UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

APROXIMACIÓN AL MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO:
APROXIMACIÓN AL MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD

Análisis de Prevención Proactiva, Arquitectura Organizativa y Gestión de Cibercrisis conforme al Esquema Nacional de Seguridad (ENS)

> *Documento de Referencia: Centro Criptológico Nacional (CCN), Ministerio de Defensa de España, 2022.*
>
> Ámbito Estratégico: Gobernanza de la Ciberseguridad, Prevención Proactiva, Gestión de Riesgos, SOC/COCS y Resiliencia Operativa.

1. Visión Estratégica y Fundamentos del Modelo

1.1. Contexto Estratégico y Diagnóstico de Amenazas

El entorno digital global enfrenta una transformación acelerada que ha ampliado exponencialmente la superficie de exposición y ataque de las organizaciones. Esta expansión responde a la adopción masiva del trabajo a distancia, la digitalización de servicios críticos y la interconexión de infraestructuras IT/OT. Paralelamente, los actores de amenaza han evolucionado hacia esquemas de alta sofisticación y persistencia:

- **Actores-Estado y Operaciones Híbridas:** Operaciones estatales dirigidas al ciberespionaje militar, político e industrial, así como ciberataques híbridos, campañas de desinformación e influencia estratégica.
- **Ciberdelincuencia Avanzada:** Profesionalización del cibercrimen mediante vectores como el Ransomware Operado por Humanos (Human-Operated Ransomware), ataques al Fraude del CEO y esquemas sofisticados de extorsión doble y triple.
- **Afectación a Sistemas Ciberfísicos (IT/OT):** Creciente focalización en entornos industriales y de control operativo donde la interrupción de la disponibilidad genera un impacto directo en la sociedad y la continuidad de servicios esenciales.

- **Exposición de Perímetros Remotos:** Compromiso masivo de soluciones VPN, protocolos de acceso remoto (RDP, SSH) e infraestructuras publicadas sin controles rigurosos de bastionado o autenticación multifactor.

1.2. El Paradigma de la Prevención Proactiva

La postura tradicional puramente reactiva (enfocada exclusivamente en la contención e investigación posterior a la intrusión) resulta estructuralmente insuficiente frente a vectores de ataque automatizados y grupos APT. El modelo del CCN postula una transición decisiva hacia la Prevención Proactiva basada en inteligencia y medición continua:

> *Axioma de la Prevención Proactiva:*
>
> «No es posible proteger lo que no se ve, ni gestionar lo que no se mide. Si se parametriza la superficie de exposición, se identifican las vulnerabilidades y se analiza la mala praxis, es posible predecir las vías de explotación del adversario y adelantarse a la materialización del ciberataque mediante decisiones orientadas al dato.»

Este enfoque traslada el ciclo de inteligencia a la arquitectura de defensa: modelar el entorno, formular hipótesis fundamentadas sobre la intención del atacante y priorizar la asignación de recursos técnicos y financieros en los puntos de mayor vulnerabilidad estructural.

1.3. El Esquema Nacional de Seguridad (ENS) como Eje Articulador

El Esquema Nacional de Seguridad (ENS, Real Decreto 3/2010 y sus actualizaciones) no debe concebirse como una carga administrativa estática, sino como un marco dinámico y estructurado de gestión del riesgo. A través de los Perfiles de Cumplimiento Específicos habilitados por el CCN, las entidades pueden rationalizar sus salvaguardas tecnológicas y organizativas, alineando la postura de ciberseguridad con la criticidad real de sus procesos de negocio y servicios prestados a la ciudadanía.

2. Arquitectura de Salvaguardas Integradas

2.1. Salvaguardas Organizativas, Normativas y Procedimentales

La ciberseguridad se sostiene prioritariamente sobre un marco de gobernanza sólido. Sin directrices claras y vinculantes aprobadas por la alta dirección, las salvaguardas tecnológicas carecen de efectividad operativa. El marco documental se articula en tres niveles jerárquicos:

Nivel Documental	Alcance y Naturaleza	Componentes y Aplicación
Política de Seguridad de la Información	Documento estratégico de alto nivel aprobado por el órgano directivo. Establece la misión, objetivos, estructura organizativa y compromiso directivo.	Atribución de responsabilidades, gestión de riesgos, roles de seguridad, mecanismos de resolución de conflictos e integración de normas internacionales (ej. ISO 22301).
Normativa Interna de Seguridad	Regulación obligatoria de uso de medios electrónicos para todo el personal y terceros con acceso a los sistemas de la entidad.	Políticas de uso aceptable de activos, obligaciones de confidencialidad, control de accesos, medidas disciplinarias y derechos de supervisión según legislación vigente.
Procedimientos de Seguridad	Documentación técnica detallada paso a paso sobre operaciones, configuraciones y mantenimiento seguro de infraestructuras.	Arquitectura de seguridad, gestión de usuarios, gestión de parches, mantenimiento, control de metadatos, copia de respaldo/recuperación y gestión de incidentes.

2.2. Salvaguardas Tecnológicas y Modelado de Amenazas

El diseño de la defensa cibernética se estructura mapeando las tácticas del adversario mediante el modelo Cyber Kill Chain de Lockheed Martin y las matrices MITRE ATT&CK Enterprise. Las defensas se despliegan en tres fases clave del ataque:

- **Fase de Intrusión:** Protección reforzada del correo electrónico (inspección de adjuntos, filtrado de macros, análisis de enlaces), bastionado estricto de servicios expuestos a Internet (RDP, SSH, VPN) e implementación estricta de doble factor de autenticación (2FA).
- **Fase de Movimiento Lateral:** Segmentación de red, control de privilegios de dominio, mitigación de técnicas de extracción de credenciales (ej. Mimikatz, Golden Ticket en Active Directory), restricción de uso de herramientas nativas del sistema operativo empleadas en ataques Living off the Land (LOL) y monitorización de scripts en memoria (PowerShell, WMI).
- **Fase de Explotación y Colonización:** Protección contra comunicación C2 (Command & Control), bloqueo de canales de exfiltración de datos, medidas anti-ransomware (aislamiento de copias de seguridad inmutables) y prevención de alteración de registros.

2.3. Vigilancia y Auditoría Continuas

Bajo los principios de un modelo Zero Trust (confianza cero), donde la legitimidad de cualquier activo o usuario debe ser constantemente verificada independientemente de su ubicación en la red, se requieren las siguientes capacidades de telemetría e inspección:

- **Visibilidad de la Red:** Descubrimiento automatizado e inventariado exhaustivo de activos conectados por cable, Wi-Fi o VPN previa concesión de acceso.
- **Monitorización Centralizada:** Sistemas SIEM/SOAR para la ingesta y correlación centralizada de logs procedentes de firewalls, controladores de dominio, IDS/IPS y plataformas EDR/XDR en endpoints.
- **Gestión de Vulnerabilidades:** Análisis automatizado de vulnerabilidades en código y sistemas, supervisión periódica de

conexiones con terceros (VPN site-to-site) y sustitución/protección compensatoria de protocolos obsoletos.

2.4. Salvaguardas Conductuales e Ingeniería Social

Reconociendo que la ingeniería social (phishing, smishing, vishing, media dropping) es la vía primaria de compromiso inicial, el factor humano debe transformarse de 'eslabón más débil' a 'primera línea de detección e informe'. El marco exige la implantación de un Plan Estratégico de Cultura en Ciberseguridad orientado por métricas de comportamiento:

- **Concienciación Adaptada:** Campañas periódicas diferenciadas para usuarios finales, personal directivo y comités ejecutivos.
- **Formación Especializada:** Capacitación en código seguro y arquitecturas de desarrollo para equipos de software; bastionado e ingeniería de detección para personal de sistemas y redes.
- **Métricas y Métodos:** Uso de indicadores de simulación de phishing, tasas de reporte activo y efectividad en la detección de incidentes conductuales.

3. Marco Organizativo de Gobernanza de la Ciberseguridad

3.1. Estructura Organizativa Básica de Gobierno

El gobierno eficaz de la ciberseguridad requiere una definición nítida de roles, competencias y líneas de reporte. El modelo básico propone una estructura funcional interconectada:

- **Comité de Seguridad TIC:** Órgano colegiado de máxima decisión ejecutiva en materia de seguridad y privacidad. Integra a responsables directivos, TI, Seguridad, Delegado de Protección de Datos (DPD), Asesoría Jurídica y Recursos Humanos.
- **Oficina de Gobernanza y Cumplimiento Normativo (OGCN):** Unidad responsable del asesoramiento normativo, alineamiento con el ENS, gestión de análisis de riesgos, plan de formación y gestión del cuadro de mando executivo.

- **Órgano de Auditoría Técnica (OAT):** Unidad especializada independiente encargada de la evaluación imparcial, auditorías de conformidad y verificación técnica de la efectividad de las salvaguardas.
- **Centro de Operaciones de Ciberseguridad (SOC / COCS):** Centro operacional encargado de los servicios de protección, monitorización 24/7, cibervigilancia, detección proactiva de amenazas y respuesta técnica a incidentes.

3.2. Funciones del Comité de Seguridad TIC

Sus competencias abordan de manera integral las dimensiones estratégicas y operativas de la entidad:

- **Desarrollo Normativo:** Aprobar y actualizar la Política de Seguridad de la Información, directrices internas e Instrucciones Técnicas de Seguridad.
- **Gestión de Riesgos:** Supervisar la Metodología de Análisis de Riesgos, validar las Declaraciones de Aplicabilidad y aprobar los niveles de riesgo asumibles por la organización.
- **Capacitación:** Establecer la estrategia de formación, concientización y certificación profesional para todo el personal.
- **Auditoría y Certificación:** Supervisar las auditorías de conformidad, la coordinación con el CCN y la integración en marcos europeos (ENISA).
- **Gestión de la Cadena de Suministro:** Garantizar la aplicación de las normativas de seguridad e interoperabilidad (ENS/ENI) en la contratación de servicios cloud y proveedores privados, exigiendo la certificación de conformidad ENS en pliegos de licitación.

3.3. Servicios de Prevención Proactiva de la Oficina de Gobernanza

La OGCN despliega un abanico de servicios continuos destinados a mantener la resiliencia operativa:

- **Gestión de Seguridad y Conformidad (INES, AMPARO, PILAR):** Uso asistido de herramientas oficiales del CCN-CERT para el cálculo del nivel de madurez, cumplimiento y riesgo dinámico.
- **Protección contra la Fuga de Información:** Implantación de controles de rotulado de documentos, DLP (Data Loss Prevention) y repositorios

seguros cifrados con gestión de derechos de acceso (soluciones LORETO y CARLA).

- **Evaluación Continuada de Exposición y Pentesting:** Realización continuada de auditorías de código, pentesting en caja blanca y negra, simulaciones de denegación de servicio e inventariado con la plataforma ANA del CCN-CERT.
- **Servicio de Cibervigilancia Externa:** Monitorización de fuentes abiertas (OSINT), redes sociales y repositorios de filtraciones para detectar registros de dominios fraudulentos, suplantaciones de marca, campañas de spam y credenciales corporativas expuestas.

3.4. El Órgano de Auditoría Técnica (OAT)

Para garantizar la validez legal de las evaluaciones de conformidad con el ENS, el OAT debe constituirse preservando su total independencia funcional y técnica respecto a la administración operativa de los sistemas. En el ámbito del Sector Público, los OAT deben seguir el proceso de reconocimiento oficial por el CCN (conforme a la Guía CCN-STIC 122), fundamentado en dos pilares: a) Capacidad técnica acreditada del equipo auditor, y b) Imparcialidad y ausencia estricta de conflicto de intereses. La acreditación expedida por el CCN tiene una validez de dos años renovables.

3.5. Modelos de Gobernanza Extendido y del COCS

En organizaciones de elevada dimensión o sometidas a regulaciones complejas (ej. Directiva NIS / Real Decreto-ley 12/2018), el modelo de gobernanza se amplía segregando estructuralmente la gestión del cumplimiento normativo de la gestión operacional:

Área de Responsabilidad	Líder Asignado	Unidades y Competencias Integradas
Área de Cumplimiento y	Responsable de Seguridad de la Información (CISO /	Dirige la Oficina de Gobernanza y Cumplimiento Normativo

Normativa	RSI)	(OGCN) y supervisa técnicamente el cumplimiento mediante el Órgano de Auditoría Técnica (OAT) y la gestión legal de incidentes.
Área de Operaciones de Seguridad	Responsable de las Operaciones de Seguridad (SOC Manager)	Dirige operativamente el Centro de Operaciones de Ciberseguridad (COCS), el Centro de Respuesta a Incidentes (CSIRT/CERT) y los servicios de vigilancia perimetral.

Por su parte, la estructura interna del COCS opera en tres niveles institucionales:

- **Nivel Estratégico:** Dirección Estratégica (RSI y representantes del CSIRT de referencia), responsable de las decisiones de alto nivel y rendición de cuentas.
- **Nivel Técnico:** Dirección Técnica, encargada de la supervisión de hitos de implantación y viabilidad técnica.
- **Nivel Operativo:** Nivel de Operación y Gestión, compuesto por la Oficina de Gestión, Oficina de Adecuación al ENS y la Oficina de Implantación (dividida en equipos especializados de Prevención, Detección, Gestión de Incidentes, Ingeniería y Protección).

4. Marco Operativo de Gestión de Cibercrisis

4.1. Concepto y Umbrales de Activación del Comité de Crisis

Una cibercrisis se define como una situación de baja probabilidad de ocurrencia pero de impacto extremo, cuyos efectos negativos perduran en el tiempo afectando la prestación de servicios, la reputación institucional, la

estabilidad económica o los derechos de los ciudadanos. La gestión de una cibercrisis exige tomar decisiones estratégicas en tiempos reducidos, bajo elevada presión y con información incompleta.

La activación del Comité de Crisis no debe realizarse de forma indiscriminada ante cualquier incidente. Conforme a las taxonomías oficiales del CCN-CERT (Guía CCN-STIC 817), el Comité se activa según la escala de peligrosidad e impacto:

- **Nivel 1 (Bajo) y Nivel 2 (Medio):** Gestionados directamente en el nivel operativo por los equipos de respuesta técnica dirigidos por el Responsable de Seguridad de la Información.
- **Nivel 3 (Alto), Nivel 4 (Muy Alto) y Nivel 5 (Crítico):** Requieren la constitución obligatoria y formal del Comité de Crisis para la toma de decisiones ejecutivas y estratégicas.

4.2. Composición y Roles Claros del Comité de Crisis

Para garantizar la fluidez en situaciones de extrema tensión, los roles del Comité de Crisis deben estar predefinidos formalmente en un Plan de Gestión de Cibercrisis, asignados a cargos institucionales concretos con suplentes claramente designados:

Rol en el Comité de Crisis	Funciones y Responsabilidades Clave durante la Crisis
Presidencia / Líder del Comité	Máxima autoridad directiva. Conduce el comité, lidera la toma de decisiones estratégicas, coordina la interlocución institucional al más alto nivel y aprueba el plan de acción.
Seguridad de la Información / Ciberseguridad	Coordinación técnica directa con el equipo de respuesta a incidentes (CSIRT), preservación de la cadena de custodia de evidencias digitales y evaluación del alcance técnico.
Sistemas y	Evaluación de la infraestructura afectada,

Tecnologías (IT / OT)	aislamiento técnico de redes, contención de daños y ejecución de medidas de recuperación de sistemas.
Cumplimiento Normativo / Jurídico / DPD	Evaluación de impacto legal, gestión de obligaciones de notificación a autoridades reguladoras (AEPD, CCN-CERT, INCIBE) en los plazos legales establecidos y protección del dato.
Continuidad de Negocio y Operaciones	Activación de planes de contingencia para mantener operativa la entidad en modo degradado/precario seguro y coordinación del restablecimiento de servicios críticos.
Comunicación Interna y Externa	Elaboración del discurso institucional unificado, designación del portavoz oficial, atención a medios de comunicación, redes sociales y gestión de expectativas de partes interesadas.
Finanzas y Recursos Humanos	Aprobación y provisión inmediata de fondos y recursos extraordinarios, así como soporte al personal operativamente afectado por situaciones de estrés extremo.

4.3. Dinámica Operativa de las Reuniones e Inter-reuniones

La gestión eficaz de la crisis exige instaurar una dinámica estructurada de 'reunión - pausa - reunión - pausa':

- **Agenda Tipo de Reunión:** Duración acotada, revisión estricta de hechos verificados (separando rumores de datos confirmados), revisión de la lista de control (checklist) preconcebida, asignación de responsabilidades individuales y fijación de la hora exacta de la siguiente reunión.

- **Documento de 'Notas y Acuerdos':** Bitácora oficial donde se registran con hora y fecha exacta todas las decisiones tomadas, medidas acordadas, responsables directos y plazos de ejecución.
- **Periodo Inter-reuniones:** Los miembros ejecutan el plan de acción, coordinan a sus equipos y recopilan nueva información que se canaliza en tiempo real hacia el Coordinador del Comité.

4.4. Criterios de Desactivación y Continuidad en Modo Degradado

La desactivación del Comité de Crisis no coincide necesariamente con la recuperación total del 100% de los servicios corporativos. Se puede asumir la operación temporal en modo degradado o precario siempre que se garanticen niveles mínimos de seguridad validados.

El Comité se desactiva cuando: a) Ya no se requiere la dirección ejecutiva de alto nivel, b) Existe una hoja de ruta formalizada de vuelta a la normalidad supervisada por equipos locales, y c) Los riesgos residuales se encuentran bajo control estricto.

4.5. Entrenamiento, Simulaciones y Lecciones Aprendidas

La capacidad de respuesta ante un evento catastrófico no se improvisa. Las organizaciones deben realizar simulaciones periódicas de cibercrisis (ejercicios Tabletop) para entrenar a los ejecutivos en la toma de decisiones bajo presión y evaluar las capacidades de comunicación interna y externa.

Tras el cierre formal de cada crisis, es imperativo realizar un análisis post-mortem de lecciones aprendidas que alimente directamente el Plan Director de Ciberseguridad, ajustando inversiones futuras y cerrando definitivamente las brechas identificadas.

5. Hoja de Ruta e Implementación Práctica

Para la puesta en marcha efectiva del Marco de Gobernanza propuesto por el CCN, se define una Hoja de Ruta en fases secuenciales de implementación:

- **Fase 1: Institucionalización (Meses 1-2):** Aprobación formal de la Política de Seguridad de la Información por la dirección ejecutiva y constitución oficial del Comité de Seguridad TIC.
- **Fase 2: Diagnóstico y Riesgos (Meses 3-4):** Identificación e inventariado de activos, categorización de sistemas según el ENS, análisis de riesgos mediante la herramienta PILAR y emisión de la Declaración de Aplicabilidad inicial.
- **Fase 3: Capacidades Operativas y SOC (Meses 5-8):** Creación de la Oficina de Gobernanza (OGCN), despliegue de soluciones de vigilancia (SIEM/EDR), integración en plataformas del CCN (INES, AMPARO, ANA) e implantación de planes de formación/concienciación.
- **Fase 4: Resiliencia y Certificación (Meses 9-12):** Redacción del Plan de Gestión de Cibercrisis, asignación formal de roles del Comité de Crisis, ejecución de pruebas de simulación y realización de la auditoría de conformidad formal por el Órgano de Auditoría Técnica (OAT) para la obtención del Certificado ENS.