridad de la información. Análisis del incidente 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información. 2.3 Responsable de seguridad de la información y responsable de sistemas. Contención del incidente 3.1 Responsable de seguridad de la información. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información. 3.4 Responsable de seguridad de la información. 3.5 Responsable de seguridad de la información. Documentación y control de evidencias 4.1 Responsable de seguridad de la información. 4.2 Responsable de seguridad de la información. 4.3 Responsable de seguridad de la información.

PLAYBOOK			
	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
MALWARE	Respuesta	Análisis forense 5.1 Análisis forense de la amenaza para identificar la motivación del ataque y su objetivo, el método utilizado y posible actor involucrado, etc. 5.2 Comunicación del estado del incidente y su gestión ante los actores de interés.	Análisis forense 5.1 Responsable de seguridad de la información. 5.2 Responsable de seguridad de la información y responsable de comunicaciones.
		Erradicación del incidente 6.1 Instalación de parches de seguridad que mitiguen la explotación de la vulnerabilidad asociada al ataque. 6.2 Implementación de configuraciones y controles personalizados de seguridad en los servidores, aplicaciones y segmentos de red.	Erradicación del incidente 6.1 Responsable de seguridad de la información. 6.2 Responsable de seguridad de la información.
		Recuperación de servicios afectados 7.1 Recuperación de la disponibilidad de los dispositivos y sistemas comprometidos.	Recuperación de servicios afectados 7.1 Responsable de seguridad de la información.
		Cierre del incidente 8.1 Generación del informe e identificación de actividades de mejora.	Cierre del incidente 8.1 Responsable de seguridad de la información y responsable de sistemas.



Ataques Internos (Insiders)

PLAYBOOK			
ATAQUES INTERNOS (INSIDERS)	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Planificación	Elaboración de un Plan de Respuesta 1.1 Conformación de un equipo de respuesta identificando roles y responsabilidades para la planificación, detección y respuesta. 1.2 Elaboración de un plan de respuesta, teniendo en cuenta recursos disponibles y contemplando el riesgo y recuperación. 1.3 Revisión y aprobación del plan que incluya la verificación del cumplimiento y efectividad de las actividades, las responsabilidades y el flujo de escalado. 1.4 Elaboración de un programa de comunicación interno y externo, incluyendo la concienciación respecto al incidente y definición del portavoz. Implementación de Medidas Preventivas 2.1 Implementación y uso de soluciones de gestión de identidad y acceso (IAM) al implementar también la segregación de funciones y soluciones de gestión de identidad privilegiada (PIM). 2.2 Implementación de soluciones de gobierno de identidad que definan y apliquen el control de acceso basado en roles y en el principio de mínimo privilegio. 2.3 Implementación herramientas complementarias que ayuden en la mitigación de los accesos no autorizados (factores de autenticación, firewall basado en host, uso de listas blancas de aplicaciones (Applications Control, etc...)) Definición de parámetros de detección 3.1 Definición de indicadores para la detección de eventos anómalos relacionados a ataques de accesos no autorizados. 3.2 Habilitación en los componentes de infraestructura (servidores, routers, entre otros) y de protección perimetral (firewall, IPS, entre otros) los registros (Logs) para obtener visibilidad de los paquetes, volumen, origen, destino y protocolos, entre otros. 3.3 Análisis de los eventos anómalos que se generan por los servicios y aplicaciones desconocidos o inesperados, que se inician automáticamente en el arranque del sistema.	Elaboración de un Plan de Respuesta 1.1 Alta dirección. 1.2 Responsable de seguridad de la información, responsable de sistemas, equipo legal y continuidad de negocio. 1.3 Alcalde, responsable de seguridad de la información, responsable de sistemas, equipo legal, continuidad de negocio y responsable de comunicaciones. 1.4 Responsable de comunicaciones y responsable de seguridad de la información. Implementación de Medidas Preventivas 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información. 2.3 Responsable de seguridad de la información. Definición de parámetros de detección 3.1 Responsable de seguridad de la información. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información.

PLAYBOOK			
ATAQUES INTERNOS (INSIDERS)	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Detección	Detección del incidente 1.1 Monitorización y detección oportuna de eventos anómalos en el tráfico de red (paquetes desconocidos o no identificados que vengan desde orígenes desconocidos, incremento en el volumen de los datos cifrados, incremento anómalo en el uso del ancho de banda, etc...). 1.2 Revisión y análisis de las alertas de los elementos de seguridad perimetral (Firewall, IPS, Sistemas DLP, entre otros) para identificar posibles ataques de Insiders. 1.3 Revisión y análisis en las fuentes de ciberinteligencia de las nuevas tendencias en relación a los ataques de Insiders, considerando las nuevas amenazas o variantes en las ya existentes, nuevas vulnerabilidades o incidentes en el contexto nacional e internacional.	Detección del incidente 1.1 Responsable de seguridad de la información 1.2 Responsable de seguridad de la información 1.3 Responsable de seguridad de la información.
	Respuesta	Evaluación del incidente 1.1 Categorización del ciberincidente como ataque de Insider y determinación del nivel de criticidad. Análisis del incidente 2.1 Obtención y análisis de distintas fuentes de la información y datos necesarios para poder comprender detalles del ciberataque. 2.2 En caso el incidente se encuentre entre los niveles de criticidad MEDIA y BAJO, verifique si se cuenta con un plan de respuesta específico para este tipo de incidente, y continúe con las actividades de contención y erradicación. Contención del incidente 3.1 Inicio de cuarentena (física o lógica) de los activos infectados, restringir o limitar el acceso a las redes mediante los dispositivos de seguridad perimetral y a las instalaciones mediante controles físicos. 3.2 Finalización de las conexiones o servicios no deseados en los servidores. 3.3 Suspensión de credenciales de inicio de sesión de las cuentas de los usuarios comprometidos y deshabilitar los servicios afectados en los servidores. 3.4 Implementación de restricciones adicionales en la navegación a internet, en el uso de dispositivos extraíbles y listas blancas para el control de aplicaciones. 3.5 Adecuación de las reglas de comportamiento en el SIEM, herramienta DLP, Firewall y software de antivirus / antimalware, y continuar monitorizando la red para detectar cualquier nueva amenaza de Insiders. 3.6 Verificación de que el antivirus / antimalware en todos los dispositivos cuenten con las últimas firmas disponibles.	Evaluación del incidente 1.1 Responsable de seguridad de la información. Análisis del incidente 2.1 Responsable de seguridad de la información. 2.2 Responsable de seguridad de la información. Contención del incidente 3.1 Responsable de seguridad de la información. 3.2 Responsable de seguridad de la información. 3.3 Responsable de seguridad de la información. 3.4 Responsable de seguridad de la información. 3.5 Responsable de seguridad de la información. 3.6 Responsable de seguridad de la información.

PLAYBOOK			
ATAQUES INTERNOS (INSIDERS)	ETAPAS	ACTIVIDADES CONTEMPLADAS	PRINCIPALES ACTORES INVOLUCRADOS
	Respuesta	Documentación y control de evidencias 4.1 Elaboración de copias de los archivos (logs) de los componentes de seguridad perimetral y de los dispositivos afectados. 4.2 Identificación y análisis de paquetes de red para identificar direcciones IP, puertos, protocolos, agentes, etc.	Documentación y control de evidencias 4.1 Responsable de seguridad de la información. 4.2 Responsable de seguridad de la información.
		Análisis forense 5.1 Análisis forense de la amenaza para identificar la motivación del ataque y su objetivo, el método utilizado y posible actor involucrado, etc. 5.2 Comunicación del estado del incidente y su gestión ante los actores de interés.	Análisis forense 5.1 Responsable de seguridad de la información. 5.2 Responsable de seguridad de la información y responsable de comunicaciones.
		Erradicación del incidente 6.1 Instalación de parches de seguridad que mitiguen la explotación de la vulnerabilidad asociada con el ataque. 6.2 Implementación de configuraciones y controles personalizados de seguridad en los servidores, aplicaciones y segmentos de red.	Erradicación del incidente 6.1 Responsable de seguridad de la información. 6.2 Responsable de seguridad de la información.
		Recuperación de servicios afectados 7.1 Recuperación de la disponibilidad de los dispositivos y sistemas comprometidos.	Recuperación de servicios afectados 7.1 Responsable de seguridad de la información.
		Cierre del incidente 8.1 Generación del informe e identificación de actividades de mejora.	Cierre del incidente 8.1 Responsable de seguridad de la información y responsable de sistemas.

