LOGO

Plan de Seguridad Informática Integral

Diseño, implementación y auditoría del sistema de seguridad de la información

CLIENTE

_____

VERSIÓN

v0.1

FECHA

Febrero 2026

CLASIFICACIÓN

Confidencial

AUTOR

_____

REFERENCIA

PSI-Febr-001

Control de Cambios

VERSIÓN	FECHA	AUTOR	DESCRIPCIÓN
v0.1	Febrero 2026	_____	Versión inicial

Distribución

NOMBRE	PUESTO	COPIA
_____ — Dirección	Dirección General	Electrónica
_____ — TI	Responsable de TI	Electrónica
_____	Consultor de seguridad	Electrónica

Confidencial

Índice

Confidencial

1. Anexo de Evidencia y Trazabilidad

Confidencial

0.1. Resumen Ejecutivo

El presente documento establece el marco de seguridad informática para la organización, definiendo las medidas de protección necesarias, el plan de implementación por fases y los mecanismos de verificación continua.

El plan se estructura en **12 dominios de seguridad** y propone un **roadmap de implementación en cuatro fases** (0–30, 30–90, 90–180 y 180+ días), priorizando las acciones de mayor impacto inmediato.

Las recomendaciones contenidas en este informe se fundamentan exclusivamente en marcos de referencia reconocidos: ENS, NIST CSF v2, CIS Benchmarks, y guías del CCN-CERT e INCIBE. No se ha incluido contenido que no esté respaldado por la documentación de referencia analizada.

Principales áreas de actuación:

- Implantación de autenticación multifactor y gestión de identidades
- Bastionado de endpoints y servidores (Windows, macOS, dispositivos móviles)
- Protección del perímetro de red y cifrado de comunicaciones
- Estrategia de copias de seguridad y recuperación ante desastres
- Desarrollo de un plan de respuesta a incidentes y continuidad de negocio
- Programa de concienciación y formación en ciberseguridad

0.2. Alcance, Supuestos y Exclusiones

Alcance

Este plan cubre la totalidad de los dominios de seguridad de la información aplicables a la organización:

DOMINIO	COBERTURA
Gobernanza y gestión de riesgos	Completa
Normativa y cumplimiento (ENS, RGPD, NIST)	Completa
Identidad y control de acceso	Completa
Endpoint y bastionado	Completa
Red y perímetro	Completa
Correo electrónico y navegadores	Completa

Confidencial

DOMINIO	COBERTURA
Dispositivos móviles	Completa
Nube y virtualización	Completa
Desarrollo seguro	Completa
Respuesta a incidentes y continuidad	Completa
Concienciación y formación	Completa
Monitorización y amenazas emergentes	Completa

Supuestos

- La organización dispone de infraestructura TI operativa con sistemas Windows y/o macOS.
- Existen servicios de correo electrónico corporativo con dominio propio.
- La organización está sujeta al cumplimiento del ENS y/o RGPD.
- Se dispone de recursos internos o externos para la ejecución técnica de las medidas propuestas.

Exclusiones

- Seguridad de entornos industriales (OT/ICS/SCADA), salvo que se amplíe el alcance.
- Pruebas de penetración y auditoría de seguridad ofensiva (se proponen como fase posterior).
- Arquitectura Zero Trust detallada (se recomienda como evolución futura).
- Implementación de SOC/SIEM (se describe como recomendación, pendiente de dimensionar).

0.3. Situación Actual (AS-IS)

La evaluación de la situación actual se realizará en la fase de discovery. A continuación se presenta la estructura que guiará dicha evaluación:

DOMINIO	ESTADO ESTIMADO	OBSERVACIONES
Gobernanza	Pendiente de evaluación	Verificar existencia de política de seguridad y roles designados
Normativa	Pendiente de evaluación	Determinar categoría ENS y estado de adecuación
IAM	Pendiente de evaluación	Verificar estado de MFA y política de contraseñas
Endpoint	Pendiente de evaluación	Inventariar SO y estado de bastionado

Confidencial

DOMINIO	ESTADO ESTIMADO	OBSERVACIONES
Red	Pendiente de evaluación	Revisar segmentación y reglas de cortafuegos
Correo	Pendiente de evaluación	Verificar registros SPF/DKIM/DMARC
Móviles	Pendiente de evaluación	Verificar existencia de MDM
Nube	Pendiente de evaluación	Identificar proveedores y certificaciones
Desarrollo	Pendiente de evaluación	Revisar ciclo de vida y prácticas actuales
Incidentes	Pendiente de evaluación	Verificar existencia de plan de respuesta
Concienciación	Pendiente de evaluación	Revisar programa formativo actual
Monitorización	Pendiente de evaluación	Evaluar capacidades de detección

Esta tabla se completará tras el taller de discovery inicial con el equipo técnico y la dirección.

0.4. Gobernanza y Gestión de Riesgos

Marco de Gobernanza

Se propone establecer una estructura de gobernanza de ciberseguridad que incluya:

- **Oficina de Seguridad:** establecimiento de una oficina que asista en la implantación de políticas, procedimientos y normativa para la protección de los activos de la organización.
- **Roles y responsabilidades:** designación formal del Responsable de Seguridad, Responsable del Sistema y Responsable de la Información según los requisitos del ENS.
- **Normativa interna:** desarrollo de políticas que definan las directrices de actuación ante circunstancias no contempladas explícitamente.
- **Capacitación:** plan de formación y concienciación continuo para todo el personal.

Análisis de Riesgos

- Aplicación de la metodología PILAR para el análisis y gestión de riesgos, incluyendo análisis de impacto y continuidad de operaciones.
- Determinación de la superficie de exposición e inventario de activos y servicios.
- Definición de métricas para la evaluación del desempeño de la gestión de seguridad.

Confidencial

Plan Director de Seguridad

Elaboración de un Plan Director que establezca objetivos, alcance, fases de implementación e indicadores de seguimiento.

0.5. Normativa y Cumplimiento

Esquema Nacional de Seguridad (ENS)

El proceso de adecuación al ENS contempla las siguientes fases:

1. **Identificación** de servicios e información incluidos en el alcance.
2. **Categorización** del sistema según criterios de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
3. **Declaración de Aplicabilidad** con los controles exigidos según la categoría del sistema.
4. **Implementación** de medidas organizativas, operacionales y de protección.
5. **Auditoría y certificación** periódica del cumplimiento.

RGPD y Protección de Datos

- Realización de evaluaciones de impacto en la protección de datos (EIPD).
- Designación del Delegado de Protección de Datos cuando sea obligatorio.
- Implementación de medidas técnicas y organizativas para garantizar confidencialidad, integridad, disponibilidad y resiliencia.
- Mantenimiento de registros de actividades de tratamiento.

NIST Cybersecurity Framework v2

Alineación de controles con las seis funciones del NIST CSF v2: Gobernar (GV), Identificar (ID), Proteger (PR), Detectar (DE), Responder (RS) y Recuperar (RC).

0.6. Identidad y Control de Acceso

Autenticación

- **Autenticación multifactor (MFA) obligatoria** en todos los accesos a sistemas críticos. El tipo y método de autenticación deben formar parte del diseño desde el inicio.

Confidencial

- **Tipos soportados:** tokens físicos o digitales, biometría, certificados electrónicos, tarjetas inteligentes.
- **Política de bloqueo:** bloqueo automático de cuentas tras 3 intentos fallidos consecutivos.

Gestión de Credenciales

- Políticas de complejidad y rotación de contraseñas.
- Prohibición de almacenamiento de credenciales en texto claro.
- Uso de gestores de contraseñas corporativos.

Principio de Privilegio Mínimo

- Asignación de permisos según la necesidad operativa (need-to-know).
- Revisiones periódicas de permisos y accesos privilegiados.
- Segmentación de roles administrativos.

0.7. Endpoint y Bastionado

Configuración Segura de Endpoints

- Aplicación de baselines de bastionado según el sistema operativo.
- Cifrado de todas las comunicaciones entre endpoints y servicios.
- Control de dispositivos USB, cifrado de disco completo y protección anti-malware.

Windows

- Aplicación del CIS Benchmark para Windows 11 Enterprise v4.0.0 (1.466 controles documentados).
- Configuración de políticas de grupo (GPO): auditoría, control de cuentas, cifrado BitLocker, Windows Defender, firewall y restricción de software.

macOS

- Aplicación de las recomendaciones de seguridad del CCN-CERT para macOS.
- Configuración de FileVault, Gatekeeper, firewall integrado y System Integrity Protection.
- Gestión centralizada de actualizaciones.

Gestión de Configuración

Implementación de un control efectivo de configuración y gestión de software, garantizando que los archivos ejecutables y plantillas compartidas residan en directorios de solo lectura.

Confidencial

0.8. Red y Perímetro

Cortafuegos y Segmentación

- Establecimiento de políticas de red que permitan controlar granularmente las conexiones permitidas.
- Aproximación de lista blanca (whitelisting): habilitación únicamente de las conectividades estrictamente necesarias.
- Segmentación de red por zonas de seguridad (DMZ, LAN interna, gestión).

Comunicaciones Cifradas (HTTPS/TLS)

- Forzado de HTTPS en todos los servicios web internos y externos.
- Configuración de TLS 1.2 como mínimo (preferiblemente TLS 1.3).
- Gestión centralizada de certificados digitales.

Protección frente a Denegación de Servicio

- Implementación de medidas anti-DDoS en cortafuegos perimetrales.
- Evaluación del uso de CDN con capacidades de mitigación.

Redes Inalámbricas

- Uso de WPA3 (o WPA2-Enterprise con RADIUS como mínimo).
- Separación de redes WiFi corporativas, de invitados y de IoT.

0.9. Correo Electrónico y Navegadores

Seguridad del Correo

- **SPF, DKIM y DMARC** en todos los dominios corporativos:
- SPF: verificación del dominio remitente autorizado.
- DKIM: firma digital de correos salientes.
- DMARC: política objetivo `p=reject` para protección contra spoofing.
- Cifrado de comunicaciones sensibles mediante GPG/S-MIME.

Confidencial

Navegadores Web

- Aplicación de configuraciones de seguridad para Chrome, Firefox y Edge según las guías del CCN-CERT.
- Deshabilitación de plugins innecesarios, forzado de actualizaciones automáticas.
- Políticas de navegación segura y lista blanca de extensiones.

0.10. Dispositivos Móviles

Gestión MDM

- Implementación de una solución de Mobile Device Management (MDM) centralizada.
- Definición de perfiles de configuración con valores recomendados por plataforma.
- Evaluación de funcionalidades MDM según las plataformas en uso.

Políticas por Plataforma

- **Android:** aplicación de las configuraciones de seguridad documentadas (162+ controles).
- **iOS/iPad:** empleo seguro según las guías del CCN-STIC para iOS 18 y servicios Apple.
- **BYOD:** políticas de separación de datos corporativos y personales.

Seguridad Nativa

- Aprovechamiento de capacidades integradas: Secure Enclave, cifrado en reposo, sandboxing de aplicaciones.
- Restricciones de instalación de aplicaciones y control de funcionalidades.

0.11. Nube y Virtualización

Protección del Dato en la Nube

- Las medidas de seguridad deben implementarse de forma preventiva, antes de que se produzca un incidente.
- Firma de Acuerdos de Nivel de Servicio (ANS) que garanticen disponibilidad, integridad, confidencialidad y trazabilidad.
- Verificación de certificaciones del proveedor cloud cuando se requiera cumplimiento con el ENS.

Confidencial

Virtualización

- Aplicación de buenas prácticas de seguridad en entornos virtualizados.
- Aislamiento de hipervisores y redes de gestión.
- Cifrado de comunicaciones entre nodos virtuales.

Contenedores y Orquestación

- Aplicación de las recomendaciones de seguridad para Kubernetes del CCN-CERT.
- Configuración de RBAC, network policies y pod security standards.
- Escaneo de imágenes de contenedores previo al despliegue.

Copias de Seguridad

- Implementación de la regla 3-2-1: 3 copias, 2 medios distintos, 1 fuera de las instalaciones.
- Verificación periódica de la integridad y restaurabilidad de las copias.
- Dimensionamiento del ancho de banda necesario para copias en la nube.

0.12. Desarrollo Seguro

Principios

- Protección de datos mediante mecanismos de autorización y segmentación entre entornos.
- Uso exclusivo de medios externos autorizados.
- Borrado seguro obligatorio de archivos con información sensible.

Controles por Fase del Ciclo de Vida

FASE	CONTROLES CLAVE
Diseño	Modelado de amenazas, requisitos de seguridad, MFA, protección de datos sensibles
Desarrollo	Revisión de código, SAST, gestión de dependencias, secrets management
Testing	DAST, pruebas de penetración, fuzzing
Despliegue	Bastionado de servidores, CI/CD seguro, configuración segura
Operación	Monitorización, parcheado, respuesta a incidentes

Confidencial

Seguridad en CMS y Bases de Datos

- **CMS (Drupal):** aplicación de las 78 recomendaciones de la guía CCN-STIC.
- **Bases de datos:** bastionado de BBDD (DB2 y general), restricción de accesos administrativos, cifrado de datos sensibles.

0.13. Respuesta a Incidentes y Continuidad

Gestión de Cibercrisis

- Establecimiento de un procedimiento formal de gestión de cibercrisis con roles, canales de comunicación y escalado definidos.
- Realización de ejercicios periódicos de simulación.
- Preparación organizativa previa: la capacidad de respuesta debe construirse antes de que se produzca un incidente.

Ransomware

FASE	MEDIDAS
Prevención	Segmentación de red, copias de seguridad offline, MFA, parcheo continuo
Detección	Monitorización de comportamientos anómalos, EDR/XDR
Respuesta	Aislamiento de equipos afectados, preservación de evidencias, comunicación de crisis
Recuperación	Restauración desde copias limpias, verificación de integridad previa a la reconexión

Continuidad de Negocio

- Elaboración de BCP/DRP con RTOs y RPOs definidos para cada servicio crítico.
- Uso de la herramienta PILAR para el análisis de impacto y continuidad de operaciones.
- Pruebas de recuperación con periodicidad mínima anual.

Prevención de Fuga de Información

- Implementación de herramientas DLP (Data Loss Prevention).
- Clasificación de la información por niveles de sensibilidad.
- Medidas preventivas implementadas antes de la ocurrencia de incidentes.

Confidencial

0.14. Concienciación, IoT y Amenazas Emergentes

Formación y Concienciación

- Programa de concienciación continuo para todos los niveles de la organización.
- Simulaciones de phishing periódicas con seguimiento de resultados.
- Formación específica por perfil: técnico, directivo y usuario general.

Internet de las Cosas (IoT)

- Inventario completo de dispositivos IoT conectados a la red.
- Segmentación de la red IoT respecto a la red corporativa.
- Políticas de actualización de firmware y cambio de credenciales por defecto.

Amenazas Emergentes

- **Cryptojacking:** monitorización de consumo anómalo de CPU/GPU, bloqueo de scripts de minería.
- **Inteligencia artificial en ciberseguridad:** evaluación de capacidades de detección basada en machine learning.
- **Desinformación:** protocolos de respuesta ante campañas que puedan afectar a la organización.

0.15. Teletrabajo

Recomendaciones

- Conexiones VPN con autenticación fuerte (MFA).
- Políticas de seguridad específicas para equipos remotos.
- Cifrado completo de disco en portátiles corporativos.
- Gestión de sesiones remotas con timeout y bloqueo automático.
- Separación de entornos personales y corporativos en equipos de teletrabajo.

Confidencial

0.16. Roadmap de Implementación por Fases

Fase 0 — Higiene Base (0–30 días)

ACCIÓN	DOMINIO	PRIORIDAD
Activar MFA en todos los accesos críticos	IAM	CRÍTICA
Implementar copias de seguridad 3-2-1	Backup	CRÍTICA
Inventario de activos y servicios	Gobernanza	CRÍTICA
Aplicar SPF+DKIM+DMARC en dominios de correo	Correo	CRÍTICA
Segmentar red WiFi (corporativa vs. invitados)	Red	ALTA
Bastionado básico de endpoints (antivirus, firewall, cifrado)	Endpoint	ALTA
Programa de concienciación básico	Personas	ALTA

Fase 1 — Bastionado Sistemático (30–90 días)

ACCIÓN	DOMINIO	PRIORIDAD
Aplicar CIS Benchmark en Windows	Endpoint	ALTA
Configurar HTTPS/TLS en todos los servicios	Red	ALTA
Implementar MDM para dispositivos móviles	Móviles	ALTA
Bastionado de navegadores (Chrome/Firefox/Edge)	Navegadores	MEDIA
Configurar whitelisting de red en cortafuegos	Red	ALTA
Bastionado de bases de datos	AppSec	MEDIA
Configurar seguridad en entornos cloud/virtual	Nube	MEDIA

Fase 2 — Gobernanza y Normativa (90–180 días)

ACCIÓN	DOMINIO	PRIORIDAD
Elaborar Plan Director de Seguridad	Gobernanza	ALTA
Análisis de riesgos con PILAR	Riesgos	ALTA

Confidencial

ACCIÓN	DOMINIO	PRIORIDAD
Declaración de Aplicabilidad ENS	Normativa	ALTA
Política de desarrollo seguro (SSDLC)	AppSec	MEDIA
Procedimientos de respuesta a incidentes	IR	ALTA
Plan de continuidad de negocio (BCP/DRP)	Continuidad	MEDIA
Adecuación RGPD	Legal	MEDIA

Fase 3 — Mejora Continua (180+ días)

ACCIÓN	DOMINIO	PRIORIDAD
Ejercicios de cibercrisis y simulacros	IR	MEDIA
Pruebas de penetración periódicas	AppSec	MEDIA
Métricas de seguridad y cuadros de mando	Gobernanza	MEDIA
Integración de IA para detección de amenazas	Monitorización	NORMAL
Revisión y actualización anual del plan	Gobernanza	MEDIA

0.17. Matriz de Riesgos

A continuación se presenta una valoración inicial de los principales riesgos identificados, basada en los dominios evaluados. Esta matriz se refinará tras la fase de discovery.

RIESGO	PROBABILIDAD	IMPACTO	NIVEL	MITIGACIÓN PROPUESTA
Acceso no autorizado por ausencia de MFA	Alta	Crítico	CRÍTICA	Implantación inmediata de MFA en sistemas críticos
Pérdida de datos por falta de copias de seguridad	Media	Crítico	CRÍTICA	Estrategia 3-2-1 con verificación periódica
Ransomware por endpoint no bastionado	Alta	Crítico	CRÍTICA	CIS Benchmark + EDR + segmentación de red
Suplantación de identidad por correo (phishing)	Alta	Alto	ALTA	SPF+DKIM+DMARC + programa de concienciación

Confidencial

RIESGO	PROBABILIDAD	IMPACTO	NIVEL	MITIGACIÓN PROPUESTA
Fuga de información por dispositivo móvil no gestionado	Media	Alto	ALTA	MDM + políticas BYOD + cifrado
Exposición de servicios internos sin cifrar	Media	Alto	ALTA	Forzado de HTTPS/TLS en todos los servicios
Incumplimiento normativo (ENS/RGPD)	Media	Alto	ALTA	Plan de adecuación con calendario definido
Vulnerabilidades en aplicaciones web	Media	Medio	MEDIA	SSDLC + SAST/DAST + bastionado CMS
Acceso a la red por dispositivos IoT inseguros	Baja	Medio	MEDIA	Segmentación de red IoT + inventario
Interrupción de negocio sin plan de recuperación	Baja	Crítico	ALTA	BCP/DRP con pruebas anuales

0.18. Matriz RACI

Asignación genérica de responsabilidades por dominio de actuación. Se ajustará a la estructura organizativa real tras la fase de discovery.

ACTIVIDAD	RESPONSABLE (R)	APROBADOR (A)	CONSULTADO (C)	INFORMADO (I)
Gobernanza y políticas	CISO / Resp. Seguridad	Dirección General	Legal, IT	Todos
Análisis de riesgos	Resp. Seguridad	CISO	Áreas de negocio	Dirección
Bastionado de endpoints	Equipo Sistemas	Resp. Seguridad	Soporte IT	CISO
Gestión de red y perímetro	Equipo Redes	Resp. Seguridad	Arquitectura IT	CISO
Seguridad del correo	Equipo Sistemas	Resp. Seguridad	Comunicación	Usuarios
	Equipo Sistemas		RRHH	Usuarios

Confidencial

ACTIVIDAD	RESPONSABLE (R)	APROBADOR (A)	CONSULTADO (C)	INFORMADO (I)
Gestión de móviles (MDM)		Resp. Seguridad		
Seguridad en la nube	Equipo Cloud	Resp. Seguridad	Proveedores	CISO
Desarrollo seguro	Equipo Desarrollo	Resp. Seguridad	QA	CISO
Respuesta a incidentes	CSIRT / Resp. Seguridad	Dirección	Legal, Comunicación	Todos
Concienciación y formación	RRHH / Resp. Seguridad	Dirección	Comunicación	Todos
Cumplimiento normativo	Legal / DPO	Dirección General	Resp. Seguridad	Auditoría
Copias de seguridad	Equipo Sistemas	Resp. Seguridad	Áreas críticas	CISO

0.19. Checklist de Implementación y Evidencias

CONTROL	ENTREGABLE	EVIDENCIA REQUERIDA AL CLIENTE
MFA activo	Configuración de MFA en sistemas críticos	Captura de configuración, informe de cobertura
Copias de seguridad	Estrategia 3-2-1 implementada	Logs de ejecución + prueba de restauración
Antivirus/EDR	Protección desplegada en endpoints	Dashboard de estado de protección
Cortafuegos	Reglas de segmentación aplicadas	Reglas exportadas + changelog
SPF/DKIM/DMARC	Registros DNS configurados	Registros DNS + informes DMARC
Bastionado Windows	CIS Benchmark aplicado	Resultado de escaneo CIS-CAT o equivalente
MDM	Dispositivos gestionados	Lista de dispositivos + políticas activas

Confidencial

CONTROL	ENTREGABLE	EVIDENCIA REQUERIDA AL CLIENTE
Cifrado de disco	BitLocker/FileVault habilitado	Estado de cifrado en inventario
Formación	Programa de concienciación ejecutado	Registro de asistencia + resultados phishing
Incidentes	Plan de respuesta documentado	Procedimiento + registro de incidentes
Actualizaciones	Parcheado gestionado	Informe de vulnerabilidades pendientes
Privilegios	Revisión de accesos completada	Listado de usuarios con permisos administrativos

0.20. Próximos Pasos

Fase Inmediata (próximas 2 semanas)

1. **Taller de Discovery:** sesión conjunta con el equipo técnico y la dirección para:
2. Completar la evaluación AS-IS de la tabla de situación actual.
3. Identificar sistemas críticos y prioridades específicas.
4. Validar el roadmap propuesto y ajustar plazos.
5. **Recolección de evidencias inicial:** el equipo facilitará:
6. Inventario de activos y servicios TI.
7. Configuración actual de correo (registros DNS).
8. Estado de los endpoints (SO, antivirus, cifrado).
9. Diagrama de red (si existe).
10. **Validación del plan:** revisión conjunta del presente documento con los responsables para confirmar prioridades y asignación de recursos.

Calendario Propuesto

HITO	PLAZO
Taller de discovery	Semana 1
Entrega de evaluación AS-IS completada	Semana 2
Inicio de Fase 0 (higiene base)	Semana 3

Confidencial

HITO	PLAZO
Revisión de progreso Fase 0	Semana 6
Inicio de Fase 1 (bastionado)	Semana 7
Revisión de progreso Fase 1	Semana 13
Inicio de Fase 2 (gobernanza)	Semana 14

0.21. Referencias Consultadas

Las recomendaciones de este plan se fundamentan en las siguientes familias de marcos, estándares y guías de referencia:

FAMILIA	ÁMBITO
CCN-CERT (Buenas Prácticas)	Guías de bastionado, correo, navegadores, teletrabajo, cibercrisis, ransomware, desarrollo seguro, IoT, IA, bases de datos, virtualización, nube
CCN-STIC	Guías de seguridad de dispositivos móviles, Apple, Drupal, PILAR, endpoint, etiquetas de seguridad
INCIBE	Guías empresariales de ciberseguridad, gestión de riesgos, ransomware, copias de seguridad, WiFi, IoT, teletrabajo, fuga de información, RGPD, plan director
NIST	Cybersecurity Framework v2 (CSF)
CIS	Center for Internet Security — Benchmark Windows 11 Enterprise v4.0.0
Apple	Apple Platform Security Guide

0.22. Cobertura y Limitaciones

Cobertura del análisis

El corpus documental analizado (70 documentos) proporciona cobertura amplia en: - Gobernanza y normativa (ENS, NIST, RGPD) - Endpoint (Windows, macOS, dispositivos móviles) - Red y perímetro (HTTPS, DDoS, WiFi) - Correo electrónico (DMARC, SPF, DKIM) - Respuesta a incidentes y ransomware - Nube y virtualización

Confidencial

Áreas recomendadas para ampliación futura

- SIEM/SOC: guías específicas de monitorización y detección.
- Zero Trust: documentación de arquitecturas Zero Trust.
- OT/ICS: si existen entornos industriales, guías ICS/SCADA.
- Pentesting: metodologías PTES/OSSTMM para test de intrusión.

Confidencial

1. Anexo de Evidencia y Trazabilidad

1.1. Propósito

Este anexo documenta las fuentes consultadas para la elaboración del Plan de Seguridad, proporcionando trazabilidad completa para fines de auditoría interna.

1.2. Corpus Documental

- **Total de documentos analizados:** 70
- **Total de fragmentos indexados:** 8.580
- **Fragmentos utilizados como evidencia:** 249
- **Documentos consultados directamente:** 59

1.3. Fuentes por Dominio

Gobernanza y Gestión de Riesgos

- `00-gobernanza_marco_ciberseguridad.md` — pp. 1 y ss.
- `16-principios_recomendaciones_basicas.md` — pp. 4–45
- `05-ens_medidas_implantacion.md` — pp. 10 y ss.
- `15-plan_director_seguridad.md` — pp. 1 y ss.
- `09-pilar_analisis_gestion_riesgos.md` — pp. 1 y ss.

Normativa y Cumplimiento

- `00-gobernanza_marco_ciberseguridad.md` — pp. 21 y ss.
- `06-ens_declaracion_aplicabilidad.md` — pp. 1 y ss.
- `07-nist_csf_v2.md` — pp. 1 y ss.
- `08-cumplimiento_legal_incibe.md` — pp. 1 y ss.
- `17-rgpd_competitividad_2024.md` — pp. 1 y ss.

Confidencial

Identidad y Control de Acceso

- `62-desarrollo_seguro.md` — pp. 76 y ss.
- `01-glosario_ccn.md` — pp. 126 y ss.
- `27-identidad_digital_ciberseguridad.md` — pp. 1 y ss.
- `16-principios_recomendaciones_basicas.md` — pp. 4 y ss.

Endpoint y Bastionado

- `40-endpoint_seguro.md` — pp. 1–55
- `41-endpoint_seguro_anexo.md` — pp. 1–19
- `42-windows11_cis_benchmark.md` — pp. 1–1.466
- `43-macos_seguridad.md` — pp. 1–49
- `16-principios_recomendaciones_basicas.md` — pp. 45 y ss.

Red y Perímetro

- `22-ransomware_incidentes_ccn.md` — pp. 3 y ss.
- `33-proteccion_dos_cortafuegos.md` — pp. 1–21
- `32-https_seguridad.md` — pp. 1–106
- `34-cdn_recomendaciones.md` — pp. 1–37
- `35-seguridad_redes_wifi.md` — pp. 1–30

Correo Electrónico y Navegadores

- `31-correo_dmarc.md` — pp. 1–50
- `30-correo_electronico_seguridad.md` — pp. 1–48
- `38-chrome_seguridad.md` — pp. 1–32
- `37-firefox_seguridad.md` — pp. 1–54
- `39-edge_seguridad.md` — pp. 1–40
- `36-navegadores_web_seguridad.md` — pp. 1–48

Dispositivos Móviles

- `48-mdm_gestion_dispositivos.md` — pp. 9–97
- `44-dispositivos_moviles_seguridad.md` — pp. 1–48
- `45-android_seguridad.md` — pp. 1–162
- `49-ios18_empleo_seguro.md` — pp. 1–38
- `50-apple_platform_security.md` — pp. 1–262

Confidencial

- `51-apple_servicios_seguridad.md` — pp. 1–123

Nube y Virtualización

- `53-nube_proteccion_dato_soberania.md` — pp. 4–71
- `52-virtualizacion_buenas_practicas.md` — pp. 1–63
- `68-kubernetes_seguridad.md` — pp. 1–43
- `57-copias_seguridad.md` — pp. 1–32
- `55-almacenamiento_nube.md` — pp. 1–7

Desarrollo Seguro

- `62-desarrollo_seguro.md` — pp. 1–96
- `63-drupal_seguridad.md` — pp. 1–78
- `64-bbdd_db2_seguridad.md` — pp. 1–35
- `65-bbdd_seguridad_general.md` — pp. 1–34

Respuesta a Incidentes y Continuidad

- `18-gestion_cibercrisis.md` — pp. 1–48
- `19-cibercrisis_entidades_locales.md` — pp. 1–92
- `20-gestion_crisis_incibe.md` — pp. 1–51
- `21-ransomware_ccn.md` — pp. 1–46
- `22-ransomware_incidentes_ccn.md` — pp. 1–37
- `23-ransomware_incibe.md` — pp. 1–34
- `24-fuga_informacion.md` — pp. 1–20
- `11-pilar_impacto_continuidad.md` — pp. 1 y ss.

Concienciación, IoT y Amenazas Emergentes

- `69-concienciacion_formacion.md` — pp. 1–7
- `58-iot_seguridad.md` — pp. 1–28
- `59-iot_ccn.md` — pp. 1–49
- `61-cryptojacking.md` — pp. 1–32
- `28-inteligencia_artificial_ccn.md` — pp. 1–107
- `26-desinformacion_ciberespacio.md` — pp. 1–51
- `60-redes_sociales.md` — pp. 1–62

Confidencial

Teletrabajo

- `66-teletrabajo_ccn.md` — pp. 1–84
- `67-teletrabajo_incibe.md` — pp. 1–44

1.4. Método de Recuperación

Las evidencias se extrajeron mediante búsqueda híbrida (FAISS vectorial + BM25 léxico) con fusión RRF sobre un índice de 8.580 chunks generados por el pipeline RAG del proyecto.

Confidencial