sosafe

Lista de tareas para la implementación de DLP para responsables de la toma de decisiones de TI

Guía completa para implementar la data leak prevention

Resumen ejecutivo

Esta lista de tareas te guía paso a paso a la hora de implementar una estrategia eficaz de data leak prevention. Contiene:

- Pasos de implementación detallados con responsabilidades
- Plantillas para políticas de DLP y planes de respuesta a incidentes
- KPI medibles para supervisar el éxito
- Correspondencia del cumplimiento de las normativas para el RGPD, la NIS2 y la norma ISO 27001
- Criterios de evaluación de herramientas
- Procesos de revisión y auditoría

Plazo: de 3 a 6 meses para la implementación completa (en función del tamaño de la organización)

1 Fase 1: Preparación e inventario (semanas 1-4)

1.1 Gestión de las partes interesadas

- [ ] Crear el equipo del proyecto
  - Responsable: director de ciberseguridad/dirección de TI
  - Implicados obligatoriamente: seguridad de TI, departamento jurídico/cumplimiento de las normativas, RR. HH., órgano de representación de los empleados, delegado de protección de datos
  - Entregable: Carta del proyecto con presupuesto, calendario y responsabilidades
- [ ] Obtener la aprobación de los directivos
  - Presentar una evaluación de riesgos (daños potenciales en caso de fuga de datos)
  - Justificación económica: ROI mediante la evitación de multas, daño reputacional
  - Recursos necesarios: Presupuesto, FTE, consultoría externa
- [ ] Involucrar al órgano de representación de los empleados/RR. HH.
  - Preparar el acuerdo de representación de los empleados para su supervisión (cuando proceda en tu jurisdicción)
  - Definir los requisitos de transparencia
  - Planificar la información para los empleados

1.2 Inventario de datos

- [ ] Llevar a cabo la detección de datos
  - ¿Dónde se encuentran los datos sensibles? (Servidores de archivos, SharePoint, almacenamiento en la nube, endpoints)
  - ¿Qué tipos de datos? (PII, datos financieros, IP, datos sanitarios)
  - ¿Quién tiene acceso? (crear matriz de autorización)
  - Herramientas recomendadas: herramientas de detección automatizada (p. ej., Microsoft Purview, Varonis, BigID)
- [ ] Asignación del flujo de datos
  - Fuente de datos → Procesamiento → Almacenamiento → Transferencia → Archivo/eliminación
  - Identificar rutas críticas (correo electrónico, cargas a la nube, USB, impresoras)
  - Visualización: Crear un diagrama de flujo de datos
- [ ] Evaluación de riesgos por categoría de datos

Categoría de datos	Sensibilidad (1-5)	Volumen	Accesos/día	¿Compartidos externamente?	Puntuación de riesgo
Datos de clientes (PII)	5	Alto	500	Sí	Crítico
Datos financieros	5	Medio	50	Raramente	Alto
Código fuente	4	Alto	200	No	Alto
Documentos internos	2	Muy alto	2000	Sí	Medio

2 Fase 2: Política y clasificación (semanas 5-8)

2.1 Definir el esquema de clasificación de datos

☐ Definir los niveles de clasificación

Nivel	Definición	Ejemplos	Regla de acceso	Gestión
Público	Destinados al público	Comunicados de prensa, material de marketing	Sin restricciones	No se requiere cifrado
Interno	Para uso interno	Planes de proyectos, notas de reuniones	Solo para empleados	Control de acceso básico
Confidencial	Críticos para el negocio	Contratos, previsiones financieras, documentos de fusiones y adquisiciones	Necesidad de saber	Cifrado + MFA
Restringido	Altamente sensibles	Datos de personal, información de pago, historiales de pacientes, secretos comerciales	Autorización explícita	Cifrado + MFA + Registro de auditoría + Bloqueo de DLP

☐ Establecer un proceso de etiquetado

- Clasificación automática: coincidencia de patrones (números de tarjetas de crédito, IBAN, etc.)
- Clasificación manual: formación para usuarios + recordatorios en las aplicaciones de Office
- Clasificación por defecto: los nuevos archivos se clasifican como "Internos" por defecto hasta su revisión

☐ Documentar la política de clasificación

Plantilla: Directriz de clasificación de datos

1. Finalidad

Esta política define cómo se clasifican, etiquetan y protegen los datos.

2. Ámbito de aplicación

Todos los empleados, contratistas y socios con acceso a los datos de la empresa.

3. Roles

- Propietario de los datos: departamento, define la clasificación
- Custodio de los datos: TI, implementa los controles técnicos

- Usuario de los datos: cualquier empleado que acceda a los datos, cumple con los requisitos de manejo

4. Árbol de decisión de clasificación

¿Contienen los datos información personal? → SÍ → Restringido
¿Su divulgación perjudicaría a la empresa? → SÍ → Confidencial
¿Son para fines internos? → SÍ → Interno
Cualquier otro tipo → Público

5. Reclasificación

Revisión anual por parte del propietario de los datos. Si se cambia: actualizar la etiqueta.

2.2 Crear la política de DLP

☐ Redactar el documento de la política

Plantilla: Política de data leak prevention

1. Finalidad

Prevención de la divulgación no autorizada de datos sensibles de la empresa.

2. Ámbito de aplicación

Todos los sistemas, redes, dispositivos finales, servicios en la nube.

3. Acciones prohibidas

- Transferencia de datos «restringidos» o «confidenciales» a direcciones de correo electrónico privadas
- Carga de datos sensibles a servicios en la nube no autorizados
- Copia de datos sensibles a memorias USB sin cifrado
- Realización de capturas de pantalla de documentos «restringidos» sin autorización

4. Puntos de control de DLP

- Pasarela de correo electrónico (entrante/saliente)
- Proxy web (cargas a la nube)
- Agentes de endpoint (USB, portapapeles, captura de pantalla)
- Integración de API en la nube (Microsoft 365, Google Workspace, Slack)

5. Modos de aplicación

- Supervisión: Solo registro, sin bloqueo (fase piloto)
- Alerta: Advertencia para el usuario + equipo de ciberseguridad
- Bloqueo: Bloqueo automático + ticket de incidente

6. Excepciones

Excepciones solo aprobadas por el director de ciberseguridad, con un plazo limitado y documentadas.

7. Respuesta a incidentes

En caso de infracción, ticket automático → Evaluación en 4 horas → Notificación de progreso si se ven afectados datos restringidos

8. Revisión

Revisión trimestral de la política, después de cada incidente.

☐ Crear matriz de privilegios mínimos

Función	Datos de clientes	Datos financieros	Datos de RR. HH.	Código fuente	Documentos de marketing
Ventas	Leer + Editar	—	—	—	Leer
Finanzas	—	Leer + Editar	—	—	—
RR. HH.	Leer (nombres /contacto)	—	Leer + Editar	—	—
Ingeniería	—	—	—	Leer + Editar	—
Marketing	Leer (anonimizados)	—	—	—	Leer + Editar
Ejecutivos	Leer (todo)	Leer (todo)	Leer (todo)	Leer (todo)	Leer (todo)

☐ Definir el proceso de revisión de acceso

- Trimestralmente: Cada responsable revisa los derechos de acceso de su equipo.
- Cuando cambian las funciones: Revocación automática de los derechos antiguos + solicitud de nuevos derechos
- A la salida: Retirada inmediata de todos los derechos de acceso.

3 Fase 3: Evaluación y selección de herramientas (semanas 9-12)

3.1 Catálogo de requisitos

- [ ] Funcionalidades imprescindibles
  - [ ] Soporte técnico para todos los canales de datos (correo electrónico, web, endpoint, nube)
  - [ ] Inspección de contenido (coincidencia de patrones, basada en aprendizaje automático, OCR)
  - [ ] Integración con sistemas existentes (SIEM, SOAR, sistema de tickets)
  - [ ] Integración de cifrado
  - [ ] Control de políticas granular (por categoría de datos, grupo de usuarios, acción)
  - [ ] Informes de cumplimiento de las normativas (RGPD, NIS2, ISO 27001)
  - [ ] Gestión de falsos positivos (ciclo de feedback de los usuarios, ajuste del aprendizaje automático)
- [ ] Funcionalidades opcionales
  - [ ] Análisis de datos de comportamiento (UEBA)
  - [ ] Escaneo de datos en reposo (descubrimiento)
  - [ ] Clasificación automática
  - [ ] Flujos de trabajo de corrección (p. ej., cifrado automático en lugar de bloqueo)
  - [ ] Autoservicio del usuario (solicitudes de liberación)

3.2 Matriz de evaluación de proveedores

- [ ] Crear y evaluar una lista de preselección

Criterio	Ponderación	Proveedor A	Proveedor B	Proveedor C
Funcionalidad				
DLP para el correo electrónico	15 %	9/10	8/10	7/10
DLP en la nube (API)	20 %	8/10	9/10	6/10
DLP para endpoints	15 %	7/10	9/10	8/10
Aprendizaje automático/Comportamiento	10 %	9/10	7/10	5/10
Integración				

Criterio	Ponderación	Proveedor A	Proveedor B	Proveedor C
SIEM/SOAR (orquestación, automatización y respuesta de seguridad)	10 %	8/10	8/10	9/10
Herramientas tecnológicas existentes	5 %	7/10	9/10	6/10
Usabilidad				
IU de administrador	5 %	8/10	7/10	9/10
Gestión de falsos positivos	10 %	9/10	8/10	7/10
Coste				
Costes de licencia	5 %	7/10	8/10	9/10
Esfuerzo de impl.	5 %	8/10	7/10	8/10
Puntuación total	100 %	8,2	8,1	7,3

- [ ] Perform POC
    - Duración de la prueba: 4 semanas
    - Alcance de la prueba: Correo electrónico + nube + 50 endpoints de prueba
    - Criterios de éxito: <5 % de falsos positivos, <100 ms de latencia, más del 95 % de porcentaje de detección

4 Fase 4: Implementación (semanas 13-20)

4.1 Implementación técnica

- [ ] DLP para el correo electrónico
  - Ajuste del registro MX o configuración del relé SMTP
  - Reglas de política: Escaneo de salida para datos restringidos/confidenciales
  - Configurar el buzón de cuarentena
  - Flujo de trabajo de notificación de progreso: equipo de ciberseguridad + responsable en caso de bloqueo
- [ ] DLP para web/nube
  - Integración de proxy o CASB en la nube
  - Habilitar la inspección SSL (precaución: implicaciones para la protección de datos)
  - Conectores API: Microsoft 365, Google Workspace, Slack, Salesforce
  - Política: Bloquear la carga de datos restringidos a servicios en la nube no aprobados
- [ ] DLP para endpoints
  - Despliegue del agente (paso a paso: TI → grupo piloto → despliegue completo)
  - Bloqueo de USB para datos restringidos (lista de permitidos para USB cifrados)
  - Control del portapapeles, prevención de capturas de pantalla
  - Modo sin conexión: aplicación de políticas incluso sin conexión a la red
- [ ] Integración de la gestión de incidentes
  - Integración de SIEM: Alertas de DLP → correlación con otros eventos de seguridad
  - Sistema de tickets: Tickets automáticos para infracciones de alta gravedad
  - Guías de SOAR (orquestación, automatización y respuesta de seguridad): Suspensión automática de cuentas para infracciones críticas

4.2 Plan de despliegue

- [ ] Fase piloto (semanas 13-16)
  - Grupo objetivo: Departamento de informática (20-50 usuarios)
  - Modo: Solo supervisión
  - Objetivo: Establecer una línea de base, determinar el porcentaje de falsos positivos, ajustar las políticas
- [ ] Despliegue progresivo (semanas 17-20)
  - Semana 17: Finanzas (modo de alerta)

- Semana 18: RR. HH. + Departamento jurídico (modo de alerta)
- Semana 19: Ingeniería + Ventas (modo de alerta)
- Semana 20: Resto de la organización (modo de alerta)

☐ Fase de aplicación (a partir de la semana 21)

- Transición gradual al modo de bloqueo
- Comenzar con datos restringidos
- Después de 2 semanas: datos confidenciales también

5 Fase 5: Gestión del riesgo humano (paralela a la fase 4)

5.1 Campaña de concienciación

- [ ] Plan de comunicación
  - Semana 12: Anuncio por parte del CEO/director de ciberseguridad (reunión general)
  - Semanas 13-16: Grupo piloto: formación intensiva + sesiones de preguntas y respuestas
  - Semana 17-20: Comunicación del despliegue: artículo en la intranet, correo electrónico, reuniones informativas para responsables
  - A partir de la semana 21: Recordatorios continuos (newsletter mensual)
- [ ] Desarrollar módulos de formación
  1. Módulo 1: ¿Por qué DLP? (5 min)
     - Riesgos de las fugas de datos (casos de ejemplo)
     - Obligaciones legales (RGPD, NIS2)
     - Responsabilidad personal
  2. Módulo 2: Clasificación de datos (10 min)
     - Niveles y ejemplos
     - ¿Cómo clasifico correctamente?
     - Ejercicio práctico: Clasificar 5 documentos de muestra
  3. Módulo 3: ¿Qué se me permite hacer (y qué no)? (10 min)
     - Qué hacer y qué no hacer
     - ¿Qué ocurre en caso de infracción?
     - ¿Cómo solicito excepciones?
  4. Módulo 4: Phishing e ingeniería social (15 min)
     - Reconocer correos electrónicos de phishing
     - Escenarios de fraude del CEO
     - Proceso de notificación
- [ ] Simulaciones de phishing
  - Frecuencia: mensual, aleatoria
  - Rotación de plantillas: fraude del CEO, factura falsa, phishing de credenciales, adjunto con malware
  - Seguimiento: Al hacer clic → Microaprendizaje inmediato (3 min)
  - Gamificación: Tabla de clasificación (anonimizada), logros para quienes notifican

5.2 Panel de métricas del riesgo humano

☐ Definir y realizar un seguimiento de los KPI

KPI	Valor objetivo	Método de medición
Porcentaje de clics de phishing	<5 %	Herramienta de simulación de phishing
Porcentaje de aviso de phishing (correos electrónicos sospechosos)	>30 %	Análisis de datos del botón de aviso de phishing
Porcentaje de finalización de la formación	>95 %	Informes del LMS (sistema de gestión de aprendizaje)
Infracciones de DLP por cada 1000 usuarios	<10/mes	Registros del sistema DLP
Infracciones repetidas (mismo usuario)	<2 %	Análisis de datos del sistema DLP
Human Security Index	>75/100	Panel de métricas de gestión del riesgo humano

6 Fase 6: Cumplimiento de las normativas y documentación (semanas 21-24)

[LOCAL PART]

6.1 Asignación del cumplimiento de las normativas

La siguiente asignación utiliza el marco normativo de la UE (RGPD, NIS2, ISO 27001) como ejemplo práctico. Adapta los artículos, plazos y autoridades específicos al marco normativo que se aplique en tu jurisdicción. En el caso de España, deben considerarse el RGPD, la LOPDGDD, el marco español NIS/NIS2, la ISO 27001, el ENS (Esquema Nacional de Seguridad) para el sector público, y la legislación sectorial española específica. La ISO 27001 se utiliza como marco común de controles, mientras que la legislación española establece los requisitos obligatorios. El Esquema Nacional de Seguridad (ENS), establecido por el Real Decreto 311/2022, es especialmente importante para las administraciones públicas españolas y para determinadas organizaciones que prestan servicios a estas. El Centro Criptológico Nacional (CCN) publica un mapeo específico entre la ISO 27001 y el RD 311/2022 (ENS) mediante CCN-STIC 825.

☐ Cubrir los requisitos del RGPD

Artículos del RGPD	Requisito	Medida de DLP	Estado
Art. 5 (1f)	Integridad y confidencialidad	Políticas de DLP + cifrado	☐
Art. 25	Privacidad desde el diseño	Clasificación por defecto «Interno»	☐
Art. 32	Medidas técnicas	DLP + Control de acceso + Supervisión	☐
Art. 33	Obligación de notificar (72 horas)	Integración de la respuesta a incidentes	☐
Art. 35	EIPD	EIPD realizada para la supervisión de DLP	☐

☐ Cubrir los requisitos de la NIS2

Artículos de la NIS2	Requisito	Medida de DLP	Estado
Art. 21	Gestión de riesgos de ciberseguridad	DLP como parte de la estrategia de gestión de riesgos	☐

Artículos de la NIS2	Requisito	Medida de DLP	Estado
Art. 23	Obligación de notificar (notificación inicial en un plazo de 24 horas)	Alertas automáticas + notificación de progreso	☐
Art. 32	Auditoría y documentación	Registros de DLP, documentos de políticas, registros de auditoría	☐

☐ Cubrir el anexo A 8.12 de la norma ISO 27001:2022

- Data leak prevention documentada como medida de control
- Descripción del proceso: ¿Cómo previene la organización la exfiltración?
- Documentos de referencia: política de DLP, configuración de herramientas, registros, informes de incidentes

6.2 Documentación

☐ Crear documentos obligatorios

- ☐ Política de DLP (ver plantilla anterior)
- ☐ Política de clasificación de datos
- ☐ Plan de respuesta a incidentes (ver más abajo)
- ☐ Acuerdo operativo (supervisión)
- ☐ Evaluación de impacto relativa a la protección de datos (EIPD)
- ☐ Manual del administrador (sistema DLP)
- ☐ Guía del usuario (clasificación de datos, proceso de excepción)

7 Fase 7: Respuesta a incidentes (continua)

7.1 Plan de respuesta a incidentes

Plantilla: Guía de respuesta a incidentes de DLP

Fase 1: Detección (0-15 min)

- [ ] Recibir alerta de DLP (correo electrónico, SIEM, ticket)
- [ ] Clasificación de la gravedad:
  - Crítica: Datos restringidos + externo + gran volumen
  - Alta: Datos confidenciales + externo
  - Media: Datos confidenciales + interno
  - Baja: Datos internos + comportamiento inusual
- [ ] Ingeniero de guardia asignado

Fase 2: Contención (15-60 min)

- [ ] Para Crítica/Alta: Medidas inmediatas
  - Bloquear la cuenta afectada
  - Retirar el correo electrónico del buzón del destinatario (si aún es posible)
  - Desconectar la conexión de red del endpoint (si hay exfiltración activa)
- [ ] Crear una instantánea forense (registros, volcado de memoria, imagen de disco)
- [ ] Informar al jefe de incidentes (director de ciberseguridad o adjunto)

Fase 3: Evaluación (1-4 horas)

- [ ] Evaluación de los datos:
  - ¿Qué datos? (clasificación, volumen, número de personas afectadas)
  - ¿Dónde? (destinatario interno/externo, dominio, servicio en la nube)
  - ¿Cómo? (correo electrónico, USB, carga a la nube, captura de pantalla)
  - ¿Por qué? (error, ingeniería social, malicioso)
- [ ] Entrevista con el usuario (si está disponible, no en casos de sospecha de intención maliciosa)
- [ ] Evaluación legal: ¿Existe obligación de notificar según la ley de protección de datos y ciberseguridad pertinente? [PARTE LOCAL - ejemplo de la UE a continuación]
  - Art. 33 del RGPD: ¿Notificación a la Agencia Española de Protección de Datos (AEPD) en un plazo de 72 horas para una entidad privada sujeta a la jurisdicción española?
  - Art. 23 de la NIS2: ¿Informe inicial al CSIRT/autoridad en un plazo de 24 horas?

- ¿Informar a las personas afectadas? (Art. 34 del RGPD)
- En resumen, cuando se produzca una violación de la seguridad de datos personales que sea probable que constituya un riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá notificarla a la autoridad de control competente sin dilación indebida y, en todo caso, a más tardar dentro de las 72 horas desde que tenga constancia de la misma, de conformidad con el artículo 33 RGPD. En España, la autoridad competente será normalmente la AEPD, sin perjuicio de las competencias de las autoridades autonómicas de protección de datos. Esta obligación es independiente de cualquier obligación de notificación de incidentes de ciberseguridad derivada del régimen NIS/NIS2 u otra legislación sectorial aplicable.

☐ Decisión: ¿Notificación de progreso a la dirección/al departamento jurídico?

Fase 4: Notificación (dentro de los plazos legales)

☐ Informes internos: Informe de incidente al director de ciberseguridad, departamento jurídico, delegado de protección de datos

☐ Informes externos (si es necesario): [PARTE LOCAL - ejemplo de la UE a continuación]

- RGPD: Notificación a la autoridad de control competente, normalmente la AEPD (formulario)
- NIS2: Informe inicial al CSIRT/autoridad competente
- Personas afectadas: Correo electrónico/carta con detalles + recomendaciones de actuación. La comunicación a los afectados debe realizarse sin dilación indebida. La AEPD recalca que el plazo de 72 horas del art. 33 no es un plazo aplicable a la comunicación a los interesados.

☐ Documentación: Actualización del ticket de incidente (cronología, medidas, comunicación)

Fase 5: Seguimiento (en el plazo de 1 semana)

☐ Análisis de la causa raíz:

- Causa técnica (brecha en la política, falso negativo)
- Causa humana (descuido, falta de formación, intención maliciosa)

☐ Corrección:

- Ajustar la política
- Controles adicionales (p. ej., principio de dos personas para datos sensibles)
- Reciclaje de usuarios (dirigido o amplio)
- Medidas disciplinarias (si es malicioso)

☐ Lecciones aprendidas: Documentación + Presentación al equipo de ciberseguridad

☐ Actualización de políticas/guías

Fase 6: Revisión (trimestral)

☐ Revisar todos los incidentes: ¿patrones? ¿Infractores reincidentes? ¿Vulnerabilidades?

- [ ] Informes de KPI para la dirección

7.2 Matriz de notificación de progreso

Gravedad	Tiempo de respuesta	¿A quién se informa?	Medidas
Crítica	< 15 min	Director de ciberseguridad, departamento jurídico, CEO, delegado de protección de datos	Bloquear cuenta, análisis forense, comprobar informe externo
Alta	< 1 hora	Director de ciberseguridad, equipo de ciberseguridad, responsable del usuario	Bloquear temporalmente la cuenta, entrevista al usuario, revisión de la política
Media	< 4 horas	Equipo de ciberseguridad, responsable del usuario	Advertencia al usuario, reciclaje, aumento de la supervisión
Baja	< 24 horas	Equipo de ciberseguridad	Registro, en caso de recurrencia → Media

8 Fase 8: KPI e informes (continuos)

8.1 Panel de métricas de KPI de DLP

☐ Métricas técnicas

KPI	Fórmula	Objetivo	Intervalo de detección
Porcentaje de detección	(Infracciones detectadas / Todas las infracciones) × 100	>95 %	Mensual (prueba con datos ficticios)
Porcentaje de falsos positivos	(Falsos positivos / Todas las alertas) × 100	<5 %	Semanalmente
Cobertura de la política	(Canales de datos cubiertos / Todos los canales de datos) × 100	100 %	Trimestralmente
MTTR (Tiempo medio de respuesta)	Tiempo medio desde la alerta hasta la contención	<1 hora (crítica)	Por incidente
Tiempo de actividad del sistema	Disponibilidad del sistema DLP	>99,5 %	Mensualmente

☐ Métricas de cumplimiento de las normativas

KPI	Descripción	Valor objetivo	Informes
Infracciones por cada 1000 usuarios	Número de infracciones de DLP normalizadas	<10/mes	Mensualmente
Infractores reincidentes	Usuarios con >2 infracciones en 3 meses	<2 % de los usuarios	Trimestralmente
Avisos de incidentes (RGPD/NIS2)	Número de incidentes notificables	0 (objetivo)	Anualmente
Hallazgos de auditoría	Hallazgos en auditorías internas/externas	0 Crítica/Alta	Después de la auditoría
Porcentaje de cumplimiento de la política	Porcentaje de usuarios que han finalizado la formación sobre la política	>95 %	Trimestralmente

☐ Métricas de riesgo humano

KPI	Descripción	Valor objetivo	Herramienta
Human Security Index	Métrica de seguridad agregada	>75/100	Panel de métricas del riesgo humano

KPI	Descripción	Valor objetivo	Herramienta
Porcentaje de clics de phishing	% de usuarios que hacen clic en la simulación	<5 %	Herramienta de simulación de phishing
Porcentaje de aviso de phishing	% de usuarios que notifican correos electrónicos sospechosos	>30 %	Análisis de datos del botón de aviso
Finalización de la formación	% de usuarios que han finalizado la formación sobre DLP	>95 %	LMS (sistema de gestión de aprendizaje)
Puntuación de concienciación	Resultados de los cuestionarios después de la formación	>80 % de aciertos	LMS (sistema de gestión de aprendizaje)

8.2 Informes para la dirección

- [ ] Informe mensual (1 página)
  - Número de infracciones (tendencia)
  - Los 3 principales tipos de infracción
  - Incidentes de gravedad crítica/alta (detalles)
  - Porcentaje de falsos positivos
  - Elementos de acción abiertos
- [ ] Resumen ejecutivo trimestral
  - Panel de métricas de KPI (visual)
  - Estado de cumplimiento de las normativas (RGPD, NIS2, ISO 27001)
  - Cálculo del ROI (daños evitados, multas evitadas)
  - Lecciones aprendidas de los incidentes
  - Hoja de ruta para el siguiente trimestre

9 Fase 9: Mejora continua (en curso)

9.1 Ciclos de revisión

- [ ] Semanal (equipo de ciberseguridad)
  - Analizar nuevos falsos positivos y ajustar las políticas
  - Revisar las infracciones críticas
  - Rendimiento de la herramienta (tiempo de actividad, latencia)
- [ ] Mensual (equipo de seguridad + operaciones de TI)
  - Revisión de KPI
  - Evaluar el feedback de los usuarios
  - Ajustes de la política
- [ ] Trimestral (director de ciberseguridad + dirección)
  - Revisión estratégica: ¿Estamos alcanzando nuestros objetivos?
  - Revisión del presupuesto: ¿Se necesitan herramientas/recursos adicionales?
  - Comprobación del cumplimiento de las normativas: ¿Se cumplen todos los requisitos?
  - Lecciones aprendidas de todos los incidentes
- [ ] Anual (auditoría completa)
  - Prueba de penetración externa (incluidos escenarios de exfiltración de datos)
  - Revisión de la política: ¿Sigue todo actualizado?
  - Evaluación de herramientas: ¿Existen mejores alternativas?
  - Acuerdo de funcionamiento: ¿Son necesarios ajustes?

9.2 Ciclos de feedback

- [ ] Canal de feedback de los usuarios
  - Formulario: «El bloqueo de DLP fue incorrecto/justificado»
  - Evaluación: Falsos positivos → ajuste de políticas
  - Respuesta: El usuario recibe una respuesta en 24 horas
- [ ] Programa de campeones de la ciberseguridad
  - 1 campeón por departamento (voluntario)
  - Reunión mensual: feedback, nuevas amenazas, casos de uso
  - Los campeones forman a sus equipos (multiplicadores)

Herramientas y plantillas

Plantilla 1: Ticket de respuesta a incidentes

ID de incidente: DLP-2026-001

Fecha/hora: [AAAA-MM-DD, HH:MM, zona horaria]

Gravedad: [Crítica / Alta / Media / Baja]

Estado: [Nuevo / En curso / Contenido / Resuelto / Cerrado]

DETECCIÓN

Fuente de la alerta: [Sistema DLP / SIEM / Notificación del usuario]

Usuario afectado: [Nombre, departamento, correo electrónico]

Detalles de los datos:

- Clasificación: [Públicos / Internos / Confidenciales / Restringidos]
- Tipo de datos: [PII / Datos financieros / IP / Otros]
- Volumen: [Número de archivos / Registros de datos / MB]

Canal: [Correo electrónico / Nube / USB / Impresora / Otro]

Destino: [Interno / Externo: Dominio/Servicio]

CONTENCIÓN

Medidas:

- ☐ Cuenta bloqueada (marca de tiempo: _____)
- ☐ Correo electrónico retirado (éxito: sí/no)
- ☐ Endpoint aislado
- ☐ Instantánea forense creada

EVALUACIÓN

Causa raíz: [Técnica / Error humano / Ingeniería social / Maliciosa]

Obligación de notificar: [PARTE LOCAL - adaptar a la legislación aplicable]

- ☐ Art. 33 del RGPD (Autoridad de control, normalmente la AEPD)
- ☐ Art. 34 del RGPD (Interesados)
- ☐ Art. 23 de la NIS2 (CSIRT)
- ☐ Sin obligación de informar (motivo: _____)

SEGUIMIENTO

Ajustes de la política: [Descripción]

Medidas para el usuario: [Reciclaje / Advertencia / Medidas disciplinarias / Ninguna]

Lecciones aprendidas: [Resumen]

Plantilla 2: Solicitud de excepción de política

Solicitante: [Nombre, Departamento]

Fecha: [AAAA-MM-DD]

Justificación empresarial: [¿Por qué es necesaria la excepción?]

Regla de la política afectada: [p. ej., «Bloqueo de USB para datos restringidos»]

Datos afectados: [Clasificación, descripción]

Duración de la excepción: [Limitada hasta AAAA-MM-DD / Ilimitada]

Medidas compensatorias: [p. ej., «USB cifrado», «Principio de control dual»]

Aprobación:

- ☐ Aprobado por: [Director de ciberseguridad / Adjunto]
- ☐ Denegado (Motivo: _____)

Plantilla 3: Agenda de revisión trimestral de DLP

1. Revisión de KPI (15 min)
   - Porcentaje de detección, porcentaje de falsos positivos, tendencia de infracciones
   - Elementos de acción del último trimestre: ¿estado?
2. Revisión de incidentes (20 min)
   - Todos los incidentes de gravedad crítica/alta: ¿patrones?
   - ¿Se han implementado las lecciones aprendidas?
3. Estado de cumplimiento de las normativas (10 min) [PARTE LOCAL]
   - RGPD: ¿Se cumplen todos los requisitos?
   - NIS2: ¿Se han probado los procesos de notificación?
   - ISO 27001: ¿Auditoría preparada?
4. Feedback de los usuarios (10 min)
   - Falsos positivos más frecuentes → ajuste de políticas
   - Feedback de los campeones
5. Hoja de ruta (15 min)
   - Nuevos requisitos (nuevas herramientas en la nube, nuevos tipos de datos)
   - Optimización de herramientas
   - Presupuesto para el próximo trimestre
6. Elementos de acción (10 min)

- ¿Quién hace qué y para cuándo?

Apéndice: Glosario y referencias

Glosario

- **CASB (Cloud Access Security Broker o agente de seguridad de acceso a la nube):** Capa de control entre los usuarios y los servicios en la nube
- **DLP (Data Leak Prevention):** Tecnología para prevenir la divulgación no autorizada de datos
- **EIPD (Evaluación de impacto relativa a la protección de datos):** Análisis obligatorio para el tratamiento de datos de alto riesgo (Art. 35 del RGPD)
- **Falso positivo:** Falsa alarma (DLP bloquea una acción inofensiva)
- **MTTR (Mean Time to Respond):** Tiempo medio de respuesta a los incidentes
- **PII (Personally Identifiable Information):** Datos personales
- **SIEM (Security Information and Event Management o Gestión de eventos e información de seguridad):** Herramienta central de registro y correlación
- **SOAR (orquestación, automatización y respuesta de seguridad):** Automatización de los flujos de trabajo de seguridad
- **UEBA (User and Entity Behaviour Analytics o Análisis del comportamiento de usuarios y entidades):** Detección de anomalías basada en el comportamiento

Referencias normativas [PARTE LOCAL]

- **RGPD (UE 2016/679):** https://eur-lex.europa.eu/eli/reg/2016/679/oj
- **Directiva NIS2 (UE 2022/2555):** https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- **ISO/IEC 27001:2022:** https://www.iso.org/es/norma/27001