

GESTIÓN DE LA INFORMACIÓN

UD 4: SEGURIDAD Y PRIVACIDAD (Parte II)



2º Grado Gestión y Administración Pública
Prof. Ignacio Díaz Cano



**4.4 Políticas de
seguridad en la
Administración
Pública**



**4.5 Continuidad
del servicio y
gestión de
incidentes**



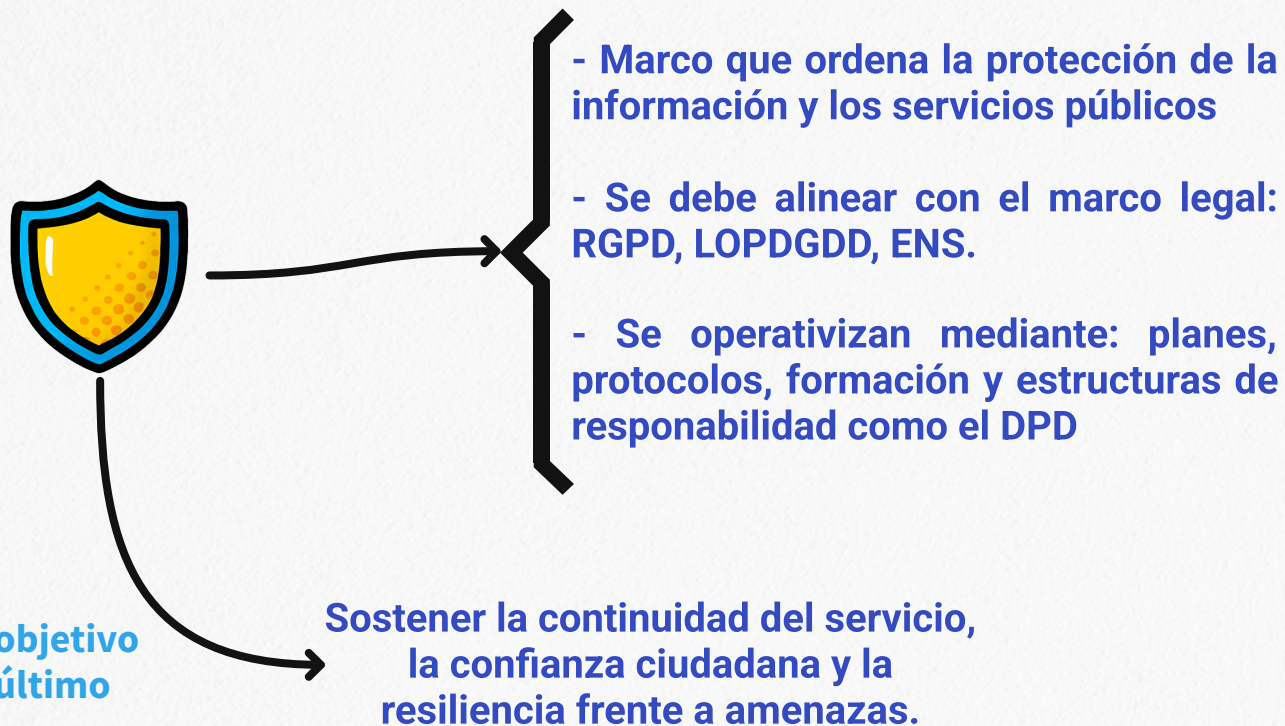
**4.6 Ciberseguridad
en servicios en la
nube y entornos
móviles**



**A4. Cuestionario
repaso. Parte II**



4.4 Políticas de seguridad en la Administración Pública



4.4.1 PLANES INTERNOS DE SEGURIDAD, PROTOCOLOS DE ACTUACIÓN, FORMACIÓN Y LA FIGURA DEL CISO



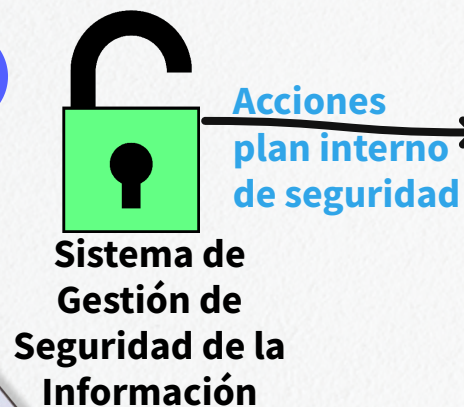
4.4.2 ORGANISMOS CLAVE EN ESPAÑA EN LA CIBERSEGURIDAD



4.4.3 MADUREZ, MÉTRICAS Y MEJORA CONTINUA

4.4.1 Planes internos de seguridad, protocolos de actuación, formación y la figura del CISO

Planes internos de seguridad (SGSI y planificación)





- Define el alcance (servicios, unidades, sistemas).
- Establece la política marco de seguridad aprobada por la alta dirección (principios, roles, cumplimiento ENS)
- Despliega políticas y normas específicas (clasificación, control de accesos, copias, cifrado, continuidad, registro y monitorización, desarrollo seguro, cloud, móviles, teletrabajo).
- Opera un ciclo PDCA (Plan-Do-Check-Act) con métricas y auditorías periódicas.
- Integra la gestión de riesgos (identificación, análisis, tratamiento y aceptación del riesgo) y la continuidad de negocio



4.4.1 Planes internos de seguridad, protocolos de actuación, formación y la figura del CISO

Protocolos de actuación (procedimientos operativos)

- Gestión de incidentes (detección → análisis → contención → erradicación → recuperación → aprendizaje). *Playbooks*(manuales) específicos: P.e. ransomware, fuga de datos, compromiso de credenciales, indisponibilidad de sede electrónica, etc.
- Gestión de vulnerabilidades y parches (inventario, escaneo periódico, priorización, ventana de mantenimiento, verificación post-parche).
- Gestión de cambios (evaluación de impacto, autorización, rollback plan).
- Copias de seguridad (3-2-1, copias offline/inmutables, pruebas de restauración).
- Alta, modificación y baja de usuarios (uniones, cambios de puesto, cese).
- Relación con terceros (onboarding, requisitos ENS, SLA de seguridad, auditorías, offboarding).
- Notificación de brechas (circuitos internos, valoración de impacto, coordinación con DPD y en su caso a la autoridad competente).



Protocolos
que traducen la
política a
acciones

4.4.1 Planes internos de seguridad, protocolos de actuación, formación y la figura del CISO

Formación y concienciación de empleados públicos

Formación de
reciclaje y
concienciación

- Módulos base (política marco, manejo de información, phishing, contraseñas, movilidad y teletrabajo).
- Formación por roles (técnicos TI, gestores de expedientes, atención ciudadana, responsables de área, directivos).
- Simulaciones de phishing, campañas temáticas y otros riesgos.
- Evaluación (tests, métricas de mejora) y certificación interna.

La información
es un factor
muy importante
en las AA.PP.



4.4.1 Planes internos de seguridad, protocolos de actuación, formación y la figura del CISO

La figura del CISO en organismos públicos

Características

- Funciones: gobernanza del SGSI, gestión de riesgos, coordinación de incidentes, interlocución con CCN-CERT e Instituto Nacional de Ciberseguridad (INCIBE) (según ámbito), supervisión de continuidad, reporte a dirección.
- Relaciones: coordinación con DPD, comunicaciones institucionales, asesoría jurídica, responsables de negocio y proveedores.
- Independencia y capacidad de reportar: debe disponer de autoridad suficiente y acceso directo a alta dirección/comités (evitar conflictos de interés).
- Estructura de soporte: Security Operations Center (SOC) o Centro de Operaciones de Seguridad interno o externalizado, gestores de vulnerabilidades, arquitectura y cumplimiento ENS, riesgos y continuidad.

Director de Seguridad (CISO), máxima autoridad

4.4.2 Organismos clave en España en la Ciberseguridad

CCN-CERT

Dependiente de



**Centro
Criptológico
Nacional (CCN)**

- Es el equipo de respuesta y el órgano de referencia para la ciberseguridad del sector público en España y para empresas que prestan servicios a éste.

- Prevención, detección y respuesta frente a ciberamenazas que afecten a sistemas del sector público.

- Normativa y guías CCN-STIC que operativizan el ENS (medidas técnicas y organizativas, valoración de sistemas, auditoría, buenas prácticas).

- Alerta temprana y coordinación de incidentes, intercambio de inteligencia de amenazas y campañas.

- Formación y ejercicios especializados para administraciones.

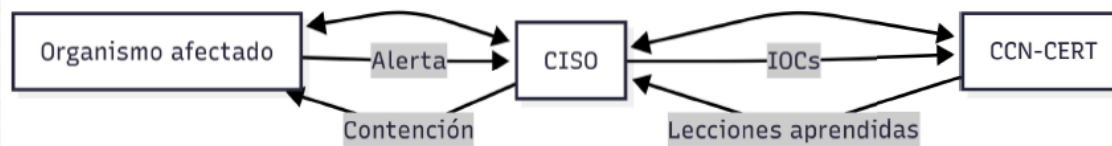


Figura 4.4: Flujo de coordinación de incidentes

4.4.2 Organismos clave en España en la Ciberseguridad

INCIBE



Instituto
Nacional de
Ciberseguridad



- Es el referente nacional para ciudadanía, empresas y ecosistema económico.

- INCIBE-CERT presta servicios de prevención y respuesta a incidentes a operadores privados y sectores económicos

- Línea 017 gratuita, de ayuda y asesoramiento.

- Programas de concienciación y recursos didácticos para ciudadanía, pymes y menores.

- Soporte a empresas: (guías, herramientas, ejercicios, apoyo a la industria y talento).

- Complementariedad: CCN-CERT / INCIBE-CERT

- CCN-CERT: foco en Administraciones Públicas (y empresas que les prestan servicios en el marco del ENS).

INCIBE-CERT: foco en tejido empresarial y ciudadanía.

Ambos coordinan la respuesta nacional y comparten inteligencia y buenas prácticas.



4.4.3 MADUREZ, MÉTRICAS
Y MEJORA CONTINUA

4.4.2 Madurez, métricas y mejora continua

Integrar políticas y organismos de referencia

se traduce en planes concretos y medibles

- Modelo de madurez (inicial → gestionado → definido → medido → optimizado) con autoevaluación anual.
- Cuadro de mando: KPIs de 4.4.1.B + indicadores de formación (% plantilla formada, tasa de clic en phishing simulado), ENS (% medidas implantadas por categoría), auditoría (no conformidades resueltas).
- Lecciones aprendidas de incidentes y ejercicios — incorporación a políticas.
- Revisión del SGSI por la dirección con prioridades y presupuesto.

-Gobernanza → 4/5 → Nivel alto de madurez, existe estructura y supervisión sólida.

Técnica → 3/5 → Madurez intermedia, con margen para mejorar en herramientas, procesos técnicos o automatización.

Respuesta → 5/5 → Dominio más fuerte: excelente capacidad de reacción ante incidentes.

Continuidad → 2/5 → Punto débil: planes de continuidad y resiliencia aún poco desarrollados o sin pruebas suficientes.

Terceros → 3/5 → Gestión aceptable de proveedores y riesgos externos, pero no robusta.

Formación → 4/5 → Alto nivel en concienciación y capacitación del personal, aunque todavía se puede afinar.

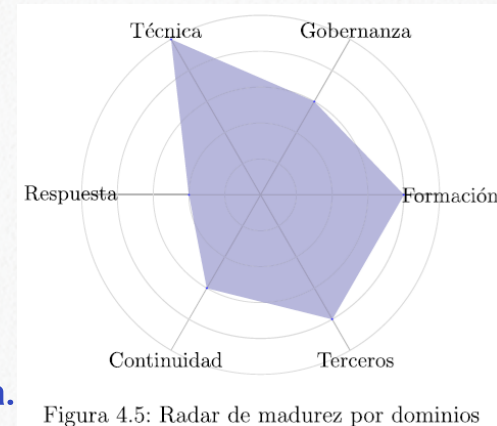


Figura 4.5: Radar de madurez por dominios

4.5 Continuidad del servicio y gestión de incidentes



- La *continuidad* se ocupa de garantizar que los servicios esenciales permanezcan disponibles ante fallos o desastres
- La *gestión de incidentes* cubre la detección, respuesta y recuperación tras eventos de seguridad (ciberataques, fallos masivos, desastres naturales)
- Ambos ámbitos deben integrarse en el SGSI y enlazarse con el ENS y los marcos internacionales



4.5.1 Importancia de planes de contingencia, copias de seguridad y DRP

Concepto y alcance

- Copias de seguridad (backups):
 - + Mecanismos para preservar datos e imágenes de sistema que permitan la recuperación.
 - + La estrategia de backups define retención, periodicidad, tipos (completo / incremental / diferencial), ubicación (on-prem / off-site / cloud) y medidas de protección (cifrado, inmutabilidad).
- Business Continuity Plan (BCP) o Plan de contingencia:
 - + Conjunto de procedimientos organizados para mantener o restablecer las funciones críticas ante una interrupción.
 - + Incluye análisis de impacto al negocio (BIA), identificación de funciones críticas, prioridades de recuperación y planes operativos.
- Disaster Recovery Plan (DRP) o Plan de Recuperación ante Desastres:
 - + Subplan técnico focalizado en la recuperación de infraestructuras y sistemas (servidores, bases de datos, comunicaciones) tras un desastre.
 - + Normalmente define procesos de *failover*, recuperación desde copias y roles técnicos.

4.5.1 Importancia de planes de contingencia, copias de seguridad y DRP

Principios y buenas prácticas

- 3-2-1: tener al menos 3 copias de los datos, en 2 medios distintos, con 1 copia off-site.
- Backups inmutables (WORM/air-gapped): para mitigar ransomware que cifra o borra copias.
- Versionado y pruebas periódicas de restauración: una copia no probada no es una copia fiable.
- Planificación por capas: aplicaciones críticas tienen DRP con replicación síncrona o asíncrona; servicios no críticos con backups diarios/semanales.
- Documentación y actualización continua: los planes deben revisarse tras cambios en arquitectura, aplicaciones o proveedores.
- Recovery Time Objective (RTO) u Objetivo de Tiempo de Recuperación y Recovery Point Objective (RPO) u Objetivo de Punto de Recuperación, deben definirse por servicio crítico tras el Business Impact Analysis (BIA) o Análisis de Impacto en el Negocio

4.5.2 Coordinación en caso de ciberataques

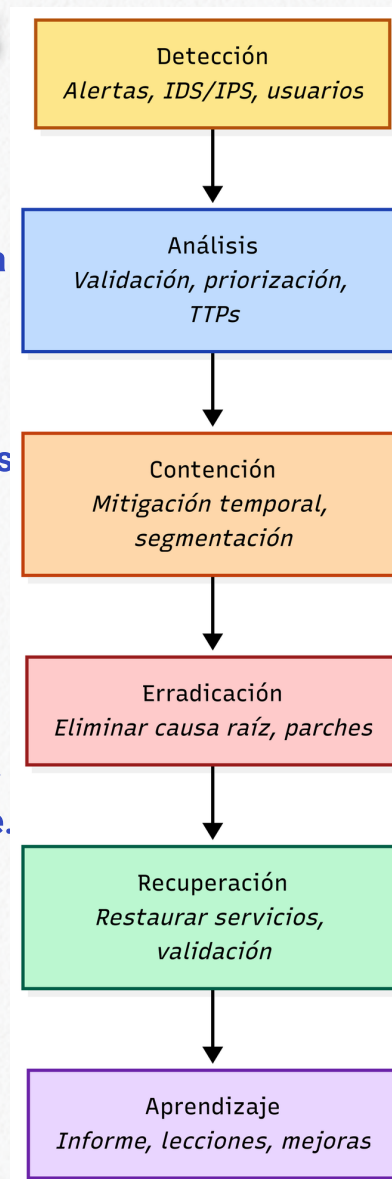
- **Detección:** alertas Sistema de Gestión de Eventos e Información de Seguridad (SIEM), Sistema de Detección de Intrusiones (IDS)/Sistema de Prevención de Intrusiones (IPS), monitoreo de tráfico anómalo, reportes de usuarios.

- **Clasificación/Contención:** determinar alcance, aislar sistemas afectados para evitar propagación (segmentación, bloqueo de cuentas comprometidas).

- **Erradicación:** eliminar causa raíz (malware, credenciales comprometidas, vulnerabilidad explotada).

- **Recuperación:** restaurar servicios desde copias seguras.

- **Lecciones aprendidas:** informe post-mortem, actualizar playbooks y políticas, comunicar resultados a dirección y a autoridades si procede.



4.5.2 Coordinación en caso de ciberataques

Roles y estructura de respuesta

- Equipo de Respuesta a Incidentes (CSIRT/SOC): responsables técnicos de detección, contención y recuperación.
- Comité de Crisis (CISO, DPD, Jurídico, Comunicación, Dirección): decisiones estratégicas, comunicación externa, coordinación legal.
- Punto de contacto con CCN-CERT / INCIBE-CERT: notificación temprana, intercambio de IOC, soporte en mitigaciones nacionales.
- Relación con proveedores/cloud: activar SLA, coordinación con subcontratas, uso de canales de emergencia.

Nivel	Descripción	Respuesta inmediata	Comunicación interna	Escalado externo
1 (Crítico)	Servicio clave caído, datos sensibles comprometidos	Inmediata (0-1 h)	Sí, Exec + prensa	Notificar CCN/INCIBE
2 (Alto)	Interferencia grave en funciones esenciales	1-4 h	Sí, equipos + dirección	Posible
3 (Medio)	Incidente operativo limitado	4-24 h	Equipos TI	No, salvo agravamiento
4 (Bajo)	Incidentes menores (p.ej. spam)	24-72 h	Registro / Seguimiento	No

Tabla 4.5: Niveles de incidentes y criterios de respuesta



4.5.3 COORDINACIÓN
INTERINSTITUCIONAL



4.5.4 COMUNICACIÓN,
ASPECTOS LEGALES Y
NOTIFICACIÓN



4.5.5 ARQUITECTURA DE
RESILIENCIA Y
CONSIDERACIONES
TÉCNICAS

4.5.3 Coordinación interinstitucional

Qué hacer



ante un incidente
de ciberseguridad

- Establecer protocolos de notificación (quién, cómo, cuándo) a CCN-CERT/INCIBE y autoridades competentes.
- Compartir conocimientos (IOCs) y participar en ejercicios conjuntos.
- Comunicación pública: disponer de planes de comunicación para prensa y ciudadanos que eviten pánico y ofrezcan instrucciones concretas.



4.5.4 COMUNICACIÓN,
ASPECTOS LEGALES Y
NOTIFICACIÓN



4.5.5 ARQUITECTURA DE
RESILIENCIA Y
CONSIDERACIONES
TÉCNICAS

4.5.4 Comunicación, aspectos legales y notificación

Aspectos
legales y



notificaciones
ante un incidente
de seguridad

- *Comunicación interna debe estar contemplada en el plan:* mensajes para empleados, instrucciones de confinamiento, prioridades de recuperación.
- *Comunicación externa:* designar portavoces, mensajes oficiales y canales alternativos para informar a la ciudadanía sin comprometer la investigación forense.
- *Notificaciones reglamentarias:* si hay afectación de datos personales, el RGPD exige notificar brechas a la autoridad de control AEPD y, cuando proceda, a los interesados; ENS y normativa sectorial pueden imponer obligaciones adicionales.
- *Preservación de evidencias:* protocolos forenses (no sobrescribir logs, conservar imágenes).



4.5.5 Arquitectura de resiliencia y consideraciones técnicas

medidas o
Arquitectura de
resiliencia

- Redundancia geográfica: replicación entre centros de datos y/o regiones cloud para tolerancia a fallos de zona/país.

- Segregación de redes: segmentación por funciones (administración, usuarios, servicios críticos) para limitar movimiento lateral.

Replicación y snapshots: uso de replicación síncrona para RTO bajos; asíncrona para eficiencia de ancho de banda.

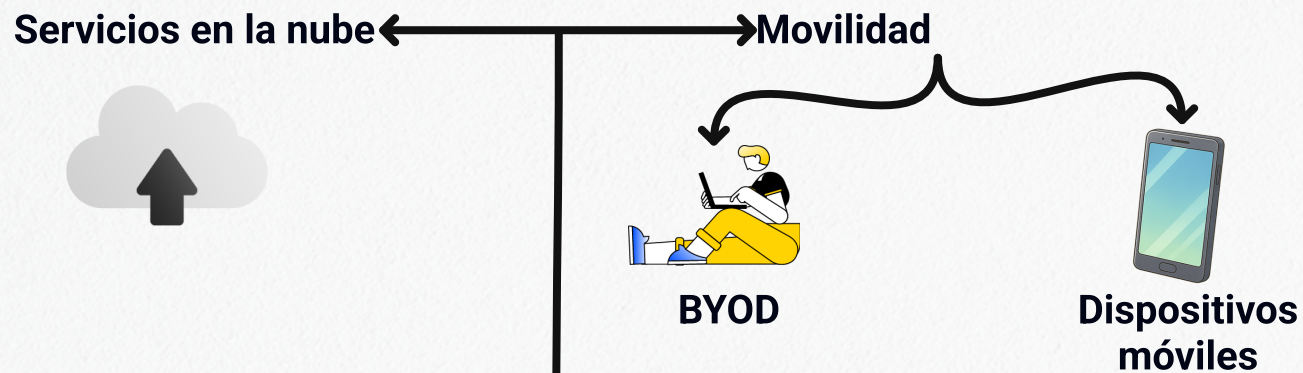
Backups inmutables y retención prolongada: protegidos contra eliminación maliciosa.

- Automatización de failover: scripts y orquestación para reducir Tiempo Medio de Recuperación (MTTR); siempre con procedimientos manuales de rollback.

- Pruebas periódicas y métricas: ejercicios programados, validación de integridad, tiempos de restauración medidos.

Un sistema
siempre
puede ser
atacado

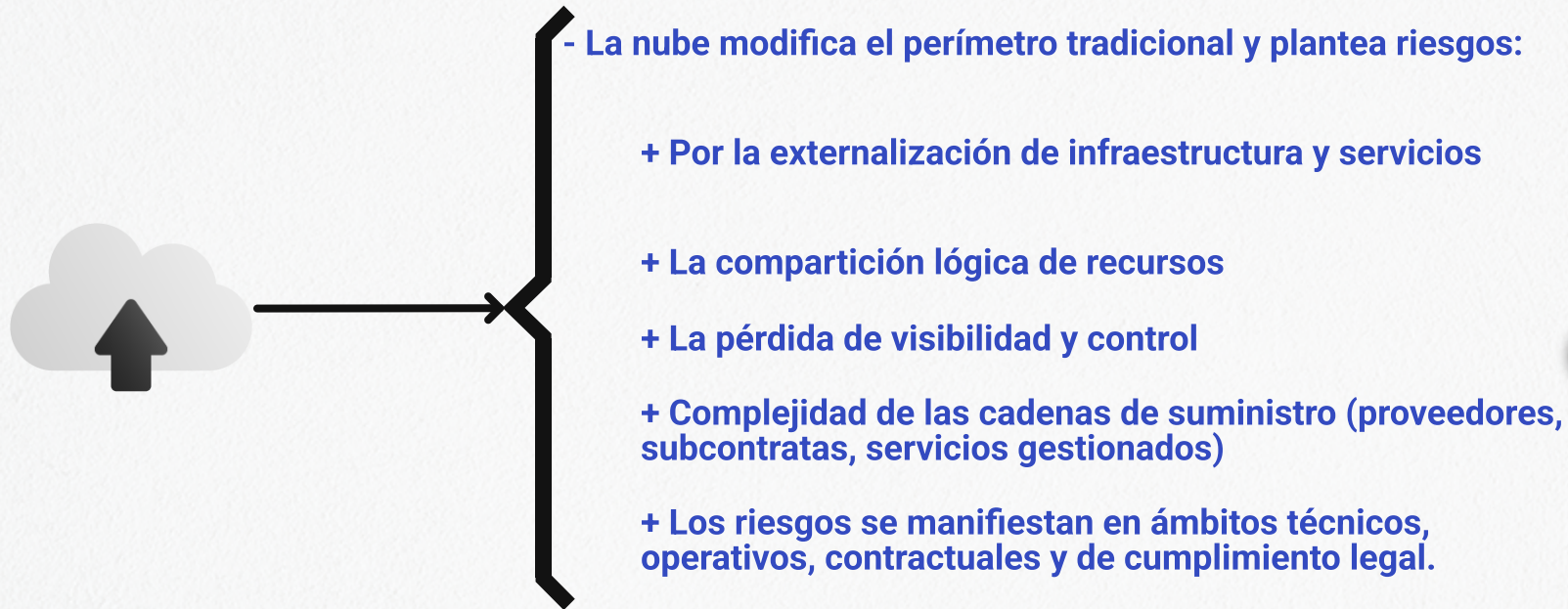
4.6 Ciberseguridad en servicios en la nube y entornos móviles



- Ha transformado la provisión de servicios públicos
- Introduce riesgos y retos específicos para la ciberseguridad de la Administración Pública.

4.6.1 Riesgos específicos de la nube

Naturaleza del riesgo



4.6.1 Riesgos específicos de la nube

Riesgos clave

1. Ubicación de datos y jurisdicción.

- + **Riesgo:** datos almacenados en centros de datos situados en jurisdicciones con normativas distintas (acceso por autoridades, transferencia internacional).
- + **Impacto:** incumplimiento de requisitos de protección de datos (p. ej. RGPD), exigencia de localización o cifrado adicional.

2. Dependencia del proveedor.

- + **Riesgo:** dificultad para migrar o recuperar datos y servicios por formatos propietarios, APIs o costos de salida.
- + **Impacto:** problemas de continuidad, coste elevado en cambio de proveedor.

3. Responsabilidad compartida.

- + **Riesgo:** confusión sobre quién es responsable de qué (proveedor vs cliente).
- + **Impacto:** lagunas en seguridad si no se definen claramente responsabilidades (p. ej. configuración de IAM, protección de datos en reposo).

4. Configuraciones erróneas y exposición pública.

- + **Riesgo:** reglas de firewall abiertas, roles con privilegios excesivos.
- + **Impacto:** exposición masiva de datos, escalada de privilegios.

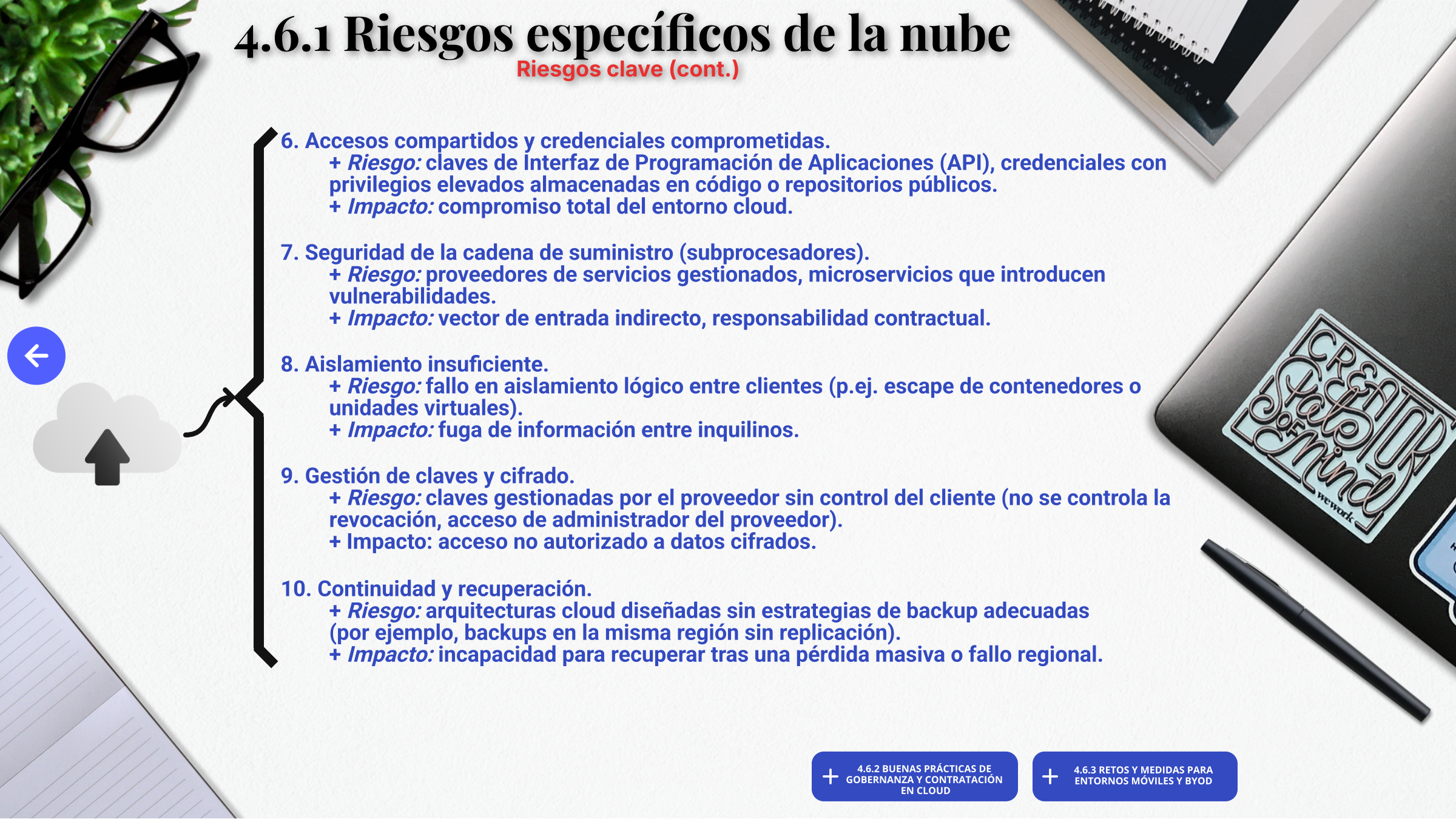



5. Falta de visibilidad y telemetría.

- + **Riesgo:** logs delegados o deshabilitados, dificultades para correlacionar eventos.
- + **Impacto:** detección tardía de incidentes y pobre respuesta forense.

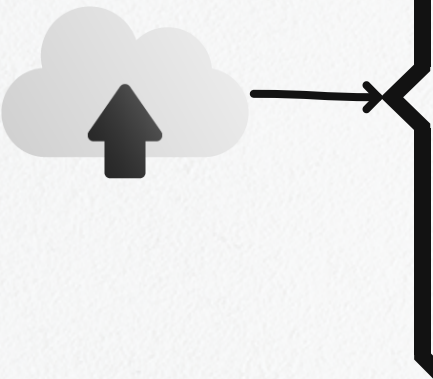


4.6.1 Riesgos específicos de la nube

Riesgos clave (cont.)

- 
- 
- 
- 
6. Accesos compartidos y credenciales comprometidas.
 - + *Riesgo*: claves de Interfaz de Programación de Aplicaciones (API), credenciales con privilegios elevados almacenadas en código o repositorios públicos.
 - + *Impacto*: compromiso total del entorno cloud.
 7. Seguridad de la cadena de suministro (subprocesadores).
 - + *Riesgo*: proveedores de servicios gestionados, microservicios que introducen vulnerabilidades.
 - + *Impacto*: vector de entrada indirecto, responsabilidad contractual.
 8. Aislamiento insuficiente.
 - + *Riesgo*: fallo en aislamiento lógico entre clientes (p.ej. escape de contenedores o unidades virtuales).
 - + *Impacto*: fuga de información entre inquilinos.
 9. Gestión de claves y cifrado.
 - + *Riesgo*: claves gestionadas por el proveedor sin control del cliente (no se controla la revocación, acceso de administrador del proveedor).
 - + *Impacto*: acceso no autorizado a datos cifrados.
 10. Continuidad y recuperación.
 - + *Riesgo*: arquitecturas cloud diseñadas sin estrategias de backup adecuadas (por ejemplo, backups en la misma región sin replicación).
 - + *Impacto*: incapacidad para recuperar tras una pérdida masiva o fallo regional.

4.6.2 Buenas prácticas de gobernanza y contratación en cloud

- 
- *Acuerdos sobre el procesamiento de datos:* incluir obligaciones de protección de datos RGPD, subprocesadores, plazos de notificación de brechas, ubicación de datos, y derechos de auditoría.
 - *SLA (Acuerdo de Nivel de Servicio de seguridad):* definir RTO/RPO, disponibilidad, créditos por incumplimiento, tiempos de respuesta ante incidentes de seguridad.
 - *Cláusulas de salida:* exportación completa de datos en formatos abiertos, procedimiento de borrado certificado, plazos y costes.
 - *Auditorías y certificaciones:* exigir ISO/IEC 27001, ISO/IEC 27701, certificaciones cloud específicas y registros de cumplimiento ENS cuando aplique.

4.6.3 Retos y medidas para entornos móviles y BYOD

1. Pérdida o robo de dispositivo.

+ **Riesgo:** acceso físico a información almacenada o sesiones abiertas.

+ **Mitigación:** cifrado del dispositivo, bloqueo remoto, borrado remoto, autenticación fuerte.

2. Dispositivos inseguros.

+ **Riesgo:** vulnerabilidades elevadas, bypass de controles de seguridad.

+ **Mitigación:** políticas de no admisión (blocklist), Mobile Threat Defense (MTD), verificación de integridad.

3. Conexiones inseguras (Wi-Fi pública).

+ **Riesgo:** ataques man-in-the-middle, interceptación de credenciales.

+ **Mitigación:** Red Privada Virtual (VPN) obligatoria para acceso a recursos sensibles, Seguridad de la Capa de Transporte (TLS) obligatorio, certificados de cliente.

4. Aplicaciones maliciosas o de terceros no controladas.

+ **Riesgo:** exfiltración de datos, keylogging, sesiones secuestradas.

+ **Mitigación:** listas blancas de apps, sandboxing o zonas de ejecución seguras.

5. Parches.

+ **Riesgo:** dispositivos con vulnerabilidades conocidas.

+ **Mitigación:** políticas de actualización forzadas, bloqueo de acceso si el Sistema Operativo está desactualizado.

4.6.3 Retos y medidas para entornos móviles y BYOD (cont.)



6. Separación de datos personal/profesional.

+ *Riesgo*: fuga de datos por uso personal (copias a nubes personales, compartir).

+ *Mitigación*: contenedorización, Prevención de Pérdida de Datos (DLP), DLP móvil, políticas BYOD claras.

7. Autenticación débil.

+ *Riesgo*: uso de PINs simples o ausencia de Autenticación MultiFactor (MFA).

+ *Mitigación*: Inicio de Sesión Único (SSO) con MFA, autenticación adaptativa

GESTIÓN DE LA INFORMACIÓN

Curso 2025/2026

UD 4: SEGURIDAD Y PRIVACIDAD (Parte II)



2º Grado Gestión y Administración Pública
Prof. Ignacio Díaz Cano



A.4 CUESTIONARIO
PARTE II



A4 Cuestionario Repaso. Parte II

1. ¿Cuál es la función principal del Sistema de Gestión de Seguridad de la Información (SGSI) en una administración pública?:

Gestionar únicamente los incidentes informáticos

Controlar los accesos físicos a los edificios

Definir, desplegar y supervisar las políticas y normas de seguridad de la información

Mantener copias de seguridad externas

Send



Índice



A4 Cuestionario Repaso. Parte II

2. ¿Qué ciclo de mejora continua aplica el SGSI para sus auditorías y métricas?:

PDCA (Plan-Do-Check-Act)

DMAIC

SCRUM

DMAIC

SWOT

Send



Índice



A4 Cuestionario Repaso. Parte II

3. ¿Cuál es el rol del CISO dentro de un organismo público?:

Gestionar el presupuesto de TI

Coordinar la gobernanza del SGSI y la respuesta ante incidentes

Supervisar únicamente el cumplimiento del RGPD

Administrar los contratos con proveedores

Send



Índice



A4 Cuestionario Repaso. Parte II

4. ¿Qué organismo español se centra en la ciberseguridad del sector público?:

Ministerio del Interior

INCIBE-CERT

AEPD

CCN-CERT

Send



Índice



A4 Cuestionario Repaso. Parte II

5. ¿Qué diferencia principal existe entre un BCP (Plan de Continuidad de Negocio) y un DRP (Plan de Recuperación ante Desastres)?:

El BCP se aplica solo a datos personales

El BCP se centra en mantener funciones críticas, mientras el DRP se enfoca en recuperar infraestructuras

El BCP es un subplan del DRP

El DRP trata aspectos legales del RGPD

Send



Índice



A4 Cuestionario Repaso. Parte II

6. Según las buenas prácticas 3-2-1, ¿cuántas copias de seguridad y en cuántos medios deben mantenerse?:

3 copias en 3 medios iguales

3 copias en 2 medios distintos, con 1 copia off-site

2 copias en 1 medio

1 copia cifrada local

Send



Índice



A4 Cuestionario Repaso. Parte II

7. ¿Qué papel desempeña el Comité de Crisis en la gestión de incidentes de ciberseguridad?:

Restaurar servidores afectados

Monitorizar el tráfico de red

Tomar decisiones estratégicas, coordinar comunicación y aspectos legales

Detectar vulnerabilidades en los sistemas

Send



Índice



A4 Cuestionario Repaso. Parte II

8. ¿Cuál de las siguientes estrategias forma parte de una arquitectura de resiliencia?:

Redundancia geográfica y backups inmutables

Reducir la frecuencia de auditorías

Desactivar logs de seguridad

Centralizar todos los servicios en un único servidor

Send



Índice



A4 Cuestionario Repaso. Parte II

9. ¿Cuál es un riesgo específico del uso de servicios en la nube?:

Dificultad para aplicar cifrado local

Incremento del almacenamiento físico

Reducción de la dependencia del proveedor

Falta de visibilidad y control debido a la externalización de infraestructura

Send



Índice



A4 Cuestionario Repaso. Parte II

10. ¿Qué medida se recomienda para mitigar los riesgos de conexiones inseguras en entornos BYOD?:

Instalar cualquier aplicación de terceros confiables

Uso obligatorio de VPN y TLS para acceso a recursos sensibles

Permitir solo contraseñas cortas

Desactivar el Wi-Fi público

Send



Índice

