Plan de Respuesta a Incidentes y Certificación: Desarrollo Detallado por Apartados

1. INTRODUCCIÓN: LA IMPORTANCIA CRÍTICA DE LA RESPUESTA A INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

1.1 Contexto de Amenazas Actuales

El panorama de ciberamenazas 2024-2025 presenta:

- Ransomware 2.0: Doble y triple extorsión con filtrado de datos (Maze, LockBit, Akira)
- Ataques supply chain: 62% de las organizaciones experimentaron incidentes en 2023 (ENISA)
- Insider threats: Causan el 34% de las fugas de datos, según el Informe de Coste de Violaciones de IBM 2024
- IA generativa en ataques: Phishing hiperpersonalizado y malware polimórfico

Coste promedio de una violación de datos: 4,45 millones USD (IBM 2024). Tiempo promedio de detección: 204 días (dwell time).

1.2 Justificación del Marco de Trabajo Integrado

La convergencia NIST-ISO 27001-DLP responde a:

- Regulaciones: GDPR (Art. 33-34), NIS2 Directive, DORA, LGPD, CCPA
- Requisitos contractuales: Seguros ciber, clientes enterprise, proveedores críticos
- Ventaja competitiva: Certificación ISO 27001 aumenta la confianza en un 73% (BSI)

2. FUNDAMENTOS DEL PLAN DE RESPUESTA A INCIDENTES (PRI)

2.1 Definición Formal y Alcance

Documento vinculante que establece:

- Ambito: Todos los activos de información (digitales, físicos, humanos)
- Trigger events: 15+ eventos definidos (ver Anexo A)
- Exclusiones: Sistemas legados sin conectividad (deben documentarse)

2.2 Objetivos Específicos y Mensurables

Objetivo	**KPI**	**Meta**
Minimizar daños	MTTD (Mean Time To Detect)	< 30 minutos
Proteger datos	% datos cifrados en reposo	100%
Continuidad operativa	RTO (Recovery Time Objective)	< 4 horas
Preservar reputación	Comunicados públicos en < 2h	100% de casos

3. RECOMENDACIONES DEL NIST

Ciclo de vida NIST SP 800-61r2:

1. Preparación: Equipo CSIRT definido, playbooks para 8 escenarios, fondos reservados.
2. Detección y análisis: Correlación de alertas, clasificación por criticidad.

3. Contención/erradicación/recuperación: Decisiones rápidas (aislar, reconstruir, restaurar).
4. Post-incidente: Reportes ejecutivo/técnico, actualización de controles.

Coordinación: Comité con CISO, CIO, Legal, Comunicaciones y HR con reuniones mensuales.

4. SGSI CONFORME A ISO 27001

Estructura:

- Gap analysis: Evaluar controles actuales vs. 93 controles del Anexo A.
- Statement of Applicability: Documentar controles aplicados y justificar exclusiones.
- Clave: Control 5.24 (gestión de incidentes) con roles, categorías y tiempos de respuesta definidos.
- Certificación: Auditoría interna y externa con vigilancia anual.

5. POLÍTICAS DLP PREVENTIVAS

Definición: Proteger datos sensibles contra pérdida, uso indebido o acceso no autorizado.

Tipos:

- Network: Inspección de tráfico saliente.
- Endpoint: Agentes en dispositivos.
- Cloud: CASB para SaaS.
- Storage: Escaneo de datos en reposo.

Reglas clave: Detección de PII, PCI, IP con acciones automáticas (cifrado, bloqueo, alertas).

6. INTEGRACIÓN DLP EN ISO 27001

Mapeo: DLP cumple controles de acceso, gestión de datos y evidencia forense.

Workflow:

1. Clasificación automática de datos sensibles.
2. Monitorización continua con alertas inmediatas al CSIRT.
3. Reportes mensuales para auditoría (eventos, falsos positivos, tiempo de respuesta).

Notificación: SLA < 15 minutos interno, < 72 horas para reguladores (GDPR).

7. PROCEDIMIENTOS Y FORMACIÓN

Canales de reporte: Hotline 24/7, email automatizado, portal interno.

Programa de formación:

- Todos: Anual (45min) sobre phishing y reporte.
- Acceso sensible: Semestral (2h) sobre clasificación y DLP.
- CSIRT: Trimestral (8h) técnicas avanzadas y simulacros.

Responsabilidades: HR (offboarding), Legal (notificaciones), IT (revocar accesos), Comms (crisis).
Simulacros: 4 ejercicios anuales (tabletop, técnico, red team, drill completo).

8. CASOS Y LECCIONES

Fracaso: Twitter 2023 - DLP no configurado para APIs, $150M+ multas.
Éxito: Banco Santander - DLP + ISO 27001 redujo fugas 80%, MTTD pasó de 4h a 12min.

Lecciones: Tuneo continuo, executive sponsorship y gamificación.

9. CONCLUSIÓN Y PRÓXIMOS PASOS

Modelo de madurez: Desde ad-hoc a líder en resiliencia.
Acción inmediata (30-60-90 días):

- Día 30: Nombrar responsable ISO, gap analysis.
- Día 60: Pilotar DLP en IT/HR, definir CSIRT.
- Día 90: Formación masiva y primer tabletop.