CASO PRÁCTICO: DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Y CUMPLIMIENTO NORMATIVO

Asignatura: Compliance y Ciberseguridad **Organización Objeto de Estudio:** TechGlobal
Autor: Gengis Rovi

RESUMEN EJECUTIVO

El presente informe detalla la estrategia integral de ciberseguridad y cumplimiento normativo diseñada para *TechGlobal*. Dada la naturaleza transnacional de la organización (operaciones en EE.UU. y UE), se ha optado por un modelo híbrido que armoniza los requisitos legales obligatorios del RGPD con los estándares de excelencia operativa de la norma ISO/IEC 27001 y el marco NIST. El objetivo es mitigar los riesgos operativos y legales derivados del tratamiento masivo de datos sensibles.

PARTE I: MARCO NORMATIVO Y ESTRATEGIA DE GOBIERNO

1.1. Contexto y Alcance del SGSI

La organización opera en un entorno de alta regulación. La estrategia de Gobierno, Riesgo y Cumplimiento (GRC) se ha diseñado para cubrir la confidencialidad, integridad y disponibilidad de los datos de clientes en ambas jurisdicciones.

1.2. Identificación del Marco Normativo y Estándares

Se ha realizado un análisis de brecha (Gap Analysis) para determinar las obligaciones legales y los estándares voluntarios que TechGlobal debe adoptar. A continuación, se detalla el ecosistema regulatorio aplicable:

Normativa / Estándar	*Ámbito Geográfico*	*Justificación para TechGlobal*
RGPD	*Unión Europea*	*Obligatorio por tratamiento de datos de ciudadanos UE.*
NIST CSF	*EE.UU. / Global*	*Marco de buenas prácticas para la sede americana.*
ISO 27001	*Internacional*	*Estándar certificable para demostrar diligencia debida a clientes.*

El cumplimiento del **Reglamento General de Protección de Datos (RGPD)** es crítico; el incumplimiento podría derivar en sanciones administrativas de hasta 20 millones de euros o el 4% del volumen de negocio total anual global. Por su parte, la adopción de la **ISO 27001** no es legalmente obligatoria, pero se establece como requisito estratégico para generar confianza en el mercado B2B.

1.3. Políticas Corporativas de Seguridad

Para garantizar la alineación con los estándares mencionados, se define la siguiente estructura documental jerárquica:

1. **Política General de Seguridad de la Información:** Documento de alto nivel aprobado por la Dirección, que establece el compromiso de la organización con la protección de datos.
2. **Política de Control de Accesos:** Se establece el principio de *Need-to-Know* (necesidad de conocer) y *Least Privilege* (mínimo privilegio).
3. **Política de Uso Aceptable de Activos:** Normativa para empleados sobre el uso de dispositivos corporativos y sistemas de información.

PARTE II: GESTIÓN DE RIESGOS Y CONTROLES TÉCNICOS

2.1. Metodología de Análisis de Riesgos

Para la evaluación de riesgos se ha seguido la metodología **ISO 31000** en conjunción con **MAGERIT**. Se ha valorado el Riesgo Inherente mediante la fórmula: .

2.2. Matriz de Riesgos Corporativos

A continuación, se presentan los riesgos residuales más significativos identificados durante la fase de evaluación:

ID	Riesgo	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo (PxI)	Posición / Color
R01	**Fuga de Datos Clientes**	3	5	**15**	**CRÍTICO**
R02	**Infección por Ransomware**	4	5	**20**	**CRÍTICO**
R03	**Acceso no autorizado (Hacking)**	3	4	**12**	**ALTO**
R04	**Incumplimiento Legal**	2	4	**8**	**MEDIO**

2.3. Plan de Tratamiento de Riesgos y Controles Técnicos

En respuesta a los riesgos críticos identificados en la matriz anterior, se ha diseñado el siguiente plan de acción técnica:

A. Mitigación del Riesgo de Ransomware y Malware

- **EDR (Endpoint Detection and Response):** Despliegue de agentes de seguridad avanzada en todos los servidores y estaciones de trabajo para detección comportamental.
- **Copias de Seguridad Inmutables:** Implementación de una política de backups 3-2-1, asegurando que una copia sea inmutable (WORM) para evitar su cifrado por malware.

B. Mitigación del Riesgo de Fuga de Información (Data Leakage)

- **DLP (Data Loss Prevention):** Implementación de soluciones DLP en red y endpoint para bloquear la exfiltración de datos sensibles (PII, tarjetas de crédito).
- **Cifrado:**
  - *En reposo:* Cifrado de discos duros (BitLocker/FileVault) y bases de datos.
  - *En tránsito:* Uso obligatorio de TLS 1.2 o superior para todas las comunicaciones web y VPN para accesos remotos.

C. Gestión de Identidades

- **MFA (Autenticación Multifactor):** Implementación obligatoria para todos los accesos remotos y cuentas con privilegios administrativos.

2.4. Monitorización y Mejora Continua

Para garantizar la eficacia de los controles, se establece un proceso de auditoría y revisión:

- **Monitorización Continua:** Despliegue de un SIEM para la correlación de eventos de seguridad en tiempo real.
- **Auditorías:** Realización de auditorías internas semestrales y una auditoría externa anual para la renovación de la certificación ISO 27001.

CONCLUSIONES

La implementación de este plan estratégico permite a TechGlobal no solo evitar sanciones regulatorias derivadas del RGPD, sino elevar su nivel de madurez en ciberseguridad. La adopción de la ISO 27001 estructura los procesos internos, mientras que los controles técnicos mitigan eficazmente las amenazas más probables en el panorama actual de ciberamenazas.