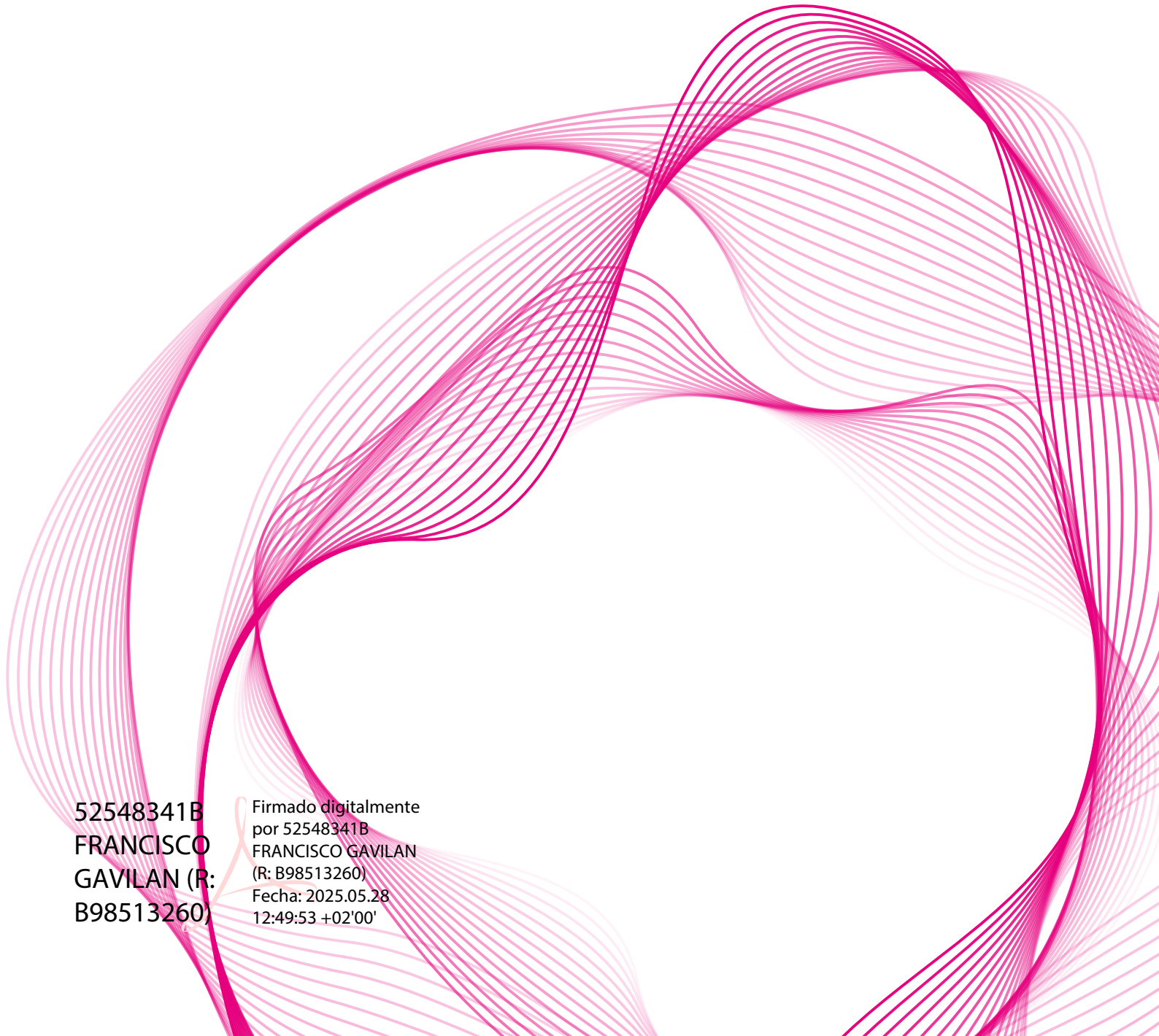
Acuerdo Marco de Suministro de Equipos Informáticos y de Servicios Asociados con destino a las entidades locales de Cataluña

Consorci Català pel Desenvolupament Local.

Expdte: 2024.01. Mayo 2025



52548341B FRANCISCO GAVILAN (R: B98513260)

Firmado digitalmente por 52548341B FRANCISCO GAVILAN (R: B98513260)
Fecha: 2025.05.28 12:49:53 +02'00'

ÍNDICE

1. Introducción

La transformación digital en la administración pública ha traído consigo importantes oportunidades de mejora en la prestación de servicios al ciudadano, pero también ha incrementado de forma exponencial los riesgos asociados a la ciberseguridad. Los sistemas de información de los entes locales procesan, almacenan y transmiten información crítica y datos personales sensibles, lo que los convierte en objetivos prioritarios para amenazas como el ransomware, el phishing o las brechas de datos. En este contexto, resulta imprescindible que las entidades públicas cuenten con servicios de ciberseguridad que no solo protejan sus infraestructuras, sino que garanticen la continuidad operativa, la respuesta ante incidentes y el cumplimiento normativo en un entorno en constante evolución.

El presente documento constituye la memoria técnica con la que **Sothis**, empresa del Grupo Nunsys, da respuesta a los requerimientos técnicos establecidos en el presente pliego para la contratación de servicios de ciberseguridad. Esta memoria está alineada con los ítems exigidos, y presenta una propuesta integral, estructurada y personalizada, orientada a acompañar a la entidad local contratante en todo el ciclo de gestión de la seguridad: desde el análisis y auditoría inicial, hasta la formación del personal y la respuesta ante situaciones de crisis.

La propuesta de **Sothis** se apoya en una trayectoria consolidada en el sector público y privado, en la capacidad operativa de su **Centro de Operaciones de Seguridad (SOC) ERIS-CERT®,** operativo 24x7 y certificado en el Esquema Nacional de Seguridad (ENS) nivel alto, ISO/IEC 27001, ISO 20000, ISO 9001 y 14001 e ISO 22301. Además, cuenta con un equipo multidisciplinar de expertos certificados (OSCP, CISM, CEH, PMP, etc.), con amplia experiencia en auditorías, gestión de incidentes, formación, concienciación y consultoría normativa. Esta combinación de infraestructura, metodología y talento nos permite garantizar una prestación del servicio rigurosa, ágil y adaptada a la realidad y necesidades del ente público.

La presente memoria desarrolla de forma detallada todos los aspectos solicitados en el pliego: el modelo de coordinación con la entidad contratante, la gestión proactiva de la seguridad, el procedimiento de actuación ante desastres, los servicios de auditoría técnica y asesoría especializada, el diseño de un plan de mejora y el despliegue de un programa formativo completo, tanto para personal general como para responsables TIC. Todos estos servicios están diseñados con un enfoque integral, escalable y conforme a los marcos normativos más exigentes, como el ENS, la Directiva NIS2, la LOPDGDD o la norma ISO/IEC 27001.

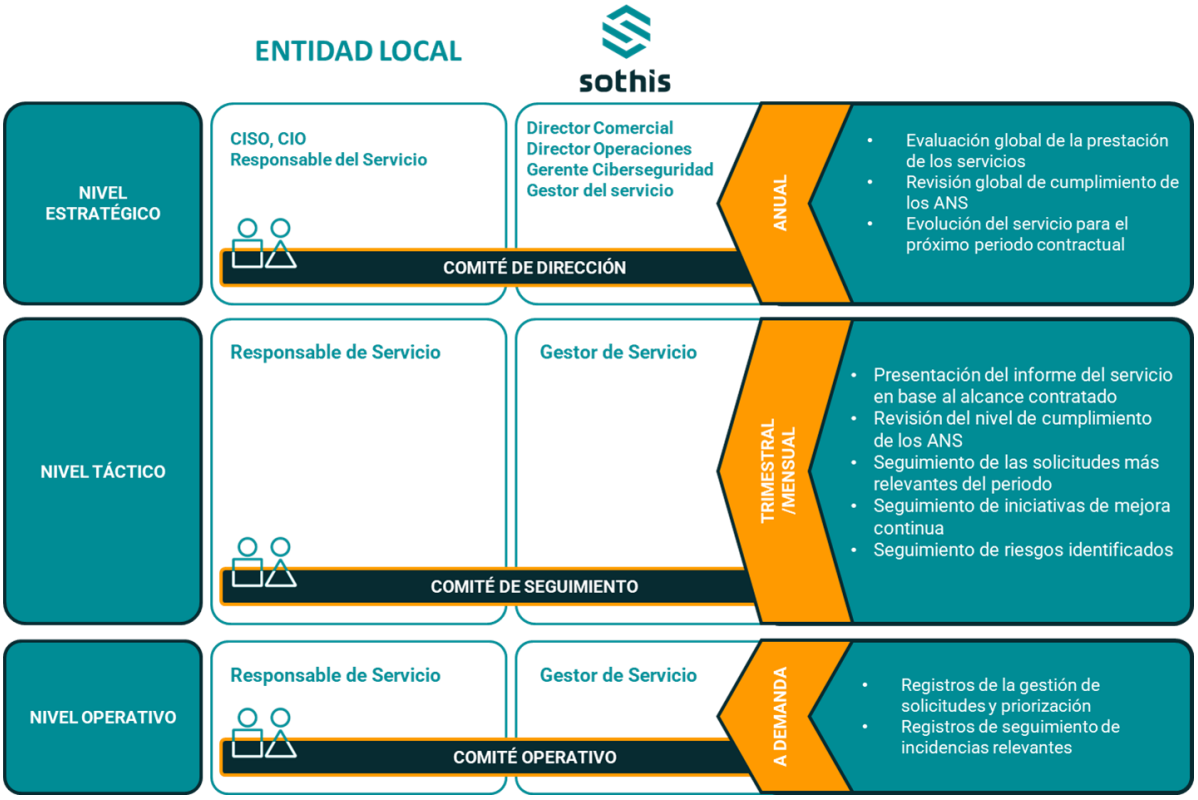
Sothis no solo ofrece capacidades técnicas contrastadas, sino también un compromiso firme con la mejora continua, la orientación al cliente y la protección efectiva del servicio público. Nuestra misión es convertirnos en un socio estratégico de la entidad contratante, aportando valor desde el primer día, anticipándonos a las amenazas, fortaleciendo la resiliencia institucional y consolidando una cultura de seguridad que perdure más allá del contrato.

2. Coordinación con la entidad local contratante

Durante toda la prestación del servicio, se establecerá un modelo de coordinación sólido, continuo y transparente entre Sothis y la entidad contratante. La relación se estructurará sobre una base de interlocución clara, con responsabilidades bien definidas, asegurando una comunicación fluida que facilite la ejecución eficiente del proyecto, el seguimiento técnico de las actividades y la resolución oportuna de cualquier incidencia que pudiera surgir.

Desde el inicio del servicio, se designará un Gestor del Servicio como punto único de contacto técnico con la entidad. Esta figura asumirá un papel central en la supervisión diaria, gestión de incidencias, coordinación de tareas planificadas y enlace con los distintos equipos de trabajo. La comunicación con el cliente se realizará de forma directa a través de canales seguros, y se dispondrá de un sistema de gestión de tickets permitiendo una trazabilidad total de todas las solicitudes y eventos reportados.

El modelo de coordinación propuesto se estructurará en tres niveles con el fin de asegurar un seguimiento exhaustivo, una resolución eficaz de incidencias y una gestión proactiva y continua del servicio.



Comité Estratégico

- **Propósito**: establecer una visión compartida de la evolución del servicio, alinear los objetivos estratégicos de la entidad con la planificación anual de ciberseguridad y revisar los compromisos adquiridos.
- **Participantes**: representantes del órgano contratante (CISO, CIO, Dirección de Sistemas) y de Sothis (Director Comercial, Responsable de Ciberseguridad, Gestor del Servicio).
- Frecuencia: anual.
- **Entregables**: actas de conclusiones, hoja de ruta estratégica, revisión de cumplimiento del plan anual y propuestas de evolución del servicio.

Comité Táctico

- **Propósito**: supervisar de forma continua el cumplimiento del contrato, gestionar la calidad del servicio, proponer acciones de mejora y resolver aspectos operativos no críticos.
- **Participantes**: responsable técnico de la entidad, Gestor del Servicio de Sothis y otros perfiles técnicos.
- **Frecuencia**: mensual o trimestral según necesidad.
- **Entregables**: informe de seguimiento del servicio (indicadores de rendimiento, estado de incidentes, acciones correctivas/preventivas, recomendaciones normativas).

Coordinación Operativa

- **Responsable**: el Gestor del Servicio (Service Manager) de Sothis, actuando como **punto único de contacto técnico (SPOC)** con la entidad.
- **Funciones**:
  - Seguimiento diario del estado de la seguridad.
  - Gestión de tickets, priorización y escalado.
  - Coordinación de actividades planificadas o reactivas (formación, auditoría, respuesta ante incidentes).

- Canal de comunicación ágil vía correo, teléfono y plataforma de ticketing 24x7.

Todo este modelo de coordinación estará documentado y sujeto a mejora continua. Se garantizará la entrega de actas, informes técnicos y resúmenes ejecutivos que reflejen el estado de las actuaciones, la situación de seguridad de la entidad y las propuestas de evolución. Así, se asegura una colaboración proactiva, eficaz y sostenida en el tiempo, en la que Sothis se integra como parte del equipo de ciberseguridad de la entidad pública.

3. Aspectos claves en materia de Ciberseguridad

La protección de los activos digitales y la continuidad operativa frente a incidentes de seguridad son pilares fundamentales en cualquier estrategia de ciberseguridad moderna, especialmente en el ámbito de la administración pública. La transformación digital, el aumento de la superficie de exposición y la sofisticación creciente de las amenazas hacen imprescindible contar con mecanismos sólidos de detección, protección, respuesta y recuperación. En este contexto, Sothis propone un enfoque integral que combina tecnología, experiencia y cumplimiento normativo, con el objetivo de garantizar la seguridad, disponibilidad e integridad de la información y los sistemas de la entidad. El presente apartado detalla los elementos esenciales de nuestra propuesta, incluyendo capacidades técnicas, metodologías de respuesta ante incidentes y planes de actuación frente a desastres, todo ello alineado con los estándares más exigentes del sector.

3.1. Servicio de asesoría

3.1.1. Auditoría y consultoría inicial

En una primera fase, se llevará a cabo una auditoría exhaustiva de los activos tecnológicos de la entidad cuyo objetivo será el de obtener una radiografía completa del estado de la ciberseguridad de la entidad contratante. Para ello el equipo de Sothis identificará vulnerabilidades en los sistemas y procedimientos de las entidades. Para ello se hará uso tanto de entrevistas con el personal de la entidad para evaluar sus procedimientos como de herramientas automatizadas de análisis de vulnerabilidades para detectar vulnerabilidades en los sistemas y técnicas manuales avanzadas perpetradas por nuestros especialistas. Este análisis incluirá tanto sistemas internos como servicios expuestos a Internet, así como el estado de la red, configuraciones de seguridad, control de accesos y políticas de cifrado. Se prestará especial atención a elementos críticos como el Directorio Activo y Azure AD, donde se revisarán privilegios, replicaciones, protocolos utilizados y mecanismos de autenticación, con el objetivo de detectar configuraciones inseguras, cuentas obsoletas o vulnerabilidades explotables. Entre otras, se podrán realizar las siguientes actividades:

- Escaneo automatizado y análisis manual de activos, usando herramientas como Tenable Nessus, OpenVAS, y scripts personalizados.
- Revisión de la arquitectura de red y sistemas críticos, tanto físicos como virtualizados (servidores, puestos, dispositivos móviles, entornos cloud).
- Auditoría de Active Directory y Azure AD:
  - Revisión de delegaciones de privilegios, cuentas huérfanas o inactivas.
  - Análisis de configuraciones inseguras, protocolos obsoletos, historial SID.
  - Revisión de logs, replicación, políticas de contraseñas, backups y confianza entre dominios.
- Análisis de aplicaciones críticas y servicios publicados: validación de su configuración segura, uso de certificados, cifrado, autenticación y protección frente a inyecciones (SQLi, XSS, etc.).
- Análisis de las políticas de seguridad implementadas en las entidades

Una vez completada la auditoría, se elaborará un informe técnico con evidencias detalladas, acompañado de un resumen ejecutivo orientado a facilitar la comprensión por parte de perfiles no técnicos. Ambos

documentos incluirán recomendaciones específicas para mitigar los riesgos identificados, priorizadas según criticidad e impacto en los servicios de la entidad.

3.1.2. Plan de Mejora

A partir de los resultados obtenidos en la fase de auditoría y consultoría inicial, se diseñará un plan de mejora que trace una hoja de ruta clara y alcanzable para la entidad contratante. Este plan incluirá propuestas técnicas y organizativas para reforzar la seguridad, como la adopción de herramientas EDR, segmentación de red, aplicación de políticas de doble factor, protección contra ransomware y revisión de procesos internos. Asimismo, el plan de mejora se alineará con los marcos normativos aplicables, incluyendo el Esquema Nacional de Seguridad (ENS), la Directiva NIS2, la LOPDGDD y la norma ISO/IEC 27001, garantizando que las actuaciones propuestas no solo mejoren la seguridad técnica, sino también el grado de cumplimiento legal y regulatorio de la organización.

El plan de mejora propuesto será acompañado de un cronograma de implementación, definición de responsables, recursos necesarios y métricas de seguimiento, permitiendo a la entidad avanzar de forma ordenada hacia un modelo de ciberseguridad robusto, resiliente y sostenible.

3.2. Servicio de formación en ciberseguridad

En un entorno digital cada vez más expuesto a amenazas sofisticadas y persistentes, la formación en ciberseguridad se consolida como un componente esencial para la protección de las organizaciones. No basta con implementar tecnologías avanzadas de defensa: es imprescindible contar con personas formadas, concienciadas y comprometidas con la seguridad. La administración pública, por la sensibilidad de los datos que gestiona y la criticidad de sus servicios, debe situar la capacitación de su personal como una prioridad estratégica. Por ello, Sothis propone un programa formativo integral, orientado tanto al personal general como a los responsables TIC, que combina contenidos actualizados, enfoque práctico, gamificación y seguimiento personalizado. A través de esta iniciativa, se busca no solo transmitir conocimientos, sino transformar hábitos y crear una cultura de seguridad sólida y transversal en toda la organización.

3.2.1. Servicio de Formación General en Ciberseguridad

Esta línea formativa está dirigida a todo el personal no técnico de la organización: personal administrativo, de atención al ciudadano, de gestión interna y operativa. El objetivo es sensibilizarles sobre los riesgos digitales a los que están expuestos en su día a día y proporcionarles las herramientas necesarias para reconocer y reaccionar adecuadamente ante posibles amenazas.

La propuesta formativa se estructura en sesiones dinámicas, accesibles y orientadas a la práctica. Las sesiones pueden desarrollarse tanto en modalidad presencial como online, adaptándose a los turnos y disponibilidad del personal. Cada sesión está conducida por profesionales con experiencia docente y técnica, que abordan los contenidos de forma cercana, empleando lenguaje claro, ejemplos reales y materiales visuales atractivos.

Los contenidos de estas sesiones incluyen, entre otros:

- **Introducción a la ciberseguridad**: por qué es importante, riesgos actuales, impactos reales.
- **Phishing y otras amenazas comunes**: cómo reconocer correos sospechosos, enlaces maliciosos, archivos adjuntos inseguros.
- **Gestión de contraseñas seguras**: buenas prácticas, riesgos del uso de contraseñas repetidas, almacenamiento seguro.
- **Uso seguro del correo electrónico y navegación**: identificación de intentos de fraude digital, control de la información compartida.
- **Redes sociales y dispositivos móviles**: riesgos de exposición, control de permisos, utilización en contextos profesionales.

- **Protección de datos personales y corporativos**: cumplimiento básico de la LOPDGDD y el deber de confidencialidad.
- **Buenas prácticas en el puesto de trabajo**: limpieza de escritorio, bloqueo de sesiones, almacenamiento físico de documentos sensibles.

Además, se podrán incorporar campañas de simulación de ataques sociales como phishing, smishing o vishing, para evaluar de forma realista el nivel de concienciación del personal. Estas campañas permiten establecer métricas de mejora y adaptar la formación a las necesidades detectadas.

Como refuerzo constante, se podrán establecer mecanismos complementarios de sensibilización, entre ellos:

- **Envío periódico de consejos prácticos de ciberseguridad** por correo electrónico, redactados en lenguaje sencillo.
- **Diseño y distribución de cartelería visual con mensajes clave**, colocada en lugares estratégicos (zonas comunes, comedores, puntos de impresión).
- Acciones puntuales como retos, concursos o “cibersemanas” temáticas, con actividades lúdico-formativas que fomentan la participación del personal.

Todas las acciones se planifican conjuntamente con la entidad, y pueden adaptarse a colectivos específicos o reforzarse en función de los resultados obtenidos. El objetivo no es solo formar, sino provocar un cambio de comportamiento sostenible, en el que cada empleado sea consciente de su rol en la defensa de la organización.

3.2.2. Formación Especializada para Responsables TIC

La segunda línea del programa de formación está destinada a los responsables técnicos, administradores de sistemas, personal del área TIC y, en general, a todos aquellos profesionales que gestionan, protegen o diseñan infraestructuras tecnológicas en la entidad.

Esta formación tiene un enfoque técnico, estratégico y normativo. No solo persigue el fortalecimiento de capacidades técnicas, sino también la capacitación del equipo para liderar el cumplimiento de las obligaciones legales en materia de seguridad de la información y garantizar la resiliencia operativa de la organización.

Las sesiones están dirigidas por expertos en ciberseguridad certificados (OSCP, CISM, ISO 27001 Lead Auditor, etc.), con amplia experiencia en gestión de proyectos, análisis de vulnerabilidades, diseño de arquitecturas seguras y respuesta ante incidentes en entornos públicos y privados.

Los contenidos formativos que se abordan son los siguientes:

- **Análisis y gestión de riesgos en sistemas de información**: identificación de activos, análisis de amenazas, evaluación del impacto y diseño de controles.
- **Diseño y operación de arquitecturas seguras**: segmentación de red, gestión de accesos, bastionado de sistemas, control de endpoints.
- **Respuesta ante incidentes de seguridad**: procedimientos de detección, contención, erradicación y recuperación. Documentación y lecciones aprendidas.
- **Gestión de vulnerabilidades**: escaneos periódicos, priorización, tratamiento y control de medidas correctoras.
- **Monitorización y correlación de eventos de seguridad**: principios de operación de SIEM, análisis de logs, reglas de correlación.
- **Cumplimiento normativo**: alineación de los sistemas con el ENS, NIS2, LOPDGDD e ISO/IEC 27001. Desarrollo de políticas, protocolos y evidencias.
- **Auditoría técnica y de cumplimiento**: preparación de entornos para auditorías internas o externas, gestión de no conformidades y planes de acción.

La formación puede estructurarse en módulos independientes o en itinerarios progresivos. Asimismo, es posible integrar laboratorios prácticos, ejercicios tipo CTF (Capture The Flag) o simulaciones controladas de ciberincidentes para una experiencia más inmersiva.

Esta capacitación se concibe como un proceso de acompañamiento, en el que el equipo TIC no solo adquiere conocimiento, sino también criterios técnicos y normativos para tomar decisiones informadas, priorizar inversiones y liderar la protección de los activos digitales de la entidad.

Al finalizar la formación, se entrega documentación técnica, materiales de referencia, ejercicios resueltos y certificados de asistencia. Además, se ofrece la posibilidad de realizar sesiones de consultoría individualizada para resolver dudas específicas o aplicar los contenidos al entorno real del cliente.

3.3. Procedimiento de actuación frente a desastres

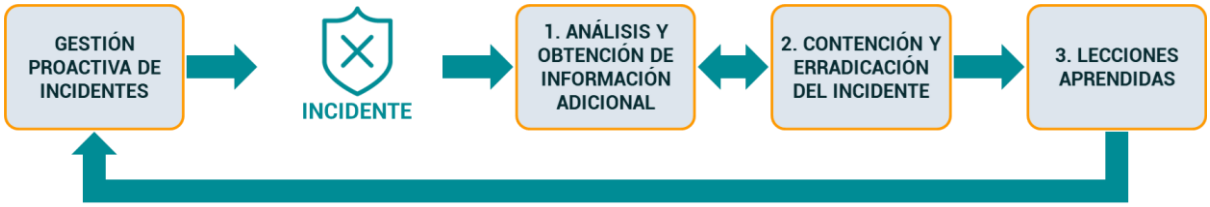
Se propone abordar la respuesta ante desastres mediante una metodología de respuesta reactiva, tal y como se describe a continuación:

1. **Respuesta reactiva**: Engloba aquellos casos impredecibles donde la respuesta de las medidas automatizadas no ha conseguido paliar el incidente. En estos casos se activa un estricto protocolo cuyo objetivo final es la mitigación del incidente causando el menor impacto de negocio posible.
2. **Cliente**: incidentes detectados directamente por los equipos y personal la entidad contratante

Etapas

Sothis dentro del marco metodológico de gestión global ante desastres, propone que tras la detección de un incidente se llevarán a cabo las siguientes etapas:

1. **Obtención de información adicional**: La recopilación preliminar de información es una de las fases más significativas del análisis y respuesta ante desastres. De esta fase se consiguen los datos contextuales necesarios para analizar la severidad del incidente y el modo de proceder.
2. **Contención y erradicación**: La mitigación se entiende como el objetivo final de la respuesta ante desastres Datos obtenidos en la fase anterior, como son la criticidad o el impacto, marcarán factores importantes de esta fase como son el marco temporal y la agresividad con la que se actúe para paliar el incidente.
3. **Lecciones aprendidas**: Una vez mitigado el incidente se iniciará una fase de lecciones aprendidas cuya finalidad es adecuar los procesos la entidad contratante para evitar casos similares. Esta fase también incluye un post análisis para asegurar la contingencia de riesgos residuales.



Metodología de Respuesta ante Incidentes

Durante las dos primeras etapas es posible que, para seguir avanzando en la respuesta al incidente, sea necesario realizar un análisis forense. Si así fuera el caso Sothis comunicaría dicha necesidad a la entidad, y en caso de que la entidad lo considerara oportuno se procedería con la metodología descrita.

Fases y actividades

Obtención de Información Adicional

Una vez que se detecta un incidente, lo más habitual es no disponer de toda la información necesaria para su contención y erradicación. Esta información varía significativamente en función del tipo de incidente. A continuación, y sin ánimo de ser exhaustivo, se enumeran algunos de los tipos de incidentes más habituales y la información que se necesita en cada uno de ellos:

- Fugas de información:
  - ISP involucrado
  - Datos de contacto del ISP.
  - Clientes afectados.
- Ataque de denegación de servicio:
  - Direcciones IPs y puertos origen del ataque.
  - Análisis de reputación: Listas negras
  - Técnica utilizada: Diferenciar entre ataques de denegación de servicio distribuidas por volumen y aquellas causadas por vulnerabilidades o fallos de implementación.
  - Búsqueda de patrones
- Intrusión en un servidor expuesto a internet:
  - Vulnerabilidad utilizada para acceder al sistema.
  - Dirección IP de origen del ataque.
  - Grado de intrusión: ¿se ha conseguido escalar privilegios?, ¿se ha instalado un rootkit?, ¿se ha accedido a terceros equipos? En estos casos el equipo de respuesta ante incidentes prestará especial atención en extraer información de manera que no se modifiquen evidencias forenses pertinentes.
- Código malicioso: Malware y ransomware:
  - Equipos afectados.
  - Archivos afectados.
  - Vector de entrada.
  - En el caso de ransomware: Técnica de cifrado empleado.

Una vez recopilada la información adecuada se procederá calcular la severidad del incidente y taxonomizarlo (contenido abusivo, código malicioso, recopilación de información, intentos de intrusión fallidos, intrusiones, ataques genéricos sin impacto, disponibilidad, fraude, acceso no autorizado).

Esta información será clave para establecer los marcos de actuación en la fase de contención y erradicación.

Caso del que el incidente afecte a datos personales

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” como “todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”

Debe quedar claro que la “brecha” definida en el RGPD, aunque es un tipo de incidente de seguridad, solo es aplicable cuando afecte a los datos de carácter personal y, por tanto, pudiera comprometer el cumplimiento lo previsto en el RGPD.

Por tanto, se debe tener en cuenta que, aunque todas las brechas de datos personales son incidentes de seguridad, no todos los incidentes de seguridad son necesariamente brechas de datos personales.

Una vez que el incidente de seguridad ha sido identificado y clasificado, el plan de acción se activará, y allí es donde el equipo de CSIRT ayudará y asesorará a la entidad en el análisis de la brecha de seguridad y el proceso de notificación, prestando el asesoramiento legal en materia de protección de datos y privacidad.