LOGO {CLIENTE}

Plan de Seguridad Informática Integral

Diseño, implementación y auditoría del sistema de seguridad de la información para {CLIENTE}

CLIENTE
{CLIENTE}

VERSIÓN
{VERSIÓN}

FECHA
2026-02-20

CLASIFICACIÓN
{CONFIDENCIALIDAD}

AUTOR
{AUTOR}

FUENTES
59 documentos / 8.580 fragmentos

Control de Cambios

VERSIÓN	FECHA	AUTOR	DESCRIPCIÓN
1.0	2026-02-20	{AUTOR}	Versión inicial — generada desde corpus RAG (70 PDFs, 8.580 chunks)

Índice

1. Resumen Ejecutivo

Este plan define un marco integral de seguridad informática para empresas, estructurado en **12 dominios** y un **plan de implementación por fases** (0–30, 30–90, 90–180 días). Se basa exclusivamente en documentación de referencia del **CCN-CERT**, **CCN-STIC**, **INCIBE**, **NIST CSF** y **CIS Benchmarks**.

Alcance

- Gobernanza y gestión de riesgos
- Normativa y cumplimiento (ENS, RGPD, NIST)
- Identidad y control de acceso
- Endpoint y hardening
- Red y perímetro
- Correo electrónico y navegadores
- Dispositivos móviles
- Nube y virtualización
- Desarrollo seguro
- Respuesta a incidentes
- Concienciación y IoT
- Monitorización de amenazas

---

2. Gobernanza y Gestión de Riesgos

2.1 Marco de Gobernanza

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

- **Oficina de Seguridad:** Se debe considerar el establecimiento de una oficina de seguridad que asista en la implantación de las políticas, procedimientos y normativa que sienten las bases de la protección de los activos de la organización.
- **Roles y responsabilidades:** Designar formalmente al Responsable de Seguridad, Responsable del Sistema y Responsable de la Información según el ENS.

- **Normativa interna:** Desarrollar políticas que definan la posición del organismo en aspectos concretos y sirvan para indicar cómo se debe actuar en caso de que una cierta circunstancia no esté recogida explícitamente.
- **Capacitación:** Plan de formación y concienciación continuo para todo el personal.

2.2 Análisis de Riesgos

- Utilizar la metodología **PILAR** para análisis y gestión de riesgos, incluyendo análisis de impacto y continuidad de operaciones.
- Determinar la **superficie de exposición** y realizar inventario de activos y servicios.
- Recopilar métricas que permitan evaluar el desempeño de la gestión de la seguridad.

2.3 Plan Director de Seguridad

Elaborar un Plan Director que establezca los objetivos, el alcance, las fases de implementación y los indicadores de seguimiento.

Fuentes: * `00-gobernanza_marco_ciberseguridad.md` — pp. `1-n/d` * `16-principios_recomendaciones_basicas.md` — pp. `4-45` * `05-ens_medidas_implantacion.md` — pp. `10-n/d` * `15-plan_director_seguridad.md` — pp. `1-n/d` * `09-pilar_analisis_gestion_riesgos.md` — pp. `1-n/d`

---

3. Normativa y Cumplimiento

3.1 Esquema Nacional de Seguridad (ENS)

El proceso de adecuación al ENS deberá contemplar las siguientes fases:

1. **Identificación de servicios e información** que deben formar parte del alcance.
2. **Categorización del sistema** según los criterios de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
3. **Elaboración de la Declaración de Aplicabilidad (DdA)** con los controles exigidos según la categoría.
4. **Implementación de medidas** de seguridad organizativas, operacionales y de protección.
5. **Auditoría y certificación** periódica.

3.2 RGPD / Protección de Datos

- Realizar evaluaciones de impacto en la protección de datos (EIPD).

- Designar Delegado de Protección de Datos cuando sea obligatorio.
- Implementar medidas técnicas y organizativas para garantizar confidencialidad, integridad, disponibilidad y resiliencia.
- Mantener registros de actividades de tratamiento.

3.3 NIST Cybersecurity Framework

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

Fuentes: * `00-gobernanza_marco_ciberseguridad.md` — pp. `21-n/d` * `06-ens_declaracion_aplicabilidad.md` — pp. `1-n/d` * `07-nist_csf_v2.md` — pp. `1-n/d` * `08-cumplimiento_legal_incibe.md` — pp. `1-n/d` * `17-rgpd_competitividad_2024.md` — pp. `1-n/d`

---

4. Identidad y Control de Acceso (IAM)

4.1 Autenticación

- **MFA obligatorio:** Utilizar autenticación multi-factor para impedir accesos no autorizados. Es la principal área de control de seguridad, por lo que el tipo y método de autenticación debe formar parte del diseño desde el inicio.
- **Tipos de MFA soportados:** autenticación basada en tokens (físicos o digitales), biometría, certificados electrónicos, tarjetas inteligentes.
- **Bloqueo de cuentas:** Implementar el bloqueo de la cuenta después de 3 intentos fallidos de contraseña.

4.2 Gestión de Credenciales

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

4.3 Principio de Privilegio Mínimo

- Asignar permisos según la necesidad de saber (need-to-know).
- Revisiones periódicas de permisos y accesos.
- Segmentación de roles administrativos.

Fuentes: * `62-desarrollo_seguro.md` — pp. `76-n/d` * `01-glosario_ccn.md` — pp. `126-n/d` * `27-identidad_digital_ciberseguridad.md` — pp. `1-n/d` * `16-principios_recomendaciones_basicas.md` — pp. `4-n/d`

---

5. Endpoint y Hardening

5.1 Configuración Segura de Endpoints

- Aplicar baselines de hardening según el tipo de sistema operativo.
- Todas las comunicaciones deben estar protegidas con canales cifrados.
- Implementar arquitectura de endpoint seguro con control de dispositivos USB, cifrado de disco y protección anti-malware.

5.2 Windows

- Aplicar el **CIS Benchmark para Windows 11** Enterprise v4.0.0 (1466 controles documentados).
- Configurar políticas de grupo (GPO) para: auditoría, control de cuentas, cifrado BitLocker, Windows Defender, firewall, restricción de software.

5.3 macOS

- Aplicar las recomendaciones de seguridad de CCN-CERT para macOS.
- Configurar FileVault, Gatekeeper, firewall integrado, System Integrity Protection.
- Gestionar actualizaciones centralizadamente.

5.4 Gestión de Configuración

La implementación efectiva de control de configuración y gestión de software es fundamental. Todos los archivos ejecutables y plantillas de documentos compartidos deben estar colocados en un directorio de solo lectura.

Fuentes: * `40-endpoint_seguro.md` — pp. `1-55` * `41-endpoint_seguro_anexo.md` — pp. `1-19` * `42-windows11_cis_benchmark.md` — pp. `1-1466` * `43-macos_seguridad.md` — pp. `1-49` * `16-principios_recomendaciones_basicas.md` — pp. `45-n/d`

---

6. Red y Perímetro

6.1 Cortafuegos y Segmentación

- A nivel de red es necesario establecer políticas que permitan controlar granularmente las conexiones permitidas.
- Seguir una aproximación de **whitelisting**, habilitando únicamente las conectividades estrictamente necesarias.
- Implementar segmentación de red por zonas de seguridad (DMZ, LAN interna, gestión).

6.2 HTTPS / TLS

- Forzar uso de HTTPS en todos los servicios web internos y externos.
- Configurar TLS 1.2 como mínimo, preferiblemente TLS 1.3.
- Gestionar certificados digitales de forma centralizada.

6.3 Protección DDoS

- Implementar medidas de protección contra denegación de servicio en cortafuegos.
- Considerar el uso de CDN con capacidades anti-DDoS.

6.4 WiFi

- Utilizar WPA3 o, como mínimo, WPA2-Enterprise con RADIUS.
- Seguir las indicaciones de la guía CCN-STIC-816 Seguridad en Redes Inalámbricas.
- Separar redes WiFi corporativas de invitados.

Fuentes: * `22-ransomware_incidentes_ccn.md` — pp. `3-n/d` * `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`

---

7. Correo Electrónico y Navegadores

7.1 Seguridad del Correo

- **Implementar SPF, DKIM y DMARC** en todos los dominios:
- SPF alineado: verificar que el correo cumple con la verificación del dominio remitente.

- DKIM: configurar firma digital de correos salientes.
- DMARC: es lo mínimo necesario para proteger contra spoofing; configurar política `p=reject` como objetivo.
- Es responsabilidad del administrador del dominio hacer los ajustes necesarios para el correcto funcionamiento de DMARC.
- Utilizar cifrado GPG/PGP para comunicaciones sensibles.

7.2 Navegadores Web

- Aplicar configuraciones de seguridad específicas para **Chrome**, **Firefox** y **Edge** según guías CCN-CERT.
- Deshabilitar plugins innecesarios, forzar actualizaciones automáticas.
- Configurar políticas de navegación segura y lista blanca de extensiones.

Fuentes: * `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`

---

8. Dispositivos Móviles

8.1 Gestión MDM

- Implementar una solución de **MDM (Mobile Device Management)** para gestión centralizada de dispositivos.
- Definir modelo de gestión con valores recomendados de configuración.
- Evaluar las características de las soluciones MDM, teniendo en cuenta que algunas solo aplican a ciertas plataformas.

8.2 Políticas por Plataforma

- **Android:** Aplicar las 162+ configuraciones de seguridad documentadas.
- **iOS/iPad:** Seguir las guías CCN-STIC para empleo seguro de iOS 18 y servicios Apple.
- **BYOD:** Establecer políticas claras de uso de dispositivos personales, separación de datos corporativos y personales.

8.3 Apple Platform Security

- Aprovechar las capacidades de seguridad nativas: Secure Enclave, cifrado de datos en reposo, sandboxing de aplicaciones.
- Configurar restricciones de instalación de aplicaciones y control de funcionalidades.

Fuentes: * `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` * `51-apple_servicios_seguridad.md` — pp. `1-123`

---

9. Nube y Virtualización

9.1 Protección del Dato en la Nube

- Las medidas de seguridad deben haberse tomado con anterioridad al incidente, porque una vez este ocurre hay poco margen de maniobra.
- Firmar **Acuerdos de Nivel de Servicio (ANS)** con el proveedor que garanticen disponibilidad, integridad, confidencialidad y trazabilidad.
- La solución de **Soberanía Digital** debe ser modular y escalable.
- Cuando se requiera cumplir con ENS, verificar que el proveedor cloud dispone de la certificación correspondiente.

9.2 Virtualización

- Aplicar las buenas prácticas de seguridad en entornos virtualizados.
- Aislar hipervisores y redes de gestión.
- Cifrar comunicaciones entre nodos virtuales.

9.3 Kubernetes

- Aplicar las recomendaciones de seguridad de CCN-CERT para Kubernetes.
- Configurar RBAC, network policies, pod security standards.
- Implementar escaneo de imágenes de contenedores.

9.4 Copias de Seguridad

- Implementar regla **3-2-1**: 3 copias, 2 medios distintos, 1 fuera de las instalaciones.

- Se necesita un ancho de banda de subida elevado para garantizar el envío de las copias a la nube en tiempo adecuado.
- Verificar periódicamente la integridad y restaurabilidad de las copias.

Fuentes: * `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`

---

10. Desarrollo Seguro (SSDLC)

10.1 Principios

- Garantizar que los datos quedan protegidos por mecanismos de autorización entre entornos mediante segmentación de red.
- Utilizar únicamente los medios externos autorizados.
- Todos los archivos que contengan información sensible deberán ser destruidos mediante **borrado seguro**.

10.2 Controles por Fases

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

10.3 Seguridad en CMS y BBDD

- **Drupal:** Aplicar las 78 recomendaciones de la guía CCN-STIC.
- **Bases de datos:** Aplicar hardening de BBDD (DB2 y general), restringir accesos administrativos, cifrar datos sensibles.

Fuentes: * `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`

11. Respuesta a Incidentes y Continuidad

11.1 Gestión de Cibercrisis

- Establecer un **procedimiento de gestión de cibercrisis** con roles, canales de comunicación y escalado.
- Realizar ejercicios periódicos de simulación.
- Tener preparada la organización con trabajo previo antes de que surja un incidente.

11.2 Ransomware

- **Prevención:** Segmentación de red, copias de seguridad offline, MFA, parcheo continuo.
- **Detección:** Monitorización de comportamientos anómalos, EDR/XDR.
- **Respuesta:** Aislar equipos afectados, preservar evidencias, gestionar comunicación de crisis.
- **Recuperación:** Restaurar desde copias limpias, verificar integridad antes de reconectar.

11.3 Continuidad de Negocio

- Elaborar **BCP/DRP** con RTOs y RPOs definidos para cada servicio crítico.
- Utilizar herramientas como **PILAR** para análisis de impacto y continuidad de operaciones.
- Realizar pruebas de recuperación al menos anualmente.

11.4 Fuga de Información

- Implementar herramientas DLP (Data Loss Prevention).
- Clasificar la información por niveles de sensibilidad.
- Las medidas de seguridad deben haberse tomado con anterioridad al incidente.

Fuentes: * `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-n/d`

12. Concienciación, IoT y Amenazas Emergentes

12.1 Formación y Concienciación

- Implementar programa de concienciación continuo para todos los niveles.
- Simulaciones de phishing periódicas.
- Formación específica para perfiles técnicos y directivos.

12.2 IoT

- Inventariar todos los dispositivos IoT conectados a la red.
- Segmentar la red IoT de la red corporativa.
- Aplicar políticas de actualización de firmware y contraseñas por defecto.

12.3 Amenazas Emergentes

- **Cryptojacking:** Monitorizar consumo anómalo de CPU/GPU, bloquear scripts de minería en navegadores.
- **IA en ciberseguridad:** Evaluar capacidades de detección basada en machine learning dentro del marco corporativo.
- **Desinformación:** Preparar protocolos de respuesta ante campañas de desinformación que puedan afectar a la organización.

Fuentes: * `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`

---

13. Teletrabajo

13.1 Recomendaciones

- Implementar conexiones VPN con autenticación fuerte (MFA).
- Aplicar políticas de seguridad específicas para equipos remotos.
- Cifrar discos completos de portátiles corporativos.
- Gestionar sesiones remotas con timeout y bloqueo automático.
- Separar entornos personales y corporativos en equipos de teletrabajo.

Fuentes: * `66-teletrabajo_ccn.md` — pp. `1-84` * `67-teletrabajo_incibe.md` — pp. `1-44`

---

14. Plan 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
Hardening básico de endpoints (antivirus, firewall, cifrado)	Endpoint	ALTA
Programa de concienciación básico	Personas	ALTA

Fase 1 — Hardening 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 móviles	Móviles	ALTA
Hardening de navegadores (Chrome/Firefox/Edge)	Navegadores	MEDIA
Configurar whitelisting de red en cortafuegos	Red	ALTA
Hardening 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
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

15. Checklist de Auditoría (Evidencias a Solicitar)

CONTROL	EVIDENCIA REQUERIDA
MFA activo	Captura de configuración de MFA en sistemas críticos
Copias de seguridad	Logs de ejecución de backups + prueba de restauración
Antivirus/EDR	Dashboard de estado de protección en endpoints
Cortafuegos	Reglas de firewall exportadas + changelog

CONTROL	EVIDENCIA REQUERIDA
SPF/DKIM/DMARC	Registros DNS del dominio + informes DMARC
Hardening Windows	Resultado de escaneo CIS-CAT o equivalente
MDM	Lista de dispositivos gestionados + políticas activas
Cifrado de disco	Estado de BitLocker/FileVault en inventario
Formación	Registro de asistencia + resultados de simulación phishing
Incidentes	Registro de incidentes + tiempos de respuesta
Actualizaciones	Informe de vulnerabilidades pendientes de parchear
Privilegios	Listado de usuarios con permisos administrativos

---

16. Limitaciones y Recomendaciones

Cobertura del corpus actual

El corpus indexado (70 documentos) cubre ampliamente los dominios de: - ✔ Gobernanza y normativa (ENS, NIST, RGPD) - ✔ Endpoint (Windows, macOS, móviles) - ✔ Red y perímetro (HTTPS, DDoS, WiFi) - ✔ Correo electrónico (DMARC, SPF, DKIM) - ✔ Respuesta a incidentes y ransomware - ✔ Nube y virtualización

Áreas que se beneficiarían de documentación adicional

- ⚠ SIEM/SOC: Se recomienda añadir guías específicas de monitorización y detección.
- ⚠ Zero Trust: Documentación de arquitecturas Zero Trust para complementar la segmentación.
- ⚠ OT/ICS: Si la empresa tiene entornos industriales, añadir guías ICS/SCADA.
- ⚠ Pruebas de penetración: Metodologías PTES/OSSTMM para test de intrusión.

Fuentes totales consultadas: 59 documentos del corpus **Fragmentos analizados:** 249 evidencias de 8.580 chunks indexados **Generado sin LLM externo:** evidencia recuperada por búsqueda híbrida FAISS+BM25