APROXIMACIÓN AL MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD

CCN
centro criptológico nacional

Año 2022

PREVENCIÓN PROACTIVA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de Edición: enero de 2022

ÍNDICE

1

INTRODUCCIÓN

El escenario actual de la ciberseguridad se caracteriza por las constantes oleadas de ciberataques de alta persistencia y sofisticación tecnológica, originados por atacantes que, además de los escenarios tradicionales, están explotando el crecimiento exponencial de la superficie de exposición que comporta el trabajo a distancia.

La postura de los responsables de seguridad ante un panorama complejo de amenazas exige, en consecuencia, con lo anterior, contemplar alternativas a la mera respuesta reactiva, incorporando la prevención proactiva de los incidentes al elenco de tácticas, técnicas y procedimientos imprescindibles para un adecuado tratamiento de estas amenazas.

Todo lo anterior cobra especial importancia cuando el éxito de la transformación digital depende, en gran medida, de garantizar los requisitos mínimos de seguridad protegiendo la información tratada y los servicios prestados, elementos consustanciales al desarrollo de nuestra sociedad.

La experiencia está demostrando que hoy en día la clave para la ciberseguridad es medir y determinar indicadores para poder parametrizar la amenaza, identificar el estado de seguridad y así determinar la superficie de exposición en función de las amenazas conocidas, vulnerabilidades de la tecnología, deficiencias en la implementación de la seguridad y mala praxis de los usuarios.

Es decir, si se conoce el problema, las carencias asociadas (vulnerabilidades, deficiencias de configuración y mala praxis) y potenciales amenazas, se puede predecir el ciberataque ya que se tiene constancia de cuáles son los flancos más débiles y las posibles vías de explotación con lo que se puede establecer una hoja de ruta que permita a la entidad adelantarse a la amenaza y, lo que es más importante, cómo poder gestionarlo a priori ante el menor indicio de materialización. Es decir, se tiene la posibilidad de gestionar una situación adversa porque se mide y parametriza el problema.

Es lo mismo que se hace cuando se aplica el ciclo de inteligencia al estudio de las situaciones: se construyen modelos, se analiza el problema y se elabora una hipótesis fundamentada (valoración, análisis, integración e interpretación) de cara a optimizar los recursos de los que la entidad dispone y priorizar la asignación de los mismos. En otras palabras, se posibilita la priorización de los recursos disponibles mejorando la capacidad de reacción y mitigación simplemente por haber implementado capacidades de prevención proactiva.

Lo que se intenta hacer es responder a la razón de ser de la ciberseguridad, que no es otra que hacer un análisis de la situación y su previsible evolución preparando la respuesta a través de una hoja de ruta adaptada a la amenaza. Lo que se está haciendo es prospectiva, adelantarse al futuro porque se puede medir y parametrizar la amenaza, predecir el potencial ataque y la materialización del ataque. Se puede anticipar y adelantarse a la situación porque se tiene conocimiento de la situación y se conoce porque se mide y se mide porque se disponen de capacidades de vigilancia.

De esta manera, la vigilancia se convierte en un elemento de apoyo a la decisión. En concreto, un profundo análisis de la situación donde se busca establecer un proceso de MEJORA CONTINUA a través de la adaptación a la amenaza y el establecimiento de prioridades en función de los recursos disponibles.

Así las cosas, la hoja de ruta para la prevención proactiva ha de pasar, ineludiblemente, por utilizar el nuevo Esquema Nacional de Seguridad (ENS)[1] como un marco de referencia para, en primer lugar, identificar las medidas de seguridad más adecuadas y, en segundo lugar, acelerar su implantación mediante los denominados perfiles de cumplimiento[2] que permitan alcanzar una adaptación de las medidas de seguridad más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

El ENS, más allá de establecer un marco rígido de cumplimiento y demandante de recursos, ofrece una hoja de ruta contrastada, metodológica y estructurada en fases, que, junto a las soluciones de seguridad disponibles, permite conocer, en primer término, la superficie de exposición a las amenazas, evaluar y tratar los riesgos y, además, justificar y poner en marcha un plan de mejora continua a corto, medio y largo plazo para la implementación de la seguridad en las organizaciones.

A fin de cuentas, todo pasa por disponer de un elenco de soluciones que propician un conocimiento y contextualización del ecosistema, al tiempo que permiten una priorización eficiente de los recursos disponibles, consiguiendo una adaptación continua a la amenaza.

Figura 1. EVENS: Entorno de Validación del ENS[3]

[1] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

[2] Conjunto de medidas de seguridad que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el Centro Criptológico Nacional.

[3] EVENS: Integración en una única plataforma de todos los recursos disponibles relacionados con el ENS. https://ens.ccn.cni.es/es/evens.

2

CIBERAMENAZA

Los actores, para materializar los ataques, hacen uso de herramientas, explotan vulnerabilidades, emplean tácticas, técnicas y procedimientos. Vías todas ellas de materialización del daño y cuyo conocimiento permite potenciar las capacidades de detección de la amenaza o del impacto causado.

Contextualizando factores relevantes para el ámbito de la ciberseguridad, algunos elementos destacables son los siguientes:

· Incremento de las acciones ligadas a actores-Estado en el ámbito de las operaciones de influencia, propaganda, desinformación, amenazas híbridas, etc...

· Mejora significativa de las capacidades técnicas y operativas de actores ligados a la delincuencia económica (fraude al CEO, Human Operated Ransomware, ...).

· Incremento del impacto contra sistemas ciberfísicos, bien como objetivo final, bien como daño colateral en ataques a infraestructuras IT/OT.

· Explotación de sistemas expuestos a internet por todo tipo de actores, hecho que se ha visto amplificado por el incremento del teletrabajo (exposición no controlada de entidades a internet).

· Necesidad, y tendencia, de elementos ligados a inteligencia artificial en el ámbito de la seguridad.

· Por último, es necesario destacar de manera global la influencia en la ciberseguridad como las provocadas por las situaciones de pandemia, sus implicaciones directas y futuras que las mismas puedan llegar a desencadenar.

La situación geopolítica de los últimos años marca una tendencia creciente en relación con las operaciones de ciberespionaje, una progresión que viene confirmada por el incremento del número de países que han adquirido la capacidad de obtener, recopilar y explotar inteligencia del ciberespacio.

Estas capacidades se instrumentalizan a través de los denominados grupos APT (Amenaza Persistente Avanzada, del inglés *Advanced Persistent Threat*), integrados por personal muy especializado, con grandes conocimientos técnicos y dotados de significativos recursos económicos y materiales, que suelen llevar a cabo acciones de intrusión en las redes objetivo para permanecer ocultos durante el mayor tiempo posible sin ser detectados mientras extraen información de interés con fines diversos.

En la actualidad, son muchos los países que disponen de la capacidad para desarrollar ataques de ciberespionaje y su especialización sigue creciendo, al tiempo que lo hace la amenaza que representan. Esta capacidad, dirigida tanto al sector público como al privado, suele provenir de países que desean mejorar su posición a nivel político, estratégico o económico, todo ello sin olvidar las mafias organizadas y grupos de mercenarios cuyos grandes beneficios no hacen prever una disminución de este tipo de actividades[4].

Sin embargo, los ataques que utilizan el ciberespacio no solo tienen como objetivo los sistemas informáticos de empresas e instituciones, sino que cada vez más están dirigidos a influir o alterar opiniones haciendo un uso intencionado, y generalmente planificado y organizado, de información dirigida a socavar la seguridad y estabilidad de los ecosistemas que conforman la sociedad.

En este sentido, España sufre diariamente ciberataques de peligrosidad muy alta o crítica contra el sector público y las empresas estratégicas. Algunas de estas acciones provienen de otros Estados, que tienen entre sus motivaciones debilitar la capacidad política, tecnológica y económica nacional. El impacto de estos ataques puede derivar tanto en pérdidas millonarias en empresas privadas hasta interferir en el normal funcionamiento de servicios públicos esenciales para la ciudadanía.

[4] Véase https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/3573-ciberespionaje-una-amenaza-al desarrollo-economico-y-la-defensa/file.html

3

SALVAGUARDAS

La seguridad de la información y la ciberseguridad se han convertido en una de las principales preocupaciones tanto de las Administraciones Públicas como de las entidades privadas, y no solo desde el prisma de la Administración General del Estado, las Comunidades Autónomas o las grandes corporaciones empresariales, sino también desde la vertiente de las entidades locales o las pequeñas y medianas empresas.

La cada vez mayor frecuencia de los incidentes en el mundo digital y su impacto están poniendo en evidencia que ninguna organización, sea cual sea su tamaño o naturaleza, escapa a la amenaza de un ciberataque. Una realidad que, de materializarse, puede afectar a su imagen reputacional o a la continuidad de sus servicios, y, por tanto, a su propia existencia.

En este sentido, la gestión de la ciberseguridad de las organizaciones debe estar totalmente alineada con la criticidad de sus procesos, sin perder de vista que la ciberseguridad no contempla únicamente aspectos técnicos, sino también organizativos, normativos y legales.

Para ello, resulta fundamental que las salvaguardas tecnológicas estén coordinadas e integradas en una capa organizativa (gobernanza) que contemple aquellos aspectos complementarios a la tecnología (cumplimiento), necesarios para asegurar que la ciberseguridad y la seguridad de la información se entienden como un proceso ordenado y metodológico dirigido a garantizar la ciberresiliencia de los procesos de negocio.

Asimismo, es necesaria la existencia de un entramado legal que garantice la disponibilidad de los servicios esenciales para el funcionamiento de un país y la protección de la sociedad y los derechos fundamentales de sus ciudadanos.

En otro orden de cosas, las Mejores Prácticas, como las Guías CCN-STIC , deben considerarse como referentes específicos en la actuación judicial, arbitral o auditora. Una inadecuación total o parcial del sistema de información evaluado a

lo dispuesto en una Guía CCN-STIC que resultare de aplicación en cada caso, podría ser calificada por un Equipo Auditor como una Observación, No Conformidad Menor o Mayor, atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.

Una de las principales consecuencias que en el contexto de las TIC ha tenido la pandemia mundial de la Covid-19 ha sido el hecho de que las organizaciones se han dado cuenta de la importancia de contar con planes de contingencia y planes de continuidad de negocio que realmente respondan a las necesidades de sus procesos de negocio, tanto desde el punto de vista de sus infraestructuras tecnológicas como desde el punto de vista del acceso a sus instalaciones y de la disponibilidad de las personas encargadas de llevar a cabo esos procesos.

Este hecho ha provocado que las organizaciones identifiquen de manera prioritaria la necesidad de revisar, actualizar y probar la efectividad de esos planes. En esta materia, el estándar de facto es la norma internacional ISO 22301, que determina los requisitos que deben contemplar los sistemas de gestión de continuidad para garantizar la disponibilidad y la resiliencia de los procesos críticos de negocio.

3.1. SALVAGUARDAS ORGANIZATIVAS, NORMATIVAS Y PROCEDIMENTALES

La construcción de la seguridad de la información pasa, en primera instancia, por disponer de los elementos organizativos, normativos y procedimentales necesarios. Para ello, cada organización involucrada en el desarrollo y mantenimiento de un proceso de seguridad de la información debe haber redactado y aprobado la siguiente batería de herramientas normativas:

- Política de Seguridad de la Información.
- Normativa Interna.
- Procedimientos de Seguridad.

3.1.1. Política de Seguridad de la Información[6]

En líneas generales, una Política de Seguridad de la Información es un conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que la organización gestiona y protege la información y los servicios que, sustentados en sistemas de información, constituyen sus competencias o funciones; conteniendo, entre otras cuestiones, la misión u objetivos de la organización, su marco normativo, la organización de la seguridad de la información, la política de concienciación y formación, la gestión de los riesgos y su propio proceso de revisión.

Además de ello, la Política de Seguridad de la Información debe detallar las atribuciones de cada departamento, unidad o persona responsable del mantenimiento de la seguridad, así como los preceptivos mecanismos de coordinación y resolución de conflictos[7].

La importancia capital de la Política de Seguridad de la Información, como base esencial para la construcción de la seguridad de la información, hace que constituya siempre el primer elemento que debe acometerse, debiendo ser públicamente aprobada por su órgano directivo, como evidencia del compromiso de la organización con la seguridad de la información y su mantenimiento[8].

[6] Se corresponde con la medida [org.1] del Anexo II del ENS.

[7] Véase Guía CCN-STIC 801 ENS: Responsabilidades y Funciones.

[8] Véase Guía CCN-STIC 805 ENS: Política de Seguridad de la Información.

3.1.2. Normativa interna[9]

Dado que la Política de Seguridad es un documento de alto nivel, es necesario desarrollarla con documentos más precisos que ayuden a llevar a cabo lo propuesto, que materialicen sus requisitos mínimos y que suelen comprender: la organización e implantación del proceso de seguridad; el análisis y gestión de los riesgos; la gestión de personal; las características de la profesionalidad exigida, interna o externamente; la autorización y control de los accesos; la protección de las instalaciones; la adquisición de productos; la seguridad por defecto; la integridad y actualización de los sistemas; la protección de la información almacenada y en tránsito; la prevención ante otros sistemas de información interconectados; el registro de actividad; la gestión de los incidentes de seguridad; la continuidad de la actividad y la mejora continua del proceso de seguridad.

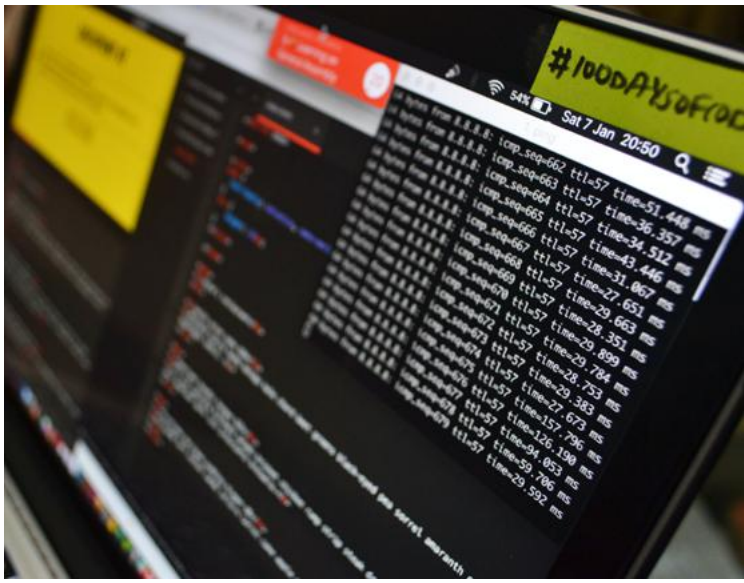
Por tanto, podemos decir que las Normas de Seguridad de la Información uniformizan el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios y, al tratarse de normas de obligatorio cumplimiento, deben ser asimismo aprobadas y adecuadamente difundidas por el órgano directivo de la organización[10].

De entre ellas, la más importante, siguiendo lo dispuesto por la Política de Seguridad de la Información de la organización, es la Normativa interna del uso de los medios electrónicos, gestionados o bajo la responsabilidad de la organización, que señalará los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso, conteniendo, entre otras cuestiones, el uso correcto de equipos, servicios e instalaciones; lo que se considerará uso indebido y la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

3.1.3. Procedimientos de seguridad[11]

Finalmente, para completar el marco normativo, cada organización inmersa en la implantación y mantenimiento de un proceso de seguridad de la información debe disponer de un conjunto documental de Procedimientos de Seguridad que aborden cómo han de realizarse tareas concretas, indicando, paso a paso, el proceder deseable en cada caso, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

Cada procedimiento de seguridad deberá estar alineado con la medida de seguridad que desarrolla y que, en consecuencia, será dependiente del nivel de seguridad requerido. A modo de ejemplo, se señalan algunos de los procedimientos de seguridad más habituales: Procedimiento de Arquitectura de Seguridad de los sistemas; Procedimiento para la adquisición de nuevos componentes; Procedimiento de Gestión de Usuarios; Procedimiento de Control de Seguridad en la Operativa; Procedimiento de Gestión del Mantenimiento; Procedimiento de formación y concienciación; Procedimiento de protección de equipos móviles; Procedimiento de protección de la autenticidad y de la integridad; Procedimiento para la protección de información y de soportes de información; Procedimiento para el transporte y entrada y salida de soportes de información; Procedimiento de Calificación y Gestión Segura de la Información; Procedimiento sobre control y borrado de metadatos; Procedimiento de Respaldo y Recuperación; etc.



[9] Se corresponde con la medida [org.2] del Anexo II del ENS.

[10] Véase Guía CCN-STIC 821 Normas de Seguridad.

[11] Se corresponde con la medida [org.3] del Anexo II del ENS.

3.2. SALVAGUARDAS TECNOLÓGICAS

Antes de pasar a describir las principales salvaguardas tecnológicas, y para dotarlas de contexto, es importante repasar brevemente el ciclo de vida de la mayoría de las ciberamenazas, modelo desarrollado por Lockheed Martin y denominado *Cyber Kill Chain*®[12].

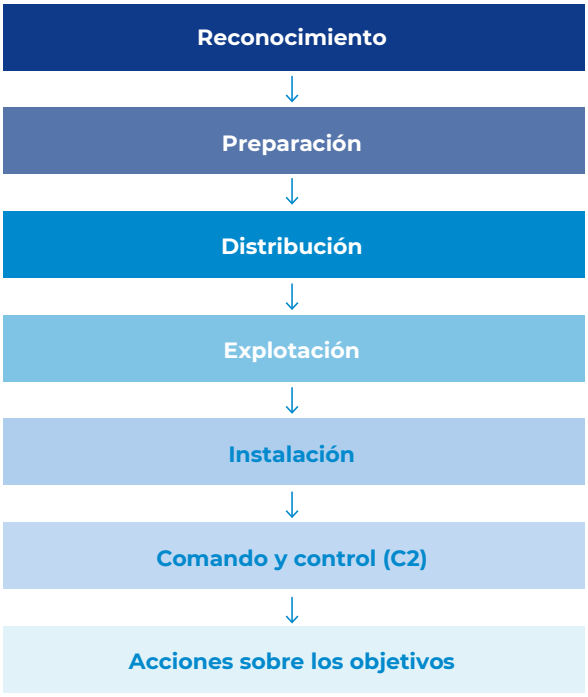


Figura 2. *Cyber Kill Chain*

De forma muy resumida, el modus operandi en muchas de las actuales campañas de distribución de malware puede resumirse en:

- Fase de intrusión.
- Movimiento lateral.
- Explotación o colonización.

Cada una de estas fases puede modelarse tomando como referencia las matrices de Tácticas, Técnicas y Conocimiento Común de Adversarios de ATT&CK[13] y pueden servir de base para establecer el plan de salvaguardas.

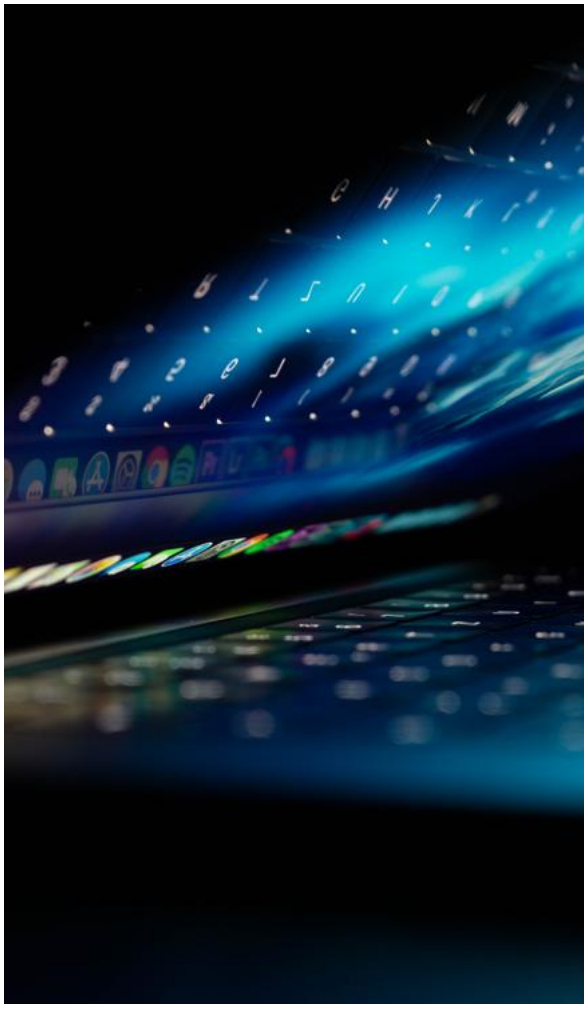
[12] Véase https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[13] Véase https://attack.mitre.org/versions/v7/matrices/enterprise/

3.2.1. Fase de intrusión

Los principales vectores de entrada que se están observando por parte de los atacantes son el correo electrónico y los servicios no seguros expuestos. Habitualmente, en el caso del correo electrónico, se trata de correos dirigidos a una o varias víctimas con un documento malicioso adjunto (generalmente, haciendo uso de macros para la descarga del código dañino) o persuadiendo al usuario para que visite una web previamente comprometida. Una vez allí, una falsa actualización del navegador, la instalación de complementos o mecanismos similares logran la descarga de la primera etapa del malware.

Por su parte, los servicios expuestos a internet son una vía de entrada muy usada por los atacantes. Servicios como RDP o SSH, que permiten acceso directo a la red interna, son analizados en busca de credenciales débiles o vulnerabilidades conocidas.



3.2.2. Fase de movimiento lateral

Una vez dentro de la organización, los atacantes buscan ganar persistencia y desactivar los sistemas de defensa. Asegurada la persistencia, la propagación del malware dentro de la organización se lleva a cabo utilizando diferentes tácticas/técnicas:

· Explotando vulnerabilidades conocidas (EternalBlue, EternalRomance, BlueKeep, etc.) que ayuden al movimiento lateral del atacante, como son las que afectan a protocolos como SMB.

· Robando credenciales y creando nuevos usuarios de administración.

· Deshabilitando cualquier sistema de protección implementado. En el caso de que el interés sea distribuir ransomware, los atacantes eliminarán también cualquier copia de seguridad.

En esta fase los atacantes suelen usar herramientas de post-explotación o que les faciliten la propagación lateral, como por ejemplo Empire, CobalStrike o Metasploit, además de herramientas nativas de los sistemas como Powershell, Batch Scripts, PSEXEC, etc.

La tendencia de los atacantes pasa por el uso de técnicas de *Living off the Land* (LOL) o el uso de *fileless malware*.

3.2.3. Fase de explotación o colonización

Una vez obtenido el control sobre la infraestructura víctima y establecido contacto con su sistema de Comando y Control, el atacante envía las órdenes de descarga y detonación del malware elegido, o bien cualquier otro tipo de acción a realizar sobre la red o sistemas víctima: exfiltración de información, alteración o eliminación de datos, cifrado, etc.

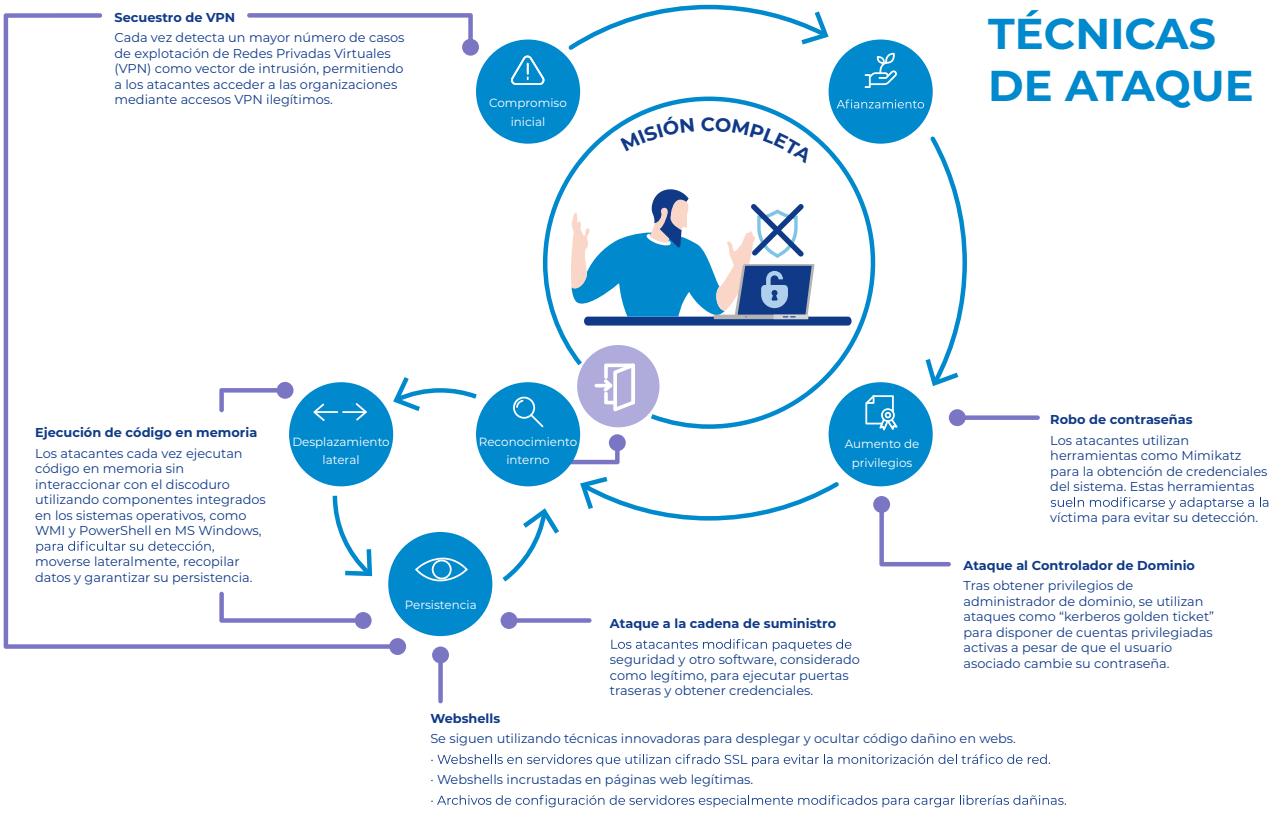


Figura 3. Fases de un ciberataque.

3.3. VIGILANCIA Y AUDITORÍA CONTINUA

Bajo la premisa de que no es posible vigilar ni auditar aquello que no se ve, la primera iniciativa para vigilar las redes corporativas es medir la superficie de exposición. Esto incluye conocer los dispositivos conectados y el mayor detalle posible asociado a estos.

Es fundamental tener una visibilidad de todos los activos conectados a la red corporativa que componen la superficie de exposición sin importar el origen de las conexiones (cable, Wi-Fi o de forma remota). En consecuencia, deben existir mecanismos implementados que permitan el descubrimiento del activo en el momento de la conexión antes de otorgar acceso al sistema.

Las principales salvaguardas tecnológicas para paliar los efectos de un ataque comienzan por la monitorización de la infraestructura bajo vigilancia. Es fundamental implementar un sistema de gestión que incluya la monitorización y correlación de alertas de fuentes como firewalls, controladores de dominios, IDS, HIDS, etc. Además, el despliegue de endpoints y herramientas anti-APT ayudarán a los analistas a detectar cualquier Táctica, Técnica o Procedimiento (TTP), Indicador de Compromiso (IOC) o comportamiento anómalo que pudiera ser un indicio o evidencia de compromiso de la seguridad[14].

Además, es fundamental tener una identificación completa y precisa sobre los servicios expuestos a internet y dicha necesidad. Una vez acotados, si los hubiera, se debe proceder a la configuración segura y bastionado estricto de los mismos.

Así como la identificación de servicios publicados en internet, también es necesario identificar los dispositivos que se conectan e interactúan en la red. Al descubrir un activo, el sistema debe implementar mecanismos para la extracción de un perfilado del activo con el fin de validar la identificación del mismo, lo cual debería estar alineado con una estrategia de Zero Trust[15].

El perfilado debe contar con el máximo contexto/información posible sobre el activo, incluyendo su criticidad, ya que será clave a la hora de establecer otras salvaguardas tecnológicas como el control de los permisos de usuarios, establecimiento de doble factor de autenticación (2FA), segmentación de la red, etc.

La visibilidad completa, en combinación con la vigilancia y auditoría continuas, otorgan a la organización información que le permite identificar vulnerabilidades y anomalías para mitigar riesgos, de manera preventiva, reduciendo la probabilidad de ocurrencia o controlando el impacto. Es importante también revisar de forma periódica y monitorizar las conexiones con terceros, en particular las VPN site-to-site activas.

Por último, es necesario llevar un control exhaustivo del estado de las actualizaciones de seguridad, tanto en servidores como en equipos cliente. Los protocolos antiguos que presenten vulnerabilidades conocidas deberían ser eliminados o, cuando no sea posible, protegidos por adecuadas medidas compensatorias o complementarias de vigilancia.

[14] Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.

[15] El modelo de seguridad de Zero Trust asume que los actores que no son de confianza ya existen dentro y fuera de la red. Por lo tanto, la confianza debe ser completamente eliminada de la ecuación.

3.4. SALVAGUARDAS CONDUCTUALES

El necesario equilibrio entre la usabilidad y la seguridad en el uso de la tecnología y el manejo de información provoca que mantener un adecuado nivel de ciberseguridad en las organizaciones requiera una adecuada implicación de las personas.

Como ha sido analizado en los puntos anteriores, los agentes de la amenaza son conscientes de esta realidad y sacan partido de ella utilizando a las personas como vector de entrada de sus ciberataques, haciendo uso de todo tipo de prácticas de ingeniería social: phishing, smishing, vishing, media dropping, etc. A esto hay que sumarle las brechas de ciberseguridad (por ejemplo, fugas de información) producidas por descuidos y prácticas inseguras de los empleados (mala praxis).

Esta situación provoca que los departamentos de ciberseguridad consideren a las personas como un elemento crítico en su estrategia de protección, acuñando la famosa frase "las personas son el eslabón más débil de la cadena". No obstante, al igual que la conducta insegura de las personas introduce riesgos en la organización, una conducta segura puede convertirse en una salvaguarda muy efectiva: salvaguardas conductuales.

Por todo ello, resulta indiscutible la necesidad de trabajar en la dimensión de las personas, con el objetivo de mejorar el nivel de ciberseguridad en las organizaciones, y así lo reflejan los principales marcos legales y normativos en materia de ciberseguridad tanto a nivel nacional como internacional.

3.4.1. Mejora del nivel de la cultura en ciberseguridad

Para lograr dicho objetivo, resulta necesario el diseño y puesta en marcha de un plan estratégico de mejora del nivel de la cultura en ciberseguridad, que promueva los cambios en la conducta de las personas mediante la realización de acciones de concienciación y formación en ciberseguridad.

Las acciones de concienciación tienen como objetivo involucrar e implicar a las personas en la gestión de la ciberseguridad, ayudándoles a entender la importancia de su rol como parte activa de la estrategia de protección.

Por su parte, las acciones formativas específicas permiten trasladar a las personas el conocimiento necesario para adoptar prácticas de comportamiento seguro que conduzcan a una gestión adecuada de los riesgos que les competen.

Si nos centramos, por ejemplo, en la gestión del riesgo asociada a las amenazas que utilizan la ingeniería social como vector de entrada, una salvaguarda conductual efectiva pasaría por lograr que los empleados conozcan:

- La amenaza y su papel en la gestión del riesgo asociado;
- Las pautas para identificar un ataque de ingeniería social en sus distintas vertientes;
- Cómo actuar cuando se detectan y cómo reportar de forma activa al equipo de ciberseguridad.

Al igual que ocurre con cualquier otra salvaguarda de ciberseguridad, es necesario que estos planes incorporen indicadores y métricas que permitan conocer la eficacia de las medidas desplegadas.

No disponer de los medios y capacidades necesarios para abordar un exhaustivo plan de mejora de la cultura en ciberseguridad no es óbice para empezar a dar pasos en esta línea. Lo importante es empezar a trabajar en la dimensión de las personas, incorporando a estas paulatinamente en la estrategia de defensa de la organización como una medida eficaz de protección ante la ciberamenaza.

4

MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza, en el que se designen a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.

Asimismo, resultará necesario describir aquellos servicios de ciberseguridad que el marco de gobernanza debe garantizar para la debida prestación de sus obligaciones en relación con los destinatarios de sus servicios (ciudadanía, empresas, otras entidades).

A continuación, se propone un modelo básico de referencia para la gobernanza de la ciberseguridad, de acuerdo con las premisas que siguen:

- Identifica una estructura organizativa de unidades prestadoras de los diferentes servicios de ciberseguridad, a adaptar al tamaño y modelo de recursos de cada entidad.
- Integra los procesos de gestión para la gobernanza de la ciberseguridad, con especial énfasis en los servicios de prevención proactiva que dicho marco debe contemplar.
- Identifica los servicios proveídos por la cadena de suministro TIC[16], así como los requisitos de cumplimiento exigibles a los suministradores.

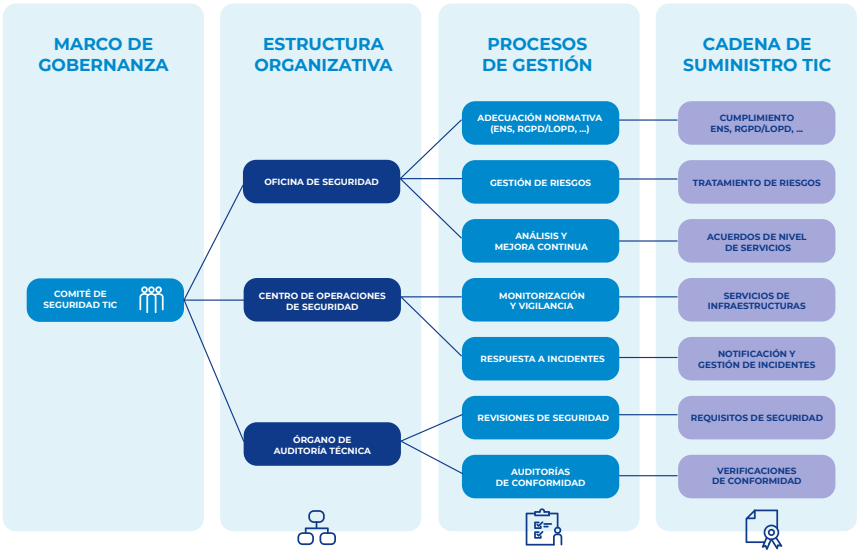


Figura 5.- Modelo básico de referencia para la gobernanza de la ciberseguridad.

[16] Tecnologías de la Información y la Comunicación (TIC).

5

ESTRUCTURA ORGANIZATIVA DEL MARCO DE GOBERNANZA

Atendiendo a la propuesta anterior, se describen a continuación las funciones y responsabilidades de cada uno de los componentes del Marco de Gobernanza de la Ciberseguridad.

5.1. COMITÉ DE SEGURIDAD TIC

En el marco de gobernanza representado, el Comité de Seguridad TIC se constituye como el órgano especializado y permanente de una organización para la ciberseguridad y estará integrado por aquellas personas de la organización con responsabilidad en la toma de decisión en materia de seguridad y privacidad de la información, así como por aquellas designadas en representación de otros órganos o comités.

En particular, el Comité de Seguridad TIC podrá integrar a vocales de otras áreas de la entidad que sean relevantes para la finalidad del comité, tales como la persona designada como Delegado de Protección de Datos de la misma o del Departamento Jurídico o de Recursos Humanos, entre otras.

5.1.1. Funciones del Comité de Seguridad TIC

Sin perjuicio de aquellas otras actuaciones que sea necesario acometer, las funciones esenciales del Comité de Seguridad TIC son las siguientes:

a) En el ámbito de la cooperación.

· El desarrollo y el mantenimiento de un marco común normativo, organizativo y colaborativo de seguridad.

· El desarrollo y el mantenimiento de un marco común de indicadores, métricas y analítica de datos de seguridad.

· El establecimiento y seguimiento de objetivos de seguridad.

· La mejora continua del proceso de seguridad.

· El intercambio de experiencias, conocimiento, herramientas y casos de éxito de seguridad.

· La integración con otros marcos de gobernanza de seguridad.

b) En el ámbito del desarrollo de la normativa en materia de seguridad.

· La propuesta, actualización, el mantenimiento y la difusión de la Política de Seguridad de los sistemas de información en los que se sustentan los servicios prestados por la entidad.

· La coordinación normativa con los Grupos de Trabajo de seguridad que se establezcan.

· La propuesta y mejora continua e innovación de la normativa de seguridad.

· La elaboración del informe anual del estado de seguridad de los sistemas TIC de la entidad.

· La integración con la normativa y las buenas prácticas de ámbito nacional y europeo.

c) En el ámbito de la gestión de riesgos en materia de seguridad.

· El desarrollo y el mantenimiento de un marco común de análisis y tratamiento de amenazas y riesgos para los sistemas TIC de la entidad, así como para los tratamientos de datos personales.

· La definición de los requisitos, niveles mínimos de seguridad, criterios comunes de Categorización y Declaración de Aplicabilidad para el establecimiento de un perfil de cumplimiento específico.

· La gestión y supervisión del tratamiento de los riesgos, que se realiza mediante la operación de la seguridad de la información (arquitectura, implantación, administración y mantenimiento de los controles de seguridad que son aplicables -necesarios-, junto con su eficacia, así como si están operando o todavía no lo están).

· La elaboración de informes previos sobre las propuestas de categorización de los sistemas TIC, así como los niveles de riesgos propuestos.

· El seguimiento de los planes de tratamiento de riesgos en materia de seguridad.

d) En el ámbito de la auditoría y certificación de conformidad de la seguridad de los sistemas TIC.

· La constitución de una unidad de auditorías técnicas y cumplimiento.

· Realización de revisiones de seguridad y su adecuación a las declaraciones de aplicabilidad.

· La planificación de auditorías de conformidad y su ejecución.

· La coordinación con el Centro Criptológico Nacional y las entidades de certificación.

· La integración con otros marcos de certificación de ámbito europeo (ENISA).

e) En el ámbito de la concienciación y formación en materia de seguridad de los sistemas TIC.

· La definición de buenas prácticas.

· El desarrollo y mantenimiento de un marco común de inclusión, formación y concienciación en materia de seguridad y protección de datos personales.

· La coordinación con universidades, centros de conocimiento, entidades de formación y de certificación.

· La integración con otros marcos de formación continua y certificación profesional.

f) En el ámbito de la gestión de incidentes en materia de seguridad de los sistemas TIC.

· Detección y ciberinteligencia.

· Notificación, gestión y respuesta a incidentes.

· La cooperación en la gestión de incidentes con las administraciones con competencias.

· La coordinación de actuaciones ante incidentes críticos de ámbito estatal con las autoridades competentes en materia de seguridad de las redes y sistemas de información.

· El intercambio de información con los CSIRT[17] de referencia y las autoridades competentes, a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

g) En el ámbito de la monitorización y vigilancia de seguridad de los sistemas TIC.

· Operaciones de la ciberseguridad (arquitectura, implantación y administración).

· Servicios de ciberseguridad para la identificación de incidencias e incidentes.

· Monitorización de eventos.

· Apoyo a la remediación de vulnerabilidades.

· El uso de herramientas comunes y compartidas.

[17] Un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.

Para la ejecución de sus funciones, el Comité de Seguridad TIC se podrá apoyar en la figura del Responsable de la Seguridad de la Información y en tres (3) unidades operativas complementarias y decisivas: una Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC, un Órgano de Auditoría Técnica y un Centro de Operaciones de Ciberseguridad e, incluso, ampliar este esquema de apoyo con una unidad específica para la Gestión de Incidentes de Seguridad de acuerdo a lo señalado en el apartado f).

La Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC sería la unidad encargada de acometer las actuaciones detalladas en los apartados a), b), c) y e) indicados anteriormente. El Órgano de Auditoría Técnica sería responsable del apartado d) y el Centro de Operaciones de Ciberseguridad sería el encargado de acometer las actuaciones detalladas en los apartados f) y g).

De esta manera, los Centros de Operaciones de Ciberseguridad se encargarán de reforzar las capacidades de vigilancia, prevención, protección, detección y respuesta ante incidentes de ciberseguridad, dando el asesoramiento y apoyo a la gestión de la ciberseguridad de un modo centralizado, que posibilite su eficacia y eficiencia.

Los Centros de Operaciones de Ciberseguridad, desde su concepción, deberán prestar a las entidades de su ámbito de aplicación un conjunto de servicios horizontales de ciberseguridad. La gestión de estos servicios incluirá, fundamentalmente, la implantación de la infraestructura técnica, herramientas, procedimientos y operación, además de aquellas cuestiones asociadas, tales como la detección y comunicación de incidentes de seguridad.

En definitiva, los Centros de Operaciones de Ciberseguridad articularán la respuesta a los incidentes de seguridad, sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración con competencias y de la función de coordinación de los CSIRT de referencia y del CCN-CERT, como coordinador nacional.

5.1.1.1. Desarrollo de instrucciones técnicas de seguridad

Como se ha señalado, la conformidad con el Esquema Nacional de Seguridad es un requisito de obligado cumplimiento, así como, cuando sea el caso, con la normativa en materia de protección de datos de carácter personal.

Para adecuar su cumplimiento, y en caso de requerir una regulación específica de acuerdo con las particularidades propias de la organización, el Comité de Seguridad TIC desarrollará instrucciones técnicas de seguridad con las exigencias de cumplimiento que en ellas se determinen, entre ellas, las que contemplen cuestiones tales como:

- Todos los servicios de seguridad dispondrán de una estructura de coordinación, supervisión y dirección técnica para facilitar la comunicación con el resto de las áreas y la dirección de las entidades.

- El Comité de Seguridad TIC será el órgano colegiado responsable de la gobernanza de la seguridad. Las decisiones tomadas en este comité tendrán impacto directo sobre las acciones que deberá realizar la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC, el órgano de Auditoría Técnica y el Centro de Operaciones de Ciberseguridad.

- Las competencias específicas del Comité de Seguridad TIC, así como su composición, regulación y la periodicidad de sus reuniones, vendrán recogidas en la Política de Seguridad de la Información aprobada en el organismo.

- El Comité de Seguridad TIC tendrá una relación directa con todos los actores involucrados en el proceso de seguridad, manteniendo representación de estos actores en todas las reuniones del Comité, de acuerdo a lo establecido en la Política de Seguridad de la información.

5.1.1.2. Elaboración y actualización de la Política de Seguridad de la Información

Corresponde al Comité de Seguridad TIC la elaboración y actualización de la Política de Seguridad de la información de la entidad.

Esta Política de Seguridad de la Información será de aplicación a todos los sistemas TIC que prestan servicios y que se encuentren comprendidos en su alcance, definiendo, de conformidad con la normativa nacional o europea que resulte de aplicación, entre otras cuestiones:

a) Los principios básicos y requisitos mínimos, que garanticen adecuadamente la seguridad de la información tratada.

b) El establecimiento del marco organizativo y tecnológico a través del Comité de Seguridad TIC.

La Política de Seguridad de la Información de la entidad se aplicará a todos los sistemas TIC y afectará a la información tratada por medios electrónicos, así como a toda la información en soporte no electrónico que haya sido causa o consecuencia directa de la citada información electrónica.

La Política de Seguridad de la Información será de obligado cumplimiento en el desarrollo de la actividad de los órganos de la entidad y por parte de todos sus miembros, así como para el personal que eventualmente pueda tener acceso a los sistemas de información o a la información, con independencia de cuál sea su destino, adscripción o relación.

5.1.1.3. Servicios y soluciones prestados por terceros pertenecientes al sector privado

Las entidades del sector privado que provean soluciones o presten servicios a las entidades del sector público, a sus organismos, y a las instituciones vinculadas, aplicarán los Esquemas Nacionales de Interoperabilidad y Seguridad, sus Normas e Instrucciones Técnicas derivadas, las guías de interoperabilidad y seguridad y las instrucciones técnicas de seguridad del Comité de Seguridad TIC que resulten de aplicación, para lo cual:

- El Comité de Seguridad TIC tendrá una relación directa con el suministrador de las antedichas soluciones o servicios para realizar un seguimiento de objetivos y mantener los índices de calidad y de respuesta a las necesidades de la entidad en materia de interoperabilidad y seguridad.

- A requerimiento expreso de la entidad, el suministrador podrá formar parte del Comité de Seguridad TIC, que podrá asignarle funciones específicas, dentro de su ámbito de responsabilidad.

De particular importancia será, en consecuencia, la debida certificación de conformidad con el Esquema Nacional de Seguridad de los sistemas de información usados por aquellos proveedores de la entidad que presten servicios tecnológicos o provean suministros en el ámbito de la Administración Digital, reflejándose dicha exigencia en los correspondientes pliegos de las licitaciones.

5.2. OFICINA DE GOBERNANZA Y CUMPLIMIENTO NORMATIVO DE LA SEGURIDAD TIC

Dentro de la estructura de seguridad, será conveniente la constitución de una unidad, denominada Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC, cuyas competencias incluirán la coordinación de los diferentes actores de seguridad de los órganos concernidos y el Centro de Operaciones de Ciberseguridad.

El director de dicha Oficina será designado por el Comité de Seguridad TIC, y actuará como enlace entre la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC y el resto de la estructura de seguridad de la organización.

La Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC tendrá funciones de asesoría legal y normativa, prestando apoyo en la resolución de cuestiones de este ámbito a toda la estructura de seguridad, pudiendo asumir competencias de asesoría legal en materia de Esquema Nacional de Seguridad, Protección de Datos y otras regulaciones del entorno de la seguridad de las TIC, la resiliencia y la privacidad.

La Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC impulsará y asegurará la adecuación al Esquema Nacional de Seguridad de los sistemas TIC dentro del alcance, desde los siguientes ámbitos:

· Normativa, gestión de la seguridad y análisis de riesgos.

· Capacitación y plan de formación y concienciación en ciberseguridad.

· Postura de seguridad y perfilado de la electrónica de red y equipos.

· Determinación de superficie de exposición/ataque ante la amenaza.

· Observatorio digital y cibervigilancia.

· Protección de la información y gestión del dato.

· Análisis y tratamiento de la información del estado de seguridad (cuadro de mando de indicadores).

· Mejora continua del proceso de seguridad.

· Otros ámbitos relacionados con la seguridad de las TIC (estudios económicos, ciberseguros, etc.).

5.2.1. Funciones de la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC

Siendo necesario unificar el uso de soluciones para asegurar una normalización de servicios y tecnologías (orquestación), limitando así el número de adaptaciones por entidad y reduciendo los tiempos de detección y respuesta, así como el impacto de las incidencias en las entidades, las labores de la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC serían, entre otras posibles, las siguientes:

· Actuaciones en relación con la adecuación al Esquema Nacional de Seguridad.

· Actuaciones en relación con la gobernanza y el desarrollo normativo en materia de ciberseguridad.

· Actuaciones en relación con las herramientas de seguridad y las aplicaciones específicas para operar el gobierno de la ciberseguridad.

· Actuaciones en relación con la concienciación y capacitación de usuarios y técnicos en materia de ciberseguridad.

· Actuaciones en relación con las auditorías de cumplimiento y determinación de la superficie de exposición en materia de ciberseguridad.

5.2.1.1. Adecuación al Esquema Nacional de Seguridad

La Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC será la unidad encargada de impulsar y asesorar a su entidad en el proceso de adecuación al Esquema Nacional de Seguridad.

El proceso de adecuación al Esquema Nacional de Seguridad deberá contemplar las siguientes fases, de acuerdo con los requisitos exigidos y la normativa vigente.

1) Planificación de la Adecuación

1. Se identificarán, en primer término, los servicios prestados que deben formar parte del alcance y se valorarán de acuerdo a sus necesidades de seguridad.

2. Seguidamente, se determinarán los niveles de seguridad del sistema y se obtendrá una categoría del sistema, de acuerdo con el procedimiento de categorización señalado en el ENS.

3. Se determinarán las medidas de seguridad que resulten de aplicación, de acuerdo a la categoría obtenida, lo que constituirá la Declaración de Aplicabilidad inicial.

4. Se revisará dicha Declaración de Aplicabilidad para su validación mediante un Análisis de Riesgos, obteniendo un riesgo final asumible para la entidad, resultando en consecuencia la Declaración de Aplicabilidad final.

5. Se revisará la Política de Seguridad de información de la entidad y se comprobará que atiende a las necesidades de seguridad actuales, así como a los requisitos exigidos en el ENS. En caso de no disponer de Política de Seguridad, se deberá proponer un documento que cumpla los requisitos para su aprobación.

2) Implantación de la Seguridad

Una vez concluido el Plan de Adecuación, se llevará a cabo la fase de Implantación de la Seguridad, donde se evaluará la implementación de medidas de seguridad en comparación a lo exigido en la Declaración de Aplicabilidad final validada.

En este sentido, se elaborará un Mapa Normativo y una Hoja de Ruta para las medidas que deben ser revisadas o implementadas.

Finalmente, se llevará a cabo la supervisión de la Implantación de la Seguridad, tanto en el ámbito técnico como en el ámbito normativo, mediante la solución AMPARO del CCN-CERT.

3) Obtención de la Certificación de Conformidad

Una vez finalizada la adecuación al ENS y junto con el seguimiento de la implantación mediante la solución AMPARO y los informes obtenidos por la solución ANA sobre la correcta evolución y aplicación de medidas técnicas para la reducción de la superficie de exposición, se realizará una auditoría de conformidad, realizada por el Órgano de Auditoría Técnica, para la verificación de la conformidad de todas las medidas implementadas.

Tras ello, se podrá llevar a cabo una Auditoría de Conformidad por medio de una Entidad de Certificación del ENS acreditada, que verifique el cumplimiento de las medidas de seguridad y, de resultar satisfactorio, expida el correspondiente Certificado de Conformidad con el ENS.

5.2.1.2. Gobernanza y desarrollo normativo en materia de ciberseguridad.

Las actuaciones consistirían en la elaboración, actualización, publicación, difusión y/o validación, como apoyo especializado, de la documentación necesaria, entre la que cabe destacar:

· Plan Director de Ciberseguridad.

· Adaptación al nuevo Real Decreto por el que se regula el Esquema Nacional de Seguridad y a lo que proceda del Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, durante el período transitorio definido.

· Perfiles de cumplimiento específicos, que comprenderán el conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una determinada categoría de seguridad, un sector específico o una actividad individualizada.

· Informes de análisis y gestión de riesgos, que recogerán la identificación, análisis, evaluación y tratamiento de los mismos de los sistemas de información.

· Normas y procedimientos para la protección de los activos de información, así como para la gestión de los procesos del sistema de gestión de seguridad de la información.

· Elaboración de las Instrucciones Técnicas de Seguridad, que precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

· Planes de continuidad del servicio de los sistemas de información de las entidades.

· Análisis y definición de cuadros de mando de ciberseguridad bajo el concepto de "prevención proactiva" orientada al dato.

· Gobernanza basada en el conocimiento del estado de la seguridad de los sistemas de información de las entidades, de conformidad con lo dispuesto en el Esquema Nacional de Seguridad.

· Adaptación a la normativa en materia de protección de datos personales, a saber: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

· En consonancia con la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, se tiene muy presente que: "Las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior", siendo de aplicación el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

5.2.1.3. Herramientas de seguridad y aplicaciones específicas

Las actuaciones consistirían en el desarrollo, implantación, operación, mantenimiento y/o actualización de herramientas avanzadas de apoyo a la gobernanza y reducción del entorno de superficie de exposición, como soporte especializado a las entidades, destacando, entre otras, las siguientes:

· La planificación y el diseño de un nuevo ecosistema de herramientas con altas capacidades predictivas y de nuevos asistentes e interfaces naturales de visualización de datos para los usuarios en función de su perfil, así como de identificación de escenarios, como ayuda a la toma de decisión para la predicción y prevención de incidentes de impacto elevado.

· El acceso a las herramientas del CCN-CERT (PILAR, INES, AMPARO, ANA, CLARA, ROCIO, ANGELES, LORETO) proponiendo una hoja de ruta de evolución organizativa, regulatoria y de roles, así como operar dichas herramientas para, llegado el caso, ampliar la funcionalidad de las mismas y conseguir una adaptación apropiada al ecosistema de aplicación.

· El desarrollo de nuevas funcionalidades de las herramientas del CCN-CERT que, aprovechando la evolución de las nuevas tecnologías, tales como Inteligencia Artificial, refuercen sus capacidades predictivas a la hora de prevenir incidentes de impacto elevado y reduzcan el perímetro de exposición a las ciberamenazas.

· La implantación y adaptación a las características que les son propias a las entidades y provisión de herramientas de evaluación del estado de seguridad y su implantación (EVENS).

· El desarrollo, implantación y provisión de herramientas de analítica de datos que aprovechen el elevado caudal de datos de eventos generados por las herramientas del CCN-CERT, que contribuyan a la ciberseguridad orientada al dato.

· El desarrollo de nuevas herramientas promovidas por las entidades de seguridad de la información, así como productos o programas específicos a propuesta del CCN-CERT, que den respuesta a necesidades no cubiertas por las herramientas disponibles.

· La construcción de un ecosistema de colaboración pública y privada, como estrategia de agilización de los cambios en las herramientas actuales y del despliegue de nuevas herramientas, aprovechando los recursos financieros disponibles.

5.2.1.4. Concienciación y capacitación de usuarios y técnicos en materia de ciberseguridad

Las actuaciones consistirían en la elaboración y actualización de contenidos, publicación, difusión, impartición y/o validación, como apoyo especializado a las entidades, destacando, entre otras, las siguientes:

· El acceso a los contenidos del Portal de Formación del CCN-CERT (ANGELES) para la adaptación de cursos formativos en ciberseguridad, presenciales y online, al perfil de los usuarios y sus correlativas exigencias formativas.

· La planificación de itinerarios formativos ajustados al perfil de los usuarios y sus correlativas exigencias formativas.

· La colaboración con la organización en la preparación e impartición de píldoras formativas, webminars, talleres prácticos, seminarios, cursos, etc. encaminados a la formación de las personas usuarias y de perfil técnico de las entidades.

· La evaluación, perfilado de competencias y adaptación en ciberseguridad al puesto de trabajo de las personas usuarias en el ámbito de las entidades.

· La elaboración de informes, procedimientos y buenas prácticas de prevención y gestión de malware, con especial incidencia en el ransomware, y de resolución de incidentes de seguridad, para su aplicación al ámbito de las entidades.

· El acceso a las series de guías CCN-STIC e Instrucciones Técnicas de Seguridad para su adaptación o aplicación al ámbito de las entidades. En caso de su difusión en otros entornos se deberá citar el origen del documento.

5.2.1.5. Auditorías en materia de ciberseguridad

Las actuaciones consistirían en la planificación, ejecución y/o reporte de auditorías, de cumplimiento normativo y técnicas, de seguridad y de certificaciones del Esquema Nacional de Seguridad, como apoyo especializado a las entidades, destacando, entre otras, las siguientes:

· La planificación de programas anuales de auditorías de cumplimiento normativo y auditorías técnicas de seguridad y certificaciones del Esquema Nacional de Seguridad.

· Establecimiento de criterios comunes de valoración de servicios, categorización de sistemas y declaración de aplicabilidad, que permitan adoptar un perfil de cumplimiento único para los sistemas de información de las entidades.

· La cooperación con el Consejo de Certificación del ENS (CoCENS), que permita una interlocución adecuada con las entidades de certificación y la convergencia con otros marcos de certificación de ámbito europeo.

5.2.2. Servicios de prevención proactiva de la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC

A continuación, se describen los servicios que la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC debe prestar, y que constituyen las capacidades de prevención proactiva de la entidad.

5.2.2.1. Formación y concienciación en ciberseguridad

Como elemento central de las capacidades de prevención y en consideración a que los recursos humanos constituyen, en muchas ocasiones, el punto más débil de la ciberseguridad, la Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC deberá proporcionar un servicio de formación y concienciación orientado a los usuarios de los sistemas de información, que incluya:

· Concienciación y formación para usuarios finales.

Se generarán e impartirán contenidos y materiales divulgativos, píldoras, infografías, presentaciones, audiovisuales, etc., destinados a los usuarios finales, con el fin de mejorar la concienciación y formación en ciberseguridad.

Los contenidos deberán ser diferenciados por público objetivo, segmentando por usuarios, personal de dirección, altos cargos, etc.

Deberán realizarse de forma periódica campañas informativas de manera que se recorran los diferentes aspectos de la ciberseguridad reforzando y mejorando aspectos tratados en anteriores campañas.

· Formación en ciberseguridad para personal técnico.

Se planificarán e impartirán contenidos formativos, presentaciones, informes, etc., destinados a personal técnico de:

- Sistemas
- Comunicaciones
- Seguridad

La formación deberá versar tanto sobre cuestiones de carácter fundamental y general de ciberseguridad, como implementaciones concretas de productos de uso generalizado en las entidades.

· Formación para personal de desarrollo de software de las entidades.

Se planificarán e impartirán contenidos destinados a desarrolladores software de las entidades, orientado a la seguridad del código fuente, mejora de procesos de desarrollo desde el punto de vista de la seguridad, arquitecturas seguras de desarrollo, etc.

· Formación para personal de la comunidad asociada al Centro de Operaciones de Ciberseguridad.

Se planificarán e impartirán contenidos formativos destinados al personal del Centro de Operaciones de Ciberseguridad, orientados a mejorar las capacidades de:

- Prevención y detección de ciberincidentes.
- Resolución de incidentes de ciberseguridad.
- Análisis forense.
- Auditorías técnicas de ciberseguridad.
- Cumplimiento normativo.

En caso de servicios prestados por terceros, el suministrador deberá proporcionar formación continua y certificaciones profesionales al personal técnico que haga uso de cualquiera de las soluciones del Centro Criptológico Nacional, proporcionando, asimismo, todas las herramientas, plataformas de formación, contenidos, etc. necesarias para el servicio, incluyendo las licencias de uso en el volumen adecuado.

5.2.2.2. Gestión de la Seguridad y Conformidad

Los Servicios de Gestión de la Seguridad y Conformidad incluirán el Análisis de Riesgos, la Planificación y Gestión de la Implantación de Seguridad y la Evaluación de la Conformidad, de acuerdo al marco de referencia que constituye el Esquema Nacional de Seguridad.

Estos servicios deben contemplar la utilización, al menos, de la Herramienta de Planificación y Gobernanza de la Seguridad INES, con las siguientes características:

· Permitirá la recopilación de métricas que permitan evaluar el grado de seguridad de los sistemas.

· Deberá disponer de capacidad de análisis de datos para la toma de decisiones estratégicas en materia de seguridad.

· Permitirá la recopilación de datos asociados a la seguridad de los sistemas TIC de los organismos y categorizarlos en función de parámetros establecidos.

· Deberá disponer de la capacidad de calcular y producir indicadores de seguridad, en base al ENS.

· Dispondrá de la capacidad de mostrar información ejecutiva y técnica sobre el grado de seguridad de los sistemas TIC.

· Permitirá realizar un seguimiento dinámico del estado de la seguridad de los sistemas.

· Proporcionará información acerca de las posibilidades de mejora de la seguridad de los sistemas de los organismos.

· Establecerá un modelo de roles de supervisión que permita la consulta de indicadores de organismos adscritos.

· Permitirá la identificación de los servicios esenciales prestados y el establecimiento de sus necesidades de seguridad.

· Proporcionará un listado de medidas de seguridad (Declaración de Aplicabilidad) que serán de aplicación, de acuerdo a las necesidades de seguridad establecidas y la aplicabilidad del ENS.

· Permitirá establecer una planificación de las medidas de seguridad y controles que deben ser implementados, de acuerdo al ENS.

· Dispondrá de capacidades de asistencia para la generación de una Política de Seguridad.

· Permitirá obtener un plan de mejora de seguridad en base a los datos obtenidos del sistema.

· Facilitará la realización de las tareas destinadas a cubrir el ciclo de mejora continua de la seguridad de los sistemas TIC.

Además, se deberá contemplar el uso de la herramienta AMPARO como asistente para la implantación de la de Normativa de Seguridad y Conformidad, con las siguientes características:

· Proporcionará asistencia en la implantación de medidas de seguridad técnicas y organizativas a través de la propuesta ordenada de materiales y recursos, de acuerdo a una Declaración de Aplicabilidad.

· Deberá disponer de capacidades que permitan establecer una visión global del proceso de implantación de seguridad, de acuerdo al ENS.

· Permitirá la gestión documental del Marco Normativo e instrucciones técnicas necesarias para la conformidad del sistema.

· Deberá disponer de capacidades de custodia de registros de conformidad, de acuerdo a la normativa de seguridad del sistema.

· Deberá disponer de capacidades de evaluación automática de la conformidad del sistema, de acuerdo al ENS.

· Deberá disponer de capacidades que permitan la identificación automática de no conformidades del sistema y proporcionar asistencia para su corrección.

· Deberá disponer de capacidades y roles de auditoría para la evaluación de conformidad del sistema, recopilando evidencias de conformidad como normativas, configuraciones, imágenes, etc.

· Permitirá la gestión de auditorías de conformidad para unidades de auditoría, reflejando el estado del proceso y permitiendo recopilar toda la información necesaria en un proceso de auditoría de conformidad.

· Permitirá la recopilación y gestión de certificaciones de conformidad y alertas de renovación.

· Deberá disponer de alertas de obsolescencia de documentos, concesiones y renovaciones de documentos, cambios en la normativa del sistema y otras alertas relevantes para la gestión de la seguridad y la conformidad.

Finalmente, se contemplará el uso de la herramienta de Análisis y Gestión de Riesgo PILAR, con las siguientes características:

· Deberá disponer de capacidades para la declaración de activos, de acuerdo a catálogos basados en una metodología de análisis de riesgos reconocida.

· Permitirá la cuantificación y la valoración cualitativa de los activos, proporcionando asistencia para la evaluación de activos que sigan las recomendaciones de la normativa vigente.

· Permitirá la creación de dominios y dependencias de activos que afecten a la valoración de los mismos y repercutan en el riesgo calculado.

· Deberá disponer de capacidades de identificación y valoración automática de amenazas, en base a un catálogo de amenazas actualizado, relacionándolas con los activos identificados.

· Permitirá la modificación de las amenazas identificadas, ajustar su valoración, eliminar las amenazas o identificar nuevas.

· Permitirá establecer factores agravantes y atenuantes a nivel global que influyan en el riesgo del sistema.

·Permitirá identificar medidas de protección técnicas, organizativas y otras salvaguardas, de acuerdo con un catálogo establecido por un estándar de seguridad reconocido.

· Permitirá la valoración de salvaguardas de acuerdo al modelo de madurez en base al ENS.

· Deberá disponer de capacidades de gestión de riesgo estableciendo fases y planes de actuación para la mitigación de riesgos identificados.

· Deberá disponer de capacidades de cálculo de riesgo dinámico que permita identificar y valorar activos, amenazas y salvaguardas en base a una ingesta de datos recopilados de fuentes automatizadas.

5.2.2.3. Protección contra la fuga de información

El Servicio de Protección de la Información incluirá herramientas de gestión de acceso a los datos, soluciones IRM , monitorización de acceso a ficheros y soluciones de etiquetado de información y DLP .

Se deberá usar un sistema compatible con el IRM para mantener los documentos protegidos de los organismos y un sistema que facilite el intercambio de documentación (por ejemplo, la solución LORETO del CCN-CERT) garantizando la confidencialidad, permitiendo a los usuarios gestionar los accesos y edición de los documentos, y permitiendo, mediante políticas, el establecimiento de carpetas protegidas.

Asimismo, el sistema debe permitir detectar la ubicación desde donde se abran los documentos protegidos tanto dentro o fuera de la entidad.

Finalmente, el sistema debe poder ser capaz de intercambiar información con el SIEM (Security Information and Event Management) y podrá incluir entre sus componentes la herramienta CARLA del CCN-CERT o permitir la interactuación con la misma.

5.2.2.4. Evaluación continua de la exposición del sistema y determinación de la superficie de ataque

Las herramientas de monitorización de la superficie de exposición permitirán mantener una trazabilidad de las vulnerabilidades y requisitos de seguridad del sistema, posibilitando la gestión de los activos y el mantenimiento de un conocimiento sobre el nivel de exposición del sistema.

Se habilitarán servicios de gestión de auditorías técnicas y pentesting, que midan continuamente la exposición del sistema y permitan obtener evaluaciones periódicas sobre las carencias de seguridad del sistema.

Los servicios para evaluar la superficie de exposición contemplarán:

· Identificación de servicios, sistemas y activos.

· Auditorías técnicas en caja blanca.

· Auditorías técnicas en caja negra, pentesting o ejercicios de hacking ético.

· Análisis automatizados de vulnerabilidades.

· Pruebas de denegación de servicio.

· Analítica de la superficie de exposición y definición de hojas de ruta de remediación.

Los resultados se tratarán en herramientas que permitan hacer un seguimiento automatizado de los resultados obtenidos (por ejemplo, ANA del CCN-CERT).

5.2.2.5. Servicio de cibervigilancia

Consiste en la recopilación y aviso de vulnerabilidades y amenazas publicadas por los CSIRT de referencia y otros organismos dedicados al seguimiento de vulnerabilidades, así como información publicada por fabricantes de software y hardware relacionados con eventos de seguridad. Este Servicio de cibervigilancia incluye tanto la detección e información de las vulnerabilidades reportadas por CSIRT y fabricantes, como el análisis de las mismas, propuesta de solución y apoyo a la entidad en el tratamiento y seguimiento del estado de actualización.

En relación con la monitorización de suplantaciones de identidad de entidades en sitios web, registro de dominios, cuentas en redes sociales, correos electrónicos, etc.:

· Deberán monitorizarse fuentes abiertas en busca de suplantaciones de identidad de cualquier tipo a entidades. Deberá monitorizarse especialmente la suplantación de sitios web, el registro de dominios simulando o suplantando directamente a entidades, suplantación de servicios oficiales (citas previas, tramitación, etc.), campañas de spam o phishing, redes sociales, etc.

· Además de la detección de suplantaciones, deberá prestarse asistencia en los procesos de resolución de este tipo de incidentes.

Por su parte, en relación con la monitorización de fuentes abiertas, redes sociales, foros, webs, etc. para detectar posibles riesgos y amenazas, deberán monitorizarse las fuentes abiertas que se considere necesarias para detectar con antelación posibles ataques organizados contra entidades. Además de la vigilancia rutinaria habitual, deberá prestarse especial atención a campañas que puedan organizarse en torno a situaciones especiales.

En este sentido, deberá obtenerse de las entidades toda la información necesaria para personalizar el servicio, determinando qué vulnerabilidades, suplantaciones, riesgos o amenazas son relevantes para la entidad.

Por tanto, será necesario realizar una revisión inicial completa para identificar su grado de exposición ante amenazas externas para, posteriormente, mantener un servicio continuado de vigilancia y alerta sobre dichas amenazas, que permita identificar los riesgos existentes para su evaluación y mitigación.

Realizar una revisión completa de cuál es la superficie de ataque de una organización contemplará las siguientes tareas:

· Identificación de dominios.

· Identificación de subdominios.

· Identificación de direcciones IP.

· Servicios disponibles y revisión pasiva de posibles vulnerabilidades.

· Metadatos publicados en los servicios disponibles.

· Perfiles de marca en RRSS.

· Posibles exfiltraciones de información (Data Leaks).

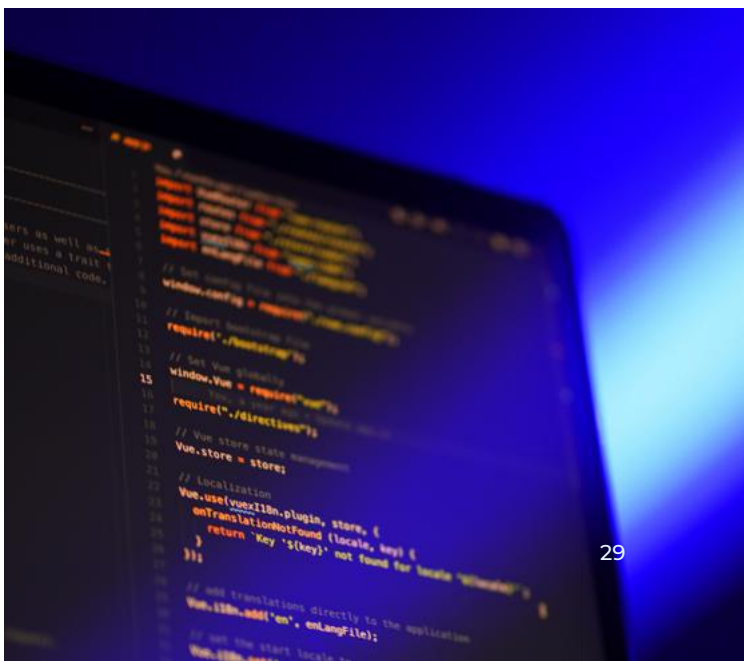
· Posibles abusos de marca.

· Apps publicadas en markets alternativos.

· Perfiles VIP en RRSS.

· Credenciales expuestas.

Todo ello desembocará en la realización de un servicio continuo de cibervigilancia que permita vigilar, identificar y gestionar las amenazas que se han detectado, ofreciendo a la entidad una visión más clara de los riesgos externos a los que se enfrenta y que el atacante podría conocer a priori.



5.3. ÓRGANO DE AUDITORÍA TÉCNICA

Dentro de la estructura organizativa del marco de gobernanza de ciberseguridad, podrá ser conveniente la constitución de un Órgano de Auditoría Técnica (OAT) independiente, para la realización de auditorías de conformidad de los sistemas, al que serán aplicables las siguientes precisiones:

- El OAT deberá preservar su independencia del resto de la estructura técnica y de seguridad, designando un Responsable del OAT (ROAT) que participará en los Comités de Seguridad.

- El OAT realizará revisiones periódicas de análisis de seguridad según el modelo establecido por el CCN para la identificación de hallazgos sobre el estado de actualizaciones y superficie de exposición.

- El OAT utilizará la solución ANA del CCN-CERT para la gestión de los hallazgos identificados y el correcto seguimiento y revisión continuada de la seguridad.

Por lo que respecta al Sector Público, la Guía CCN-STIC 122 define el procedimiento utilizado por el Centro Criptológico Nacional para el reconocimiento de la capacidad técnica y resto de requisitos de estas entidades, organismos, órganos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura, quede garantizada la debida imparcialidad y la ausencia de conflicto de intereses entre los elementos auditor y auditado, en relación con las Auditorías de Seguridad exigidas por el Esquema Nacional de Seguridad (ENS) de cara a alcanzar la preceptiva Certificación de Conformidad con el ENS.

Los OAT del Sector Público deberán satisfacer dos (2) requisitos fundamentales para ser reconocidos como tales:

1. Capacidad técnica para la realización de Auditorías de Seguridad del ENS y la evaluación de sus requisitos para los sistemas de información auditados.

2. Imparcialidad y ausencia de conflicto de intereses entre el OAT y la entidad propietaria del sistema de información en cuestión.

El procedimiento de reconocimiento como OAT del Sector Público consta de las siguientes fases:

- Solicitud de reconocimiento: mediante comunicación formal dirigida al Subdirector General del Centro Criptológico Nacional, en la que se manifieste su deseo, y adjuntando la documentación que se señala en dicha Guía, así como aquella otra que el OAT considere conveniente, en apoyo a sus pretensiones.

- Verificación de las condiciones para el reconocimiento: que comprenderá la evaluación de la competencia y capacidad técnica evidenciada por el OAT solicitante para el desarrollo de Auditorías de Seguridad del ENS (tomando en consideración la cualificación y experiencia de los miembros del Equipo Auditor de la entidad) y los requisitos de imparcialidad y ausencia de conflicto de intereses.

- Emisión del Certificado de Reconocimiento: una vez realizada la evaluación respecto de la capacidad técnica del OAT y los requisitos de imparcialidad y ausencia de conflicto de interés, y encontrándose conforme con tales requisitos, el CCN reconocerá al OAT solicitante como Órgano de Auditoría Técnica del ENS, para lo que expedirá el correspondiente Certificado de Reconocimiento, cuya validez será de dos (2) años (mientras se mantengan las condiciones que permitieron su expedición), pudiendo ser renovado por períodos iguales atendiendo a los criterios que se utilizaron en la evaluación originaria.

Dichos OAT podrán asimismo constituirse desde los departamentos centrales de las distintas Administraciones Públicas (Administración General del Estado, de las Comunidades Autónomas o de las Entidades Locales), al objeto de proporcionar una capacidad de auditoría e inspección centralizadas, con el alcance correspondiente a cada Administración.

5.4. MODELO EXTENDIDO DE GOBERNANZA

El modelo propuesto hasta ahora admite variaciones en su desarrollo atendiendo a las características de la organización, tales como: la estrategia y objetivos, que en esta materia defina la entidad a través del Comité de Seguridad TIC, la asignación de funciones y responsabilidades, las obligaciones adicionales que la entidad tenga, la dimensión de esta, las dependencias organizativas y con terceros que existan, su grado de madurez y/o sus capacidades, por citar algunas de ellas. En consecuencia, hay múltiples escenarios de desarrollo del modelo.

En todos ellos, la responsabilidad última de la seguridad siempre recae en el Comité de Seguridad TIC, el cual, partiendo de que es el órgano que aprueba la estrategia, alinea la seguridad con los objetivos del organismo, define los objetivos de cumplimiento de apetito de riesgo, y supervisa el cumplimiento del ENS con sus principios básicos y requerimientos mínimos, podría por ejemplo delegar en el rol del Responsable de Seguridad de la información, las funciones tanto de gestión del día a día de la práctica de la seguridad, como de las operaciones.

A modo de ejemplo, se muestra a continuación un ejemplo, en el cual la entidad responde a los siguientes supuestos: es de tamaño medio-alto o alto, con recursos humanos y materiales suficientes en materia de seguridad de la información, dónde a la obligación de cumplimiento del ENS se le une otras obligaciones legales como pueden ser las derivadas del RD-ley 12/2018 de seguridad de las redes y sistemas de información y de su RD 43/2021 de desarrollo y que consecuentemente, con este marco, ha debido designar un Responsable de Seguridad de la Información, asignarle las funciones que el RD 43/2021 identifica y dotarle de independencia del área de sistemas. Así mismo, dado el grado de madurez de la organización en esta materia, ha decidido segregar las funciones de seguridad en dos (2) áreas: una que lideraría el cumplimiento y otra la operación, como se muestra en la figura siguiente.

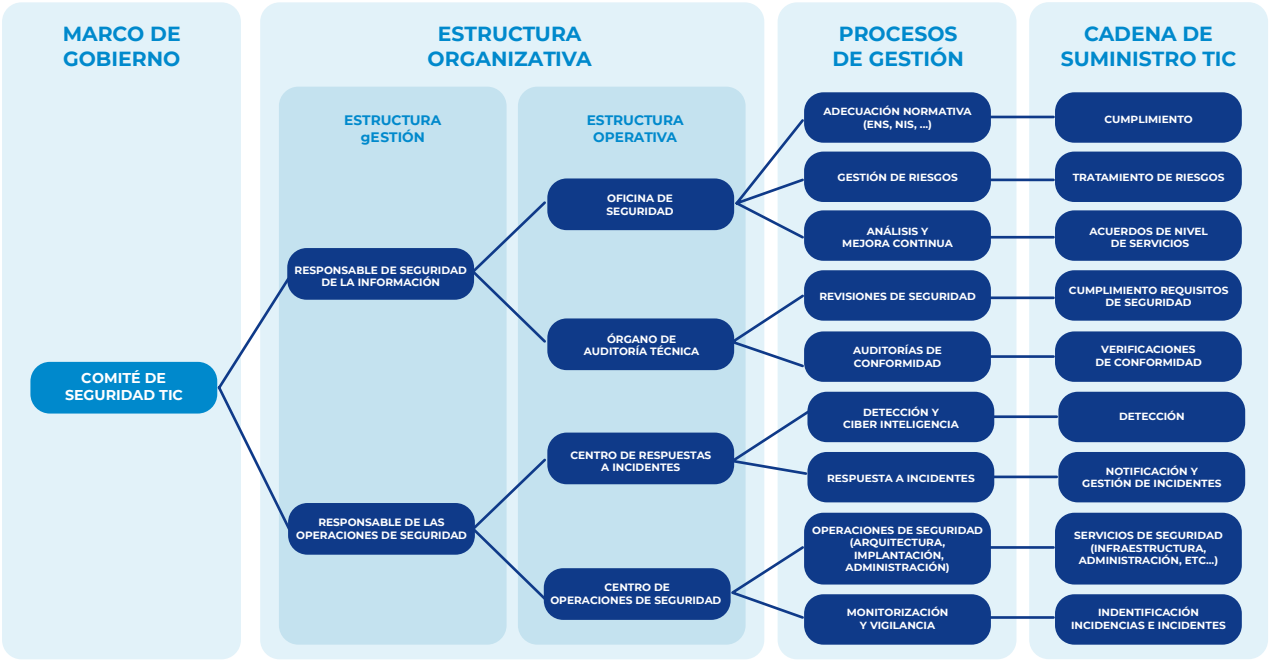


Figura 5.- Modelo extendido de referencia para la gobernanza de la ciberseguridad.

En este desarrollo del modelo, el Comité de Seguridad TIC delega parte de las funciones, del modelo básico descrito en los apartados anteriores, que tiene encomendadas por la entidad, en la figura designada por la misma para ejercer como Responsable de Seguridad de la información, que se responsabilizará de la gestión y aplicación de las directrices y guías marcadas por el Comité de Seguridad TIC, gestionando el día a día y aportando información y propuestas a este Comité, para su conocimiento y para la toma de decisiones que el ciclo continuo de la seguridad de la información requiere.

En este sentido, pueden observarse dos (2) áreas de responsabilidad diferentes: la del Responsable de Seguridad de la Información y la del Responsable de las Operaciones de la Seguridad.

· La primera corresponde al Responsable de Seguridad de la información, que, en este supuesto, dirige:

  · La Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC, con el fin de poner en práctica las directrices del Comité de Seguridad TIC, la normativa de la entidad o la identificación y seguimiento de la mejora continua.

  · La supervisión técnica del cumplimiento, mediante la supervisión de la eficacia de las medidas a través del Órgano de Auditoría Técnica y la Gestión de los incidentes.

· La segunda corresponde al Responsable de las Operaciones de Seguridad, que en este supuesto de desarrollo dirige:

  · El Centro de Operaciones de Seguridad.

Insistir una vez más que este desarrollo se muestra a modo ilustrativo y que cada entidad debe determinar su estructura organizativa, sus funciones, su marco normativo interno, sus procesos, sus actividades y cuantos elementos se hayan identificado en el modelo básico a modo de marco de referencia.

5.5. MODELO DE GOBERNANZA DE UN COCS

El modelo de gobernanza de un Centro de Operaciones de Ciberseguridad (COCS) tiene presente que:

· El COCS es responsabilidad de la entidad, a través de la Unidad responsable de la Operación de la Ciberseguridad que asume la dirección técnica y estratégica del servicio, con la colaboración de las unidades responsables de las infraestructuras y operaciones en todos aquellos elementos relacionados con la infraestructura de ciberseguridad.

· Por otro lado, los CSIRT ponen a disposición su apoyo al despliegue del COCS, su capacidad de operación de ciberseguridad, herramientas y soluciones de ciberseguridad, así como capacidades de investigación y respuesta experta ante incidentes de seguridad complejos. Así mismo, apoyarían en la dirección técnica y estratégica del servicio y en el seguimiento y ejecución de la implantación del COCS.

5.5.1. Estructura funcional del COCS

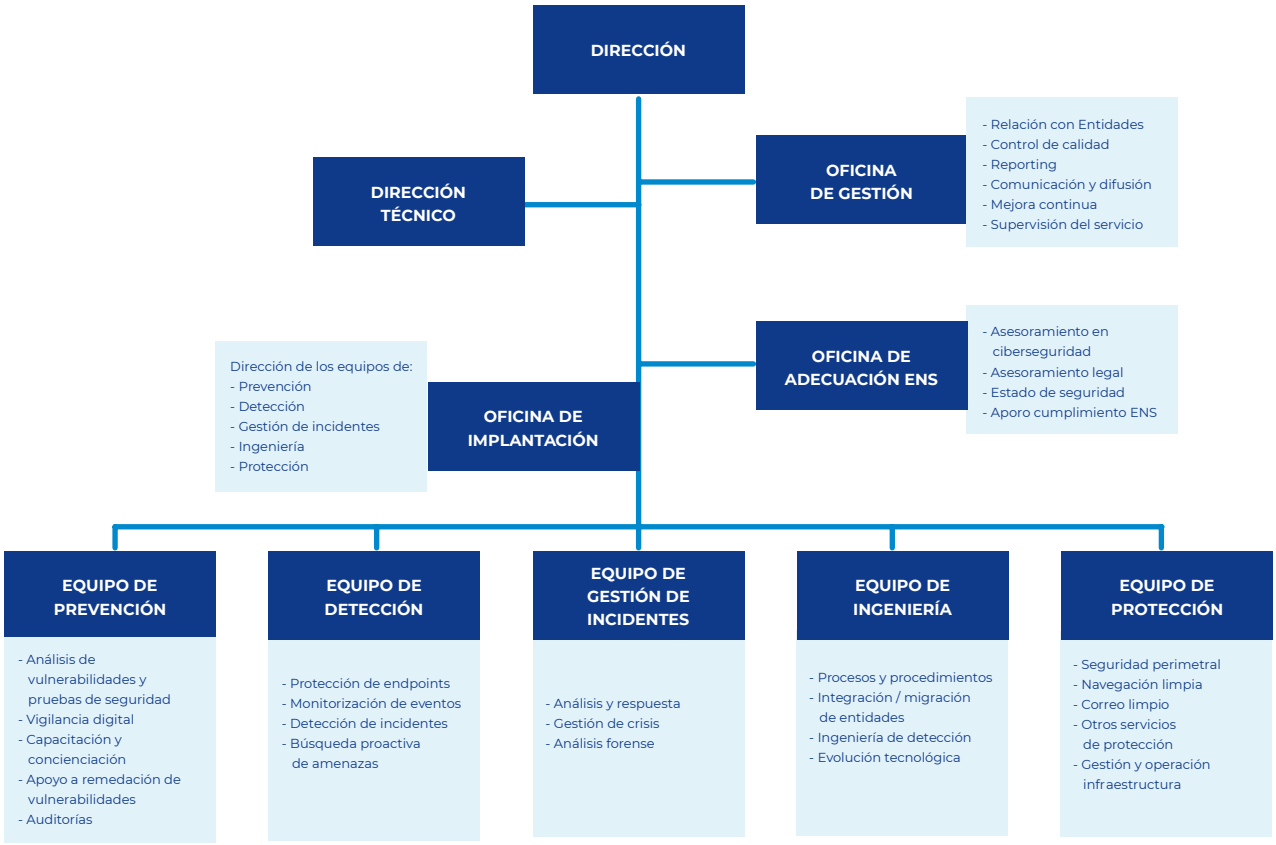


Figura 6.- Modelo de referencia para la gobernanza de un COCS.

En este sentido, se establecen tres (3) niveles de colaboración:

· **Nivel de dirección estratégica**. La dirección estratégica supone el nivel de decisión de carácter estratégico y sobre las cuestiones que se eleven desde el nivel de dirección técnica. Asimismo, será el nivel responsable de rendir cuentas del COCS.

Composición del Nivel de Dirección:

· Responsable de las Operaciones de Seguridad, sobre el que recaerá el rol de dirección.

· Representantes del CSIRT, ejerciendo el rol de colaboradores.

· **Nivel de dirección técnica**. Este nivel se encargará de coordinar y supervisar el cumplimiento de los hitos de implantación del COCS. Recibirá las peticiones del nivel inmediatamente inferior, estudiará la viabilidad técnica y, en su caso, decidirá o se elevará al nivel superior (estratégico).

· **Nivel de operación y gestión**. Este nivel se encargará de supervisar la puesta en marcha y funcionamiento de los diferentes servicios ofrecidos por el COCS. En este nivel de operación se contemplan tres (3) oficinas técnicas reportando cada una de ellas directamente al nivel de dirección técnica.

· Oficina de Gestión.

  · Supervisión del servicio.

  · Control de calidad.

  · Gestión y análisis de datos (reporting).

  · Mejora continua.

  · Comunicación y difusión.

· Oficina de Adecuación al ENS.

  · Asesoramiento en ciberseguridad.

  · Asesoramiento legal.

  · Estado se seguridad.

  · Apoyo cumplimiento ENS.

· Oficina de Implantación.

  · Equipo de ingeniería.

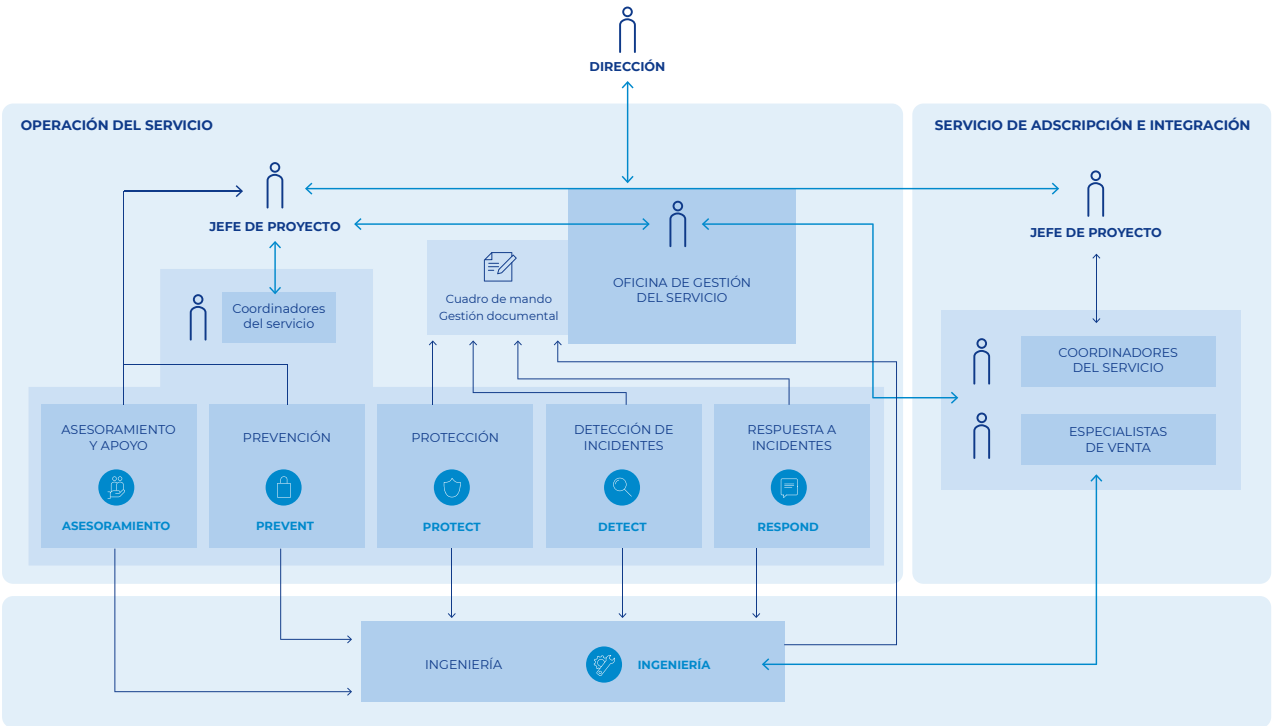
  · Equipo de prevención.

  · Equipo de protección.

  · Equipo de detección.

  · Equipo de gestión de incidentes.

Modelo de servicio



6

GESTIÓN DE CRISIS

Durante la gestión de un ciberincidente se puede detectar que no existe suficiente conciencia sobre la importancia de la seguridad de la información en las organizaciones, ya sea por no haber aparecido ésta en sus prioridades o bien por una falsa sensación de seguridad provocada por la disponibilidad de recursos (sistemas y protecciones) que finalmente resultan ser insuficientes.

En ambos casos, es muy probable que no exista una persona u órgano que asuma de un modo claro la función de Responsable de Seguridad de la Información y a menudo tampoco existe un equipo o comité que asuma la gestión de la situación cuando ya no es un incidente sino una crisis.

En primer lugar, la inversión en ciberseguridad debe ser una prioridad para las entidades. A pesar de la dificultad en calcular su retorno financiero exacto (como en toda inversión en seguridad, sea del tipo que sea), dada la cada vez mayor frecuencia de los ciberataques y el gran impacto que tienen, tanto en afectación al servicio prestado como en salvaguarda de la información y reputación de la propia entidad, no debe existir ninguna duda en acometerla. En este contexto, hay que disponer de sistemas que, al tiempo que protegen, faciliten la gestión ante un ataque (Firewalls, SIEM, EDR, ...).

En segundo lugar, y aunque la componente de sistemas es necesaria, no es suficiente, debiendo ser complementada con la disponibilidad de recursos humanos para la supervisión permanente del ecosistema, sean equipos constituidos con personal propio, externo o una mezcla de ambos.

Sin embargo, hay ciberincidentes que derivan o evolucionan hacia lo que cabe calificarse de crisis por su impacto real o potencial, y para ello es necesario prepararse también con antelación.

De entrada, 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 se producen sobre la oferta del bien o servicio por parte de la organización que lo sufre, sobre su reputación e imagen, sobre la sociedad en general.

Toda crisis implica una toma de decisiones bajo mucha presión, en poco tiempo y con información probablemente incompleta. Además, se organizan muchos frentes en paralelo y con muchos agentes y personas interviniendo.

A su vez, las crisis por un ciberincidente se caracterizan por:

- Requerir tiempo y especialistas para la investigación y análisis del incidente.
- Dificultad para conciliar prioridades entre el análisis del incidente y la recuperación.
- Diferentes lenguajes y cultura de silos.

Con independencia del tipo de ciberincidente que cause la crisis, de la definición previa se hace patente la componente de gestión que su resolución implica. Para ello, la organización afectada necesita haberse dotado de las capacidades y estructuras de gestión (comités / equipos) adecuadas que le han de permitir abordarla con garantías de éxito.

Por lo tanto, en toda crisis se identifican dos (2) esferas de actuación distintas:

1. **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.
2. **Organizativa y estratégica:** en la medida en que su impacto afecta a diferentes ámbitos de la organización (servicio, operativa, información, imagen y reputación, relación con el regulador, grupos de interés, presencia en redes sociales, etc.) y requiere de una respuesta coordinada a alto nivel.

Las capacidades y estructuras de gestión necesarias para hacer frente a una crisis no se improvisan cuando esta surge, es imprescindible desarrollarlas con antelación para disponer de la preparación necesaria en ese momento. En resumen, la capacidad de gestionar una situación de crisis depende en gran medida de las estructuras o comités que se hayan establecido antes de que ocurra el desastre causado por ese ciberincidente/suceso de “baja probabilidad y alto impacto”.

6.1. COMITÉ DE CRISIS

El Comité de Crisis es el órgano encargado de la gestión de la crisis a alto nivel dentro de la organización, con una mayor capacidad de visión 360° y visión estratégica. 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 dentro de la entidad, determinando y/o validando las estrategias de análisis, de contención y mitigación que permitan recuperar las operaciones en el menor tiempo posible, minimizando los impactos sobre las partes interesadas.

El Comité de Crisis debe tener sus roles definidos, es decir, debe tener establecidos qué responsables se necesitan para cubrir todos los frentes que requiere la gestión de una crisis. Estas funciones o roles a su vez han de asignarse a posiciones o cargos dentro de la organización. Su composición puede ser variable en función de la naturaleza del incidente o de la situación, aun así, algunos roles como el presidente del Comité, el coordinador del Comité y los responsables operativos, de comunicación y jurídicos es preferible que sean permanentes.

La clasificación y escalado de los ciberincidentes apuntan a la conveniencia de que existan distintos niveles de equipos o de comités. Desde este punto de vista cabe esperar que en función del nivel del ciberincidente establecido en base a los criterios de peligrosidad e impacto (real o potencial) se haya establecido previamente el Comité adecuado para su gestión.

Por consiguiente, el Comité de Crisis se puede apoyar para la gestión del incidente en otros equipos de un perfil más técnico y especializado (ver figura 7). Este sistema de estructuras o comités (que deben estar muy bien coordinados y alineados) depende en gran medida del tamaño o perfil de la entidad.

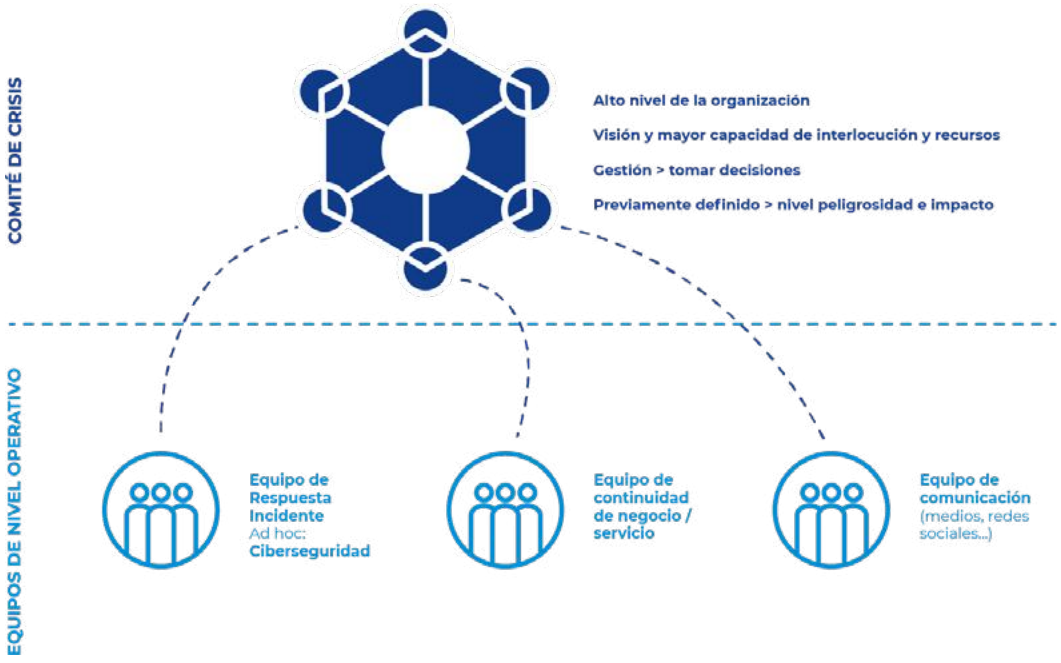


Figura 7.- Estructuras de gestión.

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

6.1.1. Activación del Comité de Crisis

El protocolo de activación del Comité de Crisis debe quedar previamente definido antes de que llegue una crisis y en gran medida dependerá del nivel de peligrosidad e impacto (o potencial impacto) del incidente. Por ello, es conveniente que la entidad tenga establecido niveles de Alerta a partir de cual se activa el Comité de Crisis.

La Guía CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes y la "Guía Nacional de Notificación y Gestión de Ciberincidentes" (ver figura 8) proporcionan una taxonomía y unos niveles de alerta y peligrosidad que sirven en primer lugar para clarificar la obligatoriedad de la notificación, pero también pueden servir para orientar si conviene o no activar un Comité de Crisis:

· En realidad, los incidentes con peligrosidad baja y media no deberían requerir la convocatoria de un comité de crisis como tal sino la organización, bajo la responsabilidad directa del Responsable de Seguridad de la Información, de equipos con conocimiento técnico suficiente para solucionar el problema desde un punto de vista operativo.

· En nivel alto, muy alto o crítico (niveles 3-4-5) se activaría el Comité de Crisis.

Esta configuración de comités no es excluyente, la constitución de uno de los niveles superiores implica, en general, el mantenimiento de la actividad de los anteriores. Es decir, en un ciberataque de categoría crítica la cúpula de la organización será quien tome las decisiones finales dentro del Comité de Crisis según las aportaciones de los equipos compuestos por representantes de direcciones funcionales y probablemente de más de un equipo trabajando en aspectos operativos, muy especializados y concretos.

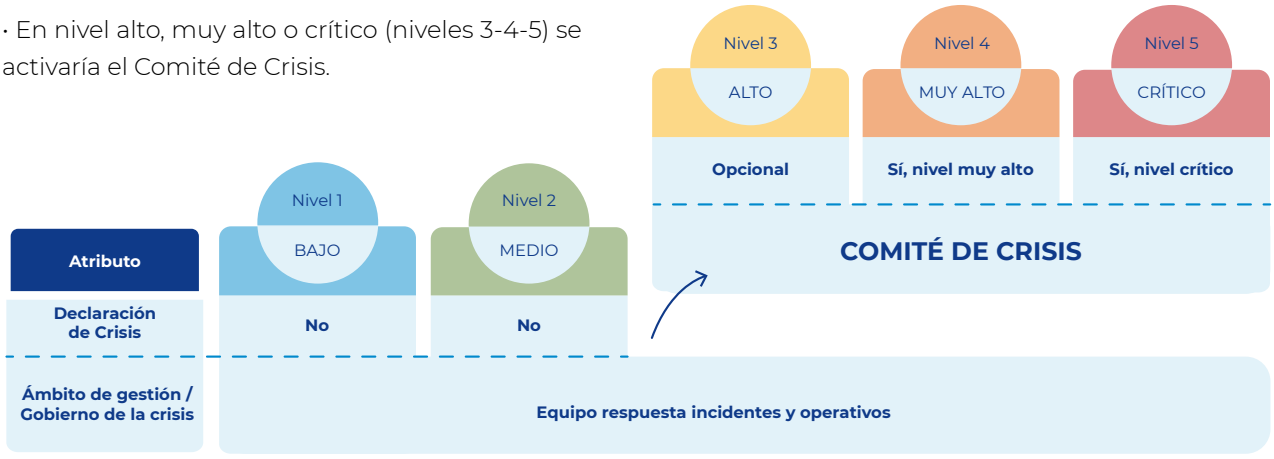


Figura 8.- Activación Comité de Crisis en función del nivel de peligrosidad e impacto.

6.1.2. Funciones del Comité de Crisis

El Comité de Crisis aporta una visión estratégica y dispone de una mayor capacidad de interlocución y de movilizar recursos extraordinarios, en caso necesario. Sus funciones 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 y las partes interesadas.
    - Mantener una previsión del impacto potencial y las consecuencias para la entidad, considerando los riesgos emergentes y los escenarios hacia donde puede evolucionar para poder acometer medidas de anticipación.
- Coordinar acciones y tomar decisiones priorizando.
    - Dar apoyo a los equipos que están sometidos a mucho tensión y presión.
    - Supervisar las medidas implementadas y las decisiones tomadas previamente por los equipos de respuesta u otros comités operativos, asegurando que los procedimientos puestos en marcha para la resolución son los más eficaces y eficientes.
    - Activar la movilización de recursos extraordinarios cuando sea preciso.
    - Hacer un seguimiento de los puntos abiertos, por ejemplo, mediante un documento de "Notas y Acuerdos".
    - Actuar como centro de referencia de información durante la respuesta al incidente y su posterior recuperación, tanto ante los agentes internos como externos (Administración y otros) involucrados o concernidos por el incidente.
    - o Asegurar las relaciones y la interlocución con todas las partes interesadas.
- Definir el posicionamiento de la entidad.
    - Definir la estrategia de comunicación interna y externa, en base a su misión, su propósito y sus valores.
    - Designar el portavoz y asegurar que se llevan a cabo las medidas de comunicación previamente diseñadas, ya sea en medios, redes sociales, marcos asociativos, etc.
    - Velar por salvaguardar la confianza, la reputación y la imagen.
- Coordinar las acciones de vuelta a la normalidad y de análisis posterior al incidente.
    - Extraer lecciones aprendidas y elementos de mejora.
    - Asegurar que se lleva a cabo el Plan de Acción resultante.

6.1.3. Composición del Comité de Crisis

El Comité de Crisis pivota sobre roles definidos (ver figura 9), que serán desempeñados por cargos dentro de la organización, los cuales, a su vez, estarán cubiertos por personas que pueden cambiar con los años. Por consiguiente, 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, ...).

Se recomienda crear una tabla con la correspondencia entre los roles dentro del Comité de Crisis y los cargos de la organización 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 en la entidad -tanto titulares como suplentes- y, por consiguiente, debe estar permanentemente actualizada.

Es importante que se haya definido y compartido con sus componentes las funciones del Comité en general y la de los miembros que lo componen en particular, con el objetivo de alinear el enfoque y facilitar el funcionamiento entre ellos.

En concreto, es clave que se tenga bien identificado quién es el presidente del Comité, y que éste tenga bien asumido su rol, pues de él dependerá en gran medida la conducción del equipo y por consiguiente el éxito de la gestión. Es una buena práctica que, como primer paso de la reunión del comité, se recuerden las principales funciones que se tienen asignadas.

Como ya se ha comentado, 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 de la crisis. En ocasiones, algunas funciones o roles pueden ser asumidos por una misma persona.

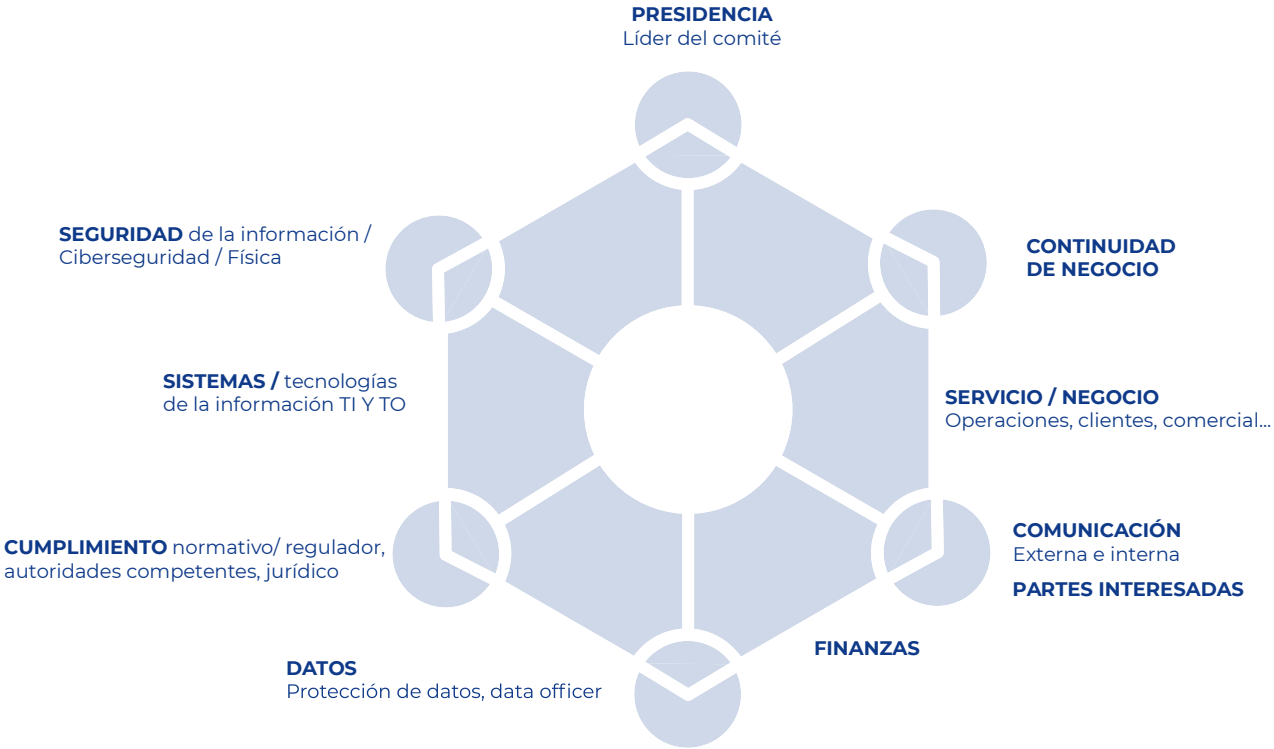


Figura 9.- Composición Comité de Cibercrisis.

A continuación, se muestran algunas de las funciones que deberían estar cubiertas en un Comité de Cibercrisis, sea bajo un mismo rol o sea dividido entre varios roles:

Función	Responsabilidades
Presidencia / líder del comité	· Liderar el comité y la crisis. · Dirigir la dinámica del Comité. · Asumir interlocución a alto nivel. ·...
Seguridad de la Información / Seguridad Física	· Coordinar al equipo de respuesta al incidente. · Asegurar la validez legal de las evidencias.
Sistemas / Tecnologías de la información IT/OT	· Gestionar los aspectos de infraestructura.
Cumplimiento normativo / Regulador, Autoridades competentes, Jurídico + Datos / Protección de datos	· Conocer los datos afectados desde el punto de vista servicio o negocio. · Repercusiones legales. · Notificación y comunicación autoridades pertinentes / regulador. · qué se notifica a los reguladores. · qué información se hace pública
Continuidad de Negocio / Servicio	· Coordinar equipos recuperación encargados de los Planes de Continuidad de negocio activados. · Recursos necesarios.
Servicio/ Negocio / Operaciones, Clientes, Comercial...	· Aportar análisis de áreas afectadas y la repercusión sobre activos, servicios, negocio... · Coordinar acciones respuesta de las operaciones.
Comunicación / Externa e Interna, Partes interesadas	- Definir los mensajes. - Plan de Comunicación: Gestionar comunicación medios, canales... - Coordinar equipo de Comunicación. - Comunicación interna: Instrucciones. - Gestión proactiva de las expectativas de las partes interesadas: (clientes, usuarios, ...)
Finanzas	- Facilitar recursos necesarios extraordinarios.

6.1.4. 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 cibercrisis. La reunión debe realizarse con la mayor brevedad posible (con titulares o suplentes) y, como se ha apuntado, puede ser de tipología diversa (presencial, videoconferencia, etc.).

Es importante 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, es recomendable disponer de:

- Agenda tipo.
- Lista de control de temas a cubrir o checklist.

Se recomienda disponer en el Plan o Manual de Crisis una propuesta de agenda para estas reuniones con el objetivo de facilitar la dinámica y el proceso de toma de decisiones, asegurando que se tratan los puntos clave. A modo de orientación la agenda puede contener los siguientes puntos:

a) Establecer la duración de la reunión.

b) Revisar hechos y pedir información actualizada del incidente.

c) Comprobar la lista de control.

d) Revisar el rol de cada miembro encaminado a 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 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 cibercrisis y evitar que las prisas o la urgencia de la situación provoquen el olvido de alguno de ellos; como se puede observar, es importante que tenga una vocación de exhaustividad en los aspectos que incluye.

Es importante registrar de un modo continuo las decisiones que vaya tomando el Comité de Crisis en un documento de “Notas y Acuerdos” a modo de bitácora, la información relevante de este primer análisis y de las medidas adoptadas (con hora y fecha) y las tareas del Plan de Acción (con responsables y plazo). Esta información debe estar disponible para los miembros del Comité durante todo el período para cubrir la más que probable dispersión geográfica que tendrán.

6.1.5. El Comité de Crisis entre reuniones

El Comité de Crisis debe realizar el seguimiento continuo de la situación, lo cual 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 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.

Para ello es necesario definir quien decidirá la frecuencia de las reuniones (horas, días, semanas) que podrá variar según el tipo de incidente y su evolución en el tiempo. Esta persona es normalmente el presidente del Comité.

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

· Llevar a cabo las tareas del Plan de Acción acordadas en la anterior reunión.

· Asignar o emprender acciones individuales.

· Supervisar el desarrollo de la estrategia.

· 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 miembros del Comité cuando no están reunidos.

6.1.6. 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 solucionadas que puedan reproducirse en el futuro.

Cabe recordar que un plan de crisis puede no perseguir necesariamente restituir los servicios de forma segura lo antes posible, operando al 100%, sino en restituirlos de forma segura a unos niveles acordados, es decir, se podría asumir trabajar un tiempo de forma segura en modo degradado/ precario pero razonable.

En ese caso, una vez superada la crisis, debe haber un plan de vuelta a la normalidad desde la operativa de recuperación (post mitigación y contención).

La vuelta a la normalidad puede alargarse en el tiempo y la desactivación del Comité de Crisis es tan sólo una de las acciones necesarias, pero no la única; ya que el cierre de las crisis requiere un trabajo programado y estructurado que sigue implicando a diferentes partes de la organización.

Se recomienda incorporar criterios que ayuden a decidir la desactivación del Comité de Crisis, por ejemplo:

· Si ya no es necesaria la implicación / dirección del personal del Comité y lo que quede pendiente puede ser ejecutado por otras personas.

· 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.

· Si los equipos operativos y/o locales pueden continuar trabajando sin el apoyo del Comité.

Independientemente de que se haya desconvocado el Comité, su Coordinador ha de velar por el correcto archivo de la información generada durante el incidente, prestando especial atención a la información que pueda ser de utilidad a servicios jurídicos en los meses siguientes y velando especialmente por las medidas de seguridad de la información.

6.1.7. Entrenamiento: simulaciones y pruebas

Para asegurar la mejor gestión de la crisis en el día D, es crucial que toda la plantilla esté entrenada (en la detección y notificación) y que los miembros de las estructuras de gestión hayan adquirido experiencia para el arranque sin dilación indebida de la gestión de incidentes.

En concreto, la mejor manera de poner a prueba al Comité de Cibercrisis es la realización de pruebas y simulaciones. Esta práctica ayuda a preparar a los miembros de los comités en la toma de decisiones bajo tensión y cómo equipo, a evaluar su reacción y capacidades y a concienciar a la organización en general de la importancia de la buena gestión de situaciones de crisis (ver figura 10). Las simulaciones también ayudan a identificar mejoras para el Plan de Gestión de Crisis y elaborar lecciones aprendidas.

Los beneficios de los ejercicios y simulaciones incluyen:

CAPACITACIÓN

- Preparación de los **miembros** de los comités
- Toma de **decisiones** en equipo y bajo tensión

EVALUACIÓN DE CAPACIDADES

- De coordinación **interna y externa**
- De **comunicación interna y externa**
- De **liderazgo**
- Revelar **carencias**, puntos débiles

CONCIENCIACIÓN

- Sobre **posibles** sucesos que deriven en crisis
- Sobre la importancia de la **preparación** para las crisis

PRUEBA

- Reacción de la organización
- Mecanismos

Figura 10.- Porqué hacer ejercicios y simulaciones de Gestión de Crisis.

6.1.8. Documentación

Toda la información previa debe quedar recogida en el Plan de Gestión de Crisis, incluyendo niveles de alerta y estados de gravedad, criterios de calificación/valoración/notificación, procedimiento de escalado, estructuras de gestión (Comité de Crisis con sus funciones, roles y miembros), protocolo de actuación por fases y medios, recursos y canales disponibles.

Además, el Plan de Gestión de Crisis es un documento global que debe incluir otros documentos más específicos como el Plan de Respuesta ante Ciberincidentes, el Plan de Continuidad o el Plan de Comunicación.

6.2. BUENAS PRÁCTICAS EN LA GESTIÓN DE CRISIS

La preparación y la adopción de las mejores prácticas para abordar una cibercrisis constituyen elementos fundamentales para manejar ciertas situaciones y para evitar que puedan desembocar en una crisis.

A continuación, se exponen buenas prácticas en la gestión de cibercrisis (más información en CCN-CERT BP/20 Buenas Prácticas en la Gestión de Cibercrisis) las cuales se relacionan a su vez con el ciclo de la gestión de riesgos - gestión de crisis (ver figura 11).

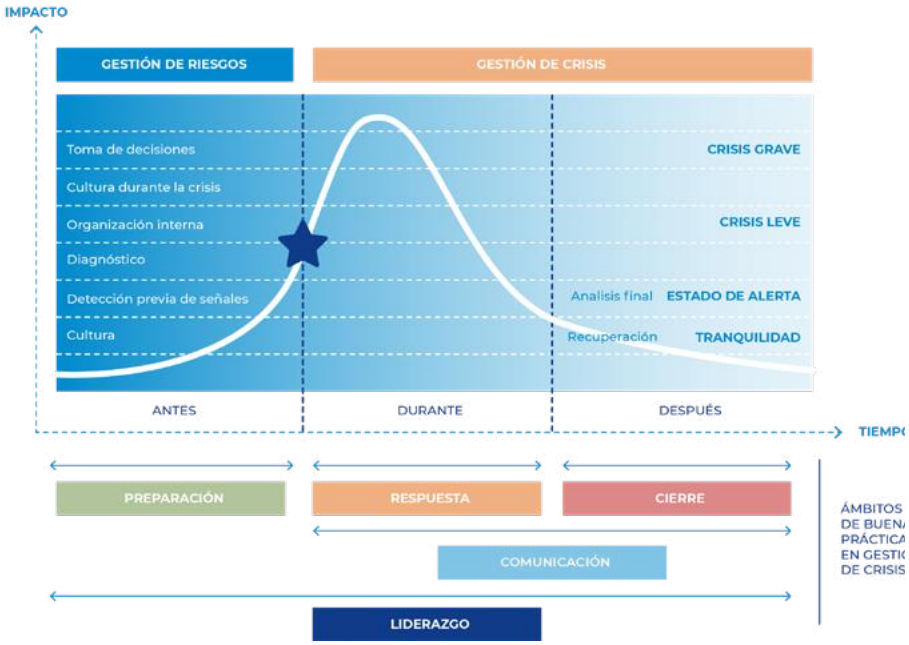


Figura 11.- Gestión de riesgos - Gestión de crisis.

6.2.1. Liderazgo, valores y control

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.

6.2.2. Planes y protocolos estructurales

Todo lo que no se prevea es prácticamente imposible improvisarlo durante la emergencia. Desde este punto de vista, las ciberamenazas exigen un constante ejercicio de prospectiva que persigue ser conscientes de las debilidades de la entidad y, de esta forma, poder preparase y anticiparse.

6.2.3. Superficie de exposición

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

6.2.4. Diagnóstico inicial y escenarios posibles

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).

6.2.5. Coordinación

La coordinación es la clave de la buena resolución de un incidente, elemento sobre el que hay que mantener una permanente vigilancia: entidades que se han preparado adecuadamente para abordar una situación grave de este tipo tienen tendencia a improvisar.

6.2.6. Iniciativa y proactividad

Del análisis de gran variedad de incidentes se observa que, en muchos casos, el ciberataque encuentra a la organización con falta de tensión para transitar rápidamente de sus prioridades habituales a la situación de crisis, no realizando un diagnóstico adecuado y perdiendo un tiempo inicial que, por una parte, da ventaja a los atacantes al no asegurar la rápida intervención del CSIRT de referencia y, por otra, hace que se vaya a remolque de los acontecimientos.

6.2.7. Cierre formal de una 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.

6.2.8. Implementación de lecciones aprendidas

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

Figura 12.- Buenas prácticas en la gestión de crisis.

centro criptológico nacional

APROXIMACIÓN AL MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD

PREVENCIÓN PROACTIVA

GOBIERNO DE ESPAÑA

MINISTERIO DE DEFENSA