Lab7 elaborado por Adrian Molano

Auditoría de Políticas de Seguridad

Estudio de caso: Cisco Systems, Inc.

Fecha: *24/06/2025*

Cisco es una empresa multinacional especializada en tecnología de redes, comunicaciones y ciberseguridad. Debido a su presencia global y a que maneja grandes cantidades de información confidencial (tanto interna como de clientes), cuenta con un robusto programa de políticas de seguridad alineado a estándares internacionales como ISO/IEC 27001 y NIST SP 800-53.

En este informe auditamos las políticas actuales para evaluar su efectividad y detectar oportunidades de mejora.

Identificación de puntos fuertes y débiles

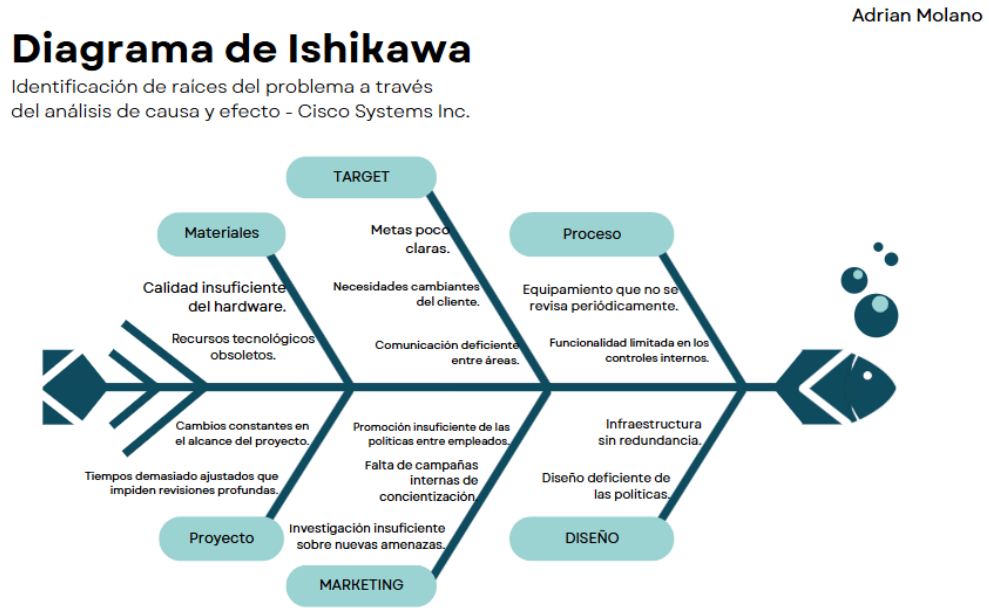
Puntos fuertes:

- **Control de accesos avanzado** mediante autenticación multifactor (MFA) y segmentación por roles.
- **Cifrado de extremo a extremo** en los datos en tránsito y en reposo.
- **Programa continuo de concientización** en ciberseguridad para empleados.
- **Centro de operaciones de seguridad (SOC)** operando 24/7.

Puntos débiles:

- Falta de una política documentada y actualizada para proveedores externos y contratistas.
- Auditorías internas realizadas solo una vez al año, sin seguimiento trimestral.
- Informes de incidentes centralizados, pero sin roles y responsables definidos claramente para su resolución.
- La documentación del Plan de Continuidad del Negocio (BCP) no ha sido probada en los últimos 18 meses.

Análisis de causas:



No conformidades encontradas

- **No conformidad 1**: La política de control de acceso a proveedores externos es ambigua y no incluye los requisitos que establece ISO/IEC 27001 Anexo A.9.

- **No conformidad 2**: Las revisiones de logs de actividad solo se efectúan semestralmente, incumpliendo los tiempos recomendados por NIST SP 800-53 (control AU-2).

- **No conformidad 3**: Falta de un plan formal de respuesta a incidentes aprobado y ensayado regularmente.

Recomendaciones de mejora

- Revisar y actualizar las políticas para incluir explícitamente a proveedores externos y contratistas, siguiendo los lineamientos de ISO/IEC 27001.

- Implementar un proceso trimestral para la revisión y auditoría interna de registros de actividad.

- Nombrar a un responsable para la creación, mantenimiento y prueba del plan de respuesta a incidentes.

- Programar una prueba anual del BCP y una auditoría del plan por un tercero independiente.

Propuesta de plan de acción

Actividad	Responsable	Plazo	Seguimiento
Actualización política de proveedores	**CISO**	**1 mes**	**Revisión por Gerencia de Riesgos**
Revisar y auditar registros trimestralmente	**Equipo de Seguridad**	**2 meses**	**Informes internos cada trimestre**
Redacción y aprobación del plan de incidentes	**Gerente de IT**	**2 meses**	**Simulación en 3 meses y mejoras**
Prueba del BCP	**PMO y Gerencia de IT**	**3 meses**	**Informe a la dirección general**