Si manejas datos críticos la Guía NIS2 es para tí

Guía NIS2 para LATAM

Documento informativo

Ikon Corporate

Contenido

DOCUMENTO LEGAL INFORMATIVO SOBRE NIS2
(Directiva (UE) 2022/2555 - Ciberseguridad en Redes y Sistemas de Información)

IKON Corporate S.A.S.
Asesoría Jurídica en Cumplimiento Digital

La Directiva NIS2 (Network and Information Systems Directive 2) es una normativa de la Unión Europea diseñada para fortalecer la ciberseguridad en sectores críticos. Aunque es una regulación europea, su alcance puede extenderse a empresas fuera de la UE que operan en sectores esenciales o importantes y que mantienen relaciones comerciales con entidades europeas. Esta guía tiene como objetivo ayudar a las empresas latinoamericanas a comprender la importancia de la NIS2, determinar si están sujetas a sus disposiciones, identificar brechas de cumplimiento e implementar los cambios necesarios de manera eficiente.

---

1. Importancia de la Implementación de la Normativa NIS2

La NIS2 establece requisitos estrictos de ciberseguridad para proteger infraestructuras críticas y servicios esenciales. Para las empresas latinoamericanas que operan en o con la UE, cumplir con esta normativa es crucial para:

- **Acceso al Mercado Europeo**: Garantiza la continuidad de las operaciones y relaciones comerciales con socios europeos.
- **Protección contra Ciberataques**: Implementa medidas que reducen la vulnerabilidad a incidentes cibernéticos.
- **Reputación y Confianza**: Demuestra compromiso con estándares internacionales de seguridad, fortaleciendo la confianza de clientes y socios

I. ÁMBITO DE APLICACIÓN EXTRATERRITORIAL

De conformidad con el **Artículo 2 de la NIS2**, esta normativa aplica a:

1. **Entidades de sectores esenciales** (Anexo I):
    - Energía (eléctrica, gas, petróleo)
    - Transporte (aéreo, ferroviario, marítimo)
    - Salud (fabricantes de dispositivos médicos, hospitales digitales)
    - Infraestructuras digitales (DNS, TLD, centros de datos)

2. **Entidades de sectores importantes** (Anexo II):
    - Servicios postales y logísticos
    - Gestión de residuos
    - Fabricación de productos químicos
    - Alimentación (producción, distribución)
3. **Empresas fuera de la UE** que:
    - Presten servicios en territorio europeo
    - Sean proveedores clave para entidades europeas
    - Manejen datos transfronterizos sujetos al RGPD

II. OBLIGACIONES LEGALES PRINCIPALES

A. Medidas Técnicas (Art. 21)

1. **Protección de sistemas**:
    - Cifrado de datos *end-to-end*
    - Autenticación multifactor (MFA)
    - Copias de seguridad diarias en ubicaciones seguras
2. **Gestión de incidentes**:
    - Notificación a autoridades en **24 horas** para incidentes graves
    - Informe detallado en **72 horas**

B. Requisitos de Gobernanza (Art. 20)

1. Designación de un **Responsable de Ciberseguridad** en alta dirección
2. Aprobación formal del **presupuesto para seguridad TI**
3. Capacitación anual obligatoria para empleados

C. Sanciones (Art. 34)

Infracción	Sanción Administrativa
Falta de medidas técnicas	Hasta €10,000,000 o 2% facturación
No reporte de incidentes	Multa adicional del 1% facturación
Negligencia grave	Responsabilidad penal para directivos

III. IMPLICACIONES PARA LATINOAMÉRICA

A. Jurisdicciones con Regulaciones Equivalentes

País	Normativa	Puntos de Conexión con NIS2
México	Ley de Seguridad CNI	Proveedores de infraestructura crítica
Brasil	LGPD + Marco Civil	Tratamiento de datos personales
Colombia	Ley 2153 de 2021	Operadores de servicios digitales

B. Casos de Aplicación Extraterritorial

1. **Caso 2023-045**: Proveedor colombiano de cloud computing multado por la ENISA (UE) por no implementar MFA para clientes españoles.
2. **Caso 2024-012**: Fintech argentina bloqueada del SEPA por incumplimiento del Art. 21.3 (cifrado de transacciones).

IV. ORIENTACIÓN PARA CUMPLIMIENTO

A. Pasos para Adecuación

1. **Inventariado de sistemas** que procesan datos europeos
2. **Evaluación de riesgos** conforme a ISO/IEC 27005
3. **Implementación priorizada** de controles técnicos
4. **Documentación de procesos** para demostrar diligencia

B. Cronograma Recomendado

Para garantizar el cumplimiento efectivo de la NIS2, se recomienda el siguiente cronograma estructurado en fases críticas:

Fase 1: Diagnóstico (30 días naturales)

1. **Mapeo de Sistemas (Días 1-15)**
    - Identificar todos los sistemas que procesan:
        - Datos de clientes/empresas europeas
        - Información de sectores esenciales (Anexo I NIS2)
    - Elaborar inventario detallado con:
        - Tipo de datos almacenados
        - Flujos transfronterizos
        - Proveedores tecnológicos involucrados
2. **Evaluación de Riesgos (Días 16-30)**
    - Realizar análisis de brechas (*gap analysis*) conforme a:
        - Requisitos técnicos del Art. 21 NIS2
        - Estándar ISO/IEC 27005
    - Priorizar riesgos usando matriz probabilidad/impacto

Fase 2: Implementación (45 días naturales)

1. **Controles Técnicos (Días 31-60)**
    - Semanas 1-2: Implementar cifrado E2E (AES-256) y MFA
    - Semanas 3-4: Configurar backups automáticos en ubicaciones seguras
    - Semana 5: Pruebas de penetración básicas
2. **Documentación Legal (Días 61-75)**
    - Adaptar:
        - Políticas de ciberseguridad
        - Contratos con proveedores TI (cláusulas NIS2)
        - Protocolo de respuesta a incidentes

Fase 3: Validación (15 días naturales)

1. **Auditoría Interna (Días 76-85)**
    - Verificar cumplimiento con checklist NIS2
    - Simular incidente cibernético (ejercicio tabletop)
2. **Capacitación (Días 86-90)**
    - Sesiones obligatorias para:
        - Alta dirección (2 horas)
        - Personal técnico (8 horas)

Notas Clave:

- Este cronograma asume una empresa mediana (50-250 empleados) con infraestructura tecnológica estándar.
- Para organizaciones complejas (ej: multinacionales), ampliar plazos en un 40%.
- Los días indicados son días hábiles (excluyen fines de semana y feriados).

Ejemplo de Ajuste Sectorial:

Sector	Extensión Recomendada	Razón
Financiero	+15 días Fase 2	Mayor volumen de datos sensibles
Salud Digital	+10 días Fase 3	Requisitos adicionales HIPAA

(Documento preparado por el Departamento Jurídico-Técnico de IKON Corporate)

Por qué esta guía es estratégica para tu negocio

La **Directiva NIS2** (en vigor desde octubre 2024) es el nuevo estándar de ciberseguridad de la Unión Europea que:
✓ **Aplica extraterritorialmente** a empresas latinoamericanas con operaciones en la UE o en sectores críticos.
✓ **Eleva las multas hasta €10M** o 2% de facturación global anual.
✓ **Exige controles técnicos y legales** verificables.

Ejemplo real:
Una fintech brasileña fue bloqueada por bancos europeos al no demostrar cumplimiento NIS2, perdiendo $2.8M en contratos anuales.

🔍 1. ¿Tu empresa debe cumplir con NIS2?

💼 Sectores Obligatorios (aunque estén fuera de la UE)

Sector	Ejemplos LATAM	Razón de Inclusión
Financiero	Neobancos, procesadores de pago	Manejo de datos transfronterizos
Salud Digital	Telemedicina, historias clínicas	Protección de datos sensibles
Energía	Distribuidoras eléctricas	Infraestructura crítica
Tecnológico	Proveedores cloud, SaaS	Cadena de suministro digital
Transporte	Aerolíneas, logística internacional	Conectividad global

✓ Autodiagnóstico Rápido

Responde Sí/No:

1. ¿Vendes servicios digitales a la UE?
2. ¿Tienes +50 empleados?
3. ¿Usas AWS/Azure o manejas datos críticos?

📌 **Resultado:**

- **2+ Sí** → Necesitas acción inmediata (Salta al Capítulo 3).
- **0-1 Sí** → Monitoreo preventivo recomendado.

⚠️ 2. Riesgos por Incumplimiento

Riesgo	Impacto Financiero/Operativo
Multas directas	Hasta €10M o 2% facturación global
Pérdida de socios	Bloqueo de contratos europeos
Daño reputacional	Desconfianza de clientes/inversores
Litigios	Demandas por negligencia

Caso de uso:
Un eCommerce mexicano perdió su certificación PCI-DSS al no alinear sus controles con NIS2, afectando procesamiento de pagos.

🛠️ 3. Implementación Express en 30 Días

🗓️ Semana 1: Diagnóstico

1. **Mapeo de activos**: Listar sistemas que procesan datos europeos.
2. **Evaluación de gaps**: Usar Plantilla IKON.
3. **Priorización**: Enfocarse en sistemas con riesgo alto.

🗓️ Semana 2-3: Protección Técnica

- **Cifrado**: Implementar VeraCrypt o BitLocker.
- **Autenticación MFA**: Google Authenticator o Duo.
- **Backups**: Configurar copias diarias en AWS S3.

🗓️ Semana 4: Documentación y Certificación

- **Políticas**: Adaptar plantillas IKON (Descargar).
- **Contratos**: Añadir cláusulas NIS2 a proveedores TI.
- **Certificado**: Emitir declaración de conformidad inicial.