Universidad del País INNOVA

Asignatura:

Liderazgo Ejecutivo en Seguridad de la Información

Actividad:

Fase 3 – Actores Involucrados e Indicadores Estratégicos

Estudiante:

Ing. Samuel Aguilera Mendoza

Profesor:

Mtro. Jesús Andrés Ovallos Ovallos

Tuxtla Gutiérrez, Chiapas a 20 de noviembre del 2025

Introducción

La Fase 3 tiene como propósito definir la estructura organizacional y funcional que soportará la ejecución del programa de liderazgo y gestión en seguridad cibernética.

A partir de los lineamientos establecidos en las fases anteriores, se identifican los actores clave involucrados, sus responsabilidades, los canales de supervisión y los indicadores estratégicos que permitirán medir el desempeño, eficacia y alineación del programa con los objetivos empresariales.

El enfoque se sustenta en los marcos internacionales NIST CSF, ISO 27001, COBIT 2019 y ISDIL CISO Reference 2022, destacando la importancia del liderazgo ejecutivo y la gobernanza integral de la seguridad.

Título del Programa

Protección Integral de Datos y Resiliencia Digital FASTNOM 2025

(Programa ejecutivo de fortalecimiento en ciberseguridad, privacidad y cumplimiento regulatorio del ecosistema FastNom SaaS).

Contexto Organizacional

Organización: MWConsultores de México

Producto principal: FastNom, plataforma SaaS para gestión de nómina, incidencias, seguridad social y recursos humanos.

Giro: Tecnología – Desarrollo de software en la nube (SaaS/PaaS).

Tamaño y estructura: 25 colaboradores distribuidos en áreas de desarrollo, QA/Testing, infraestructura, soporte, ventas y administración.

Nivel de madurez en ciberseguridad: Medio. Existen controles técnicos básicos (acceso por roles, autenticación con Sanctum, cifrado en tránsito, respaldo de datos), pero no un programa formal de gestión de seguridad ni auditorías regulares.

Retos actuales:

- Protección de información confidencial (CFDI, datos fiscales, NSS, CURP, etc.).
- Cumplimiento con normativas de protección de datos (LFPDPPP, ISO 27001, y requisitos del SAT).
- Prevención de accesos no autorizados, ataques de fuerza bruta o inyección de código.
- Reforzar cultura de ciberseguridad entre personal técnico y administrativo.

Justificación Estratégica

La creación del Programa de Protección Integral de Datos y Resiliencia Digital FASTNOM 2025 surge de la necesidad de fortalecer la seguridad y confiabilidad de los servicios SaaS que MWConsultores ofrece a empresas y entidades públicas.

Durante los últimos meses se han identificado brechas potenciales en la gestión de accesos, actualización de dependencias y capacitación del personal, así como la ausencia de políticas formales para respuesta ante incidentes.

Implementar este programa permitirá:

- **Prevenir vulnerabilidades** que puedan afectar la disponibilidad, integridad o confidencialidad de los datos de clientes.
- **Alinear la seguridad con los objetivos de negocio**, garantizando continuidad operativa, cumplimiento regulatorio y reputación corporativa.
- **Optimizar la confianza del mercado,** fortaleciendo la imagen de MWConsultores como proveedor responsable y seguro.

En términos estratégicos, el programa responde a los riesgos financieros, legales y reputacionales asociados con la pérdida o filtración de información fiscal y personal, así como la necesidad de contar con un liderazgo ejecutivo en seguridad que oriente las decisiones técnicas bajo una visión corporativa.

Objetivo General

Fortalecer la resiliencia digital y la protección integral de datos del ecosistema FastNom, mediante la implementación de políticas, controles y prácticas de ciberseguridad alineadas con estándares internacionales (ISO 27001, OWASP Top 10) y con la legislación mexicana en materia de protección de datos personales.

Objetivos Específicos (SMART)

1. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001 en un plazo de 12 meses, cubriendo procesos críticos de desarrollo, infraestructura y soporte.
2. Capacitar al 100% del personal técnico y administrativo en políticas de seguridad, respuesta a incidentes y protección de datos antes de finalizar el segundo trimestre 2025.
3. Reducir un 50% las vulnerabilidades detectadas en análisis de seguridad y pruebas de penetración para el tercer trimestre 2025, mediante parches, refactorización de código y control de accesos.
4. Desarrollar un plan formal de continuidad y recuperación ante desastres (DRP/BCP) para FastNom antes de diciembre 2025, garantizando tiempos de recuperación menores a 4 horas.

Delimitación del Alcance

Áreas y procesos de intervenidos:

- Desarrollo de software (código fuente, control de versiones, CI/CD).
- Infraestructura y servidores (hosting, base de datos, copias de seguridad, logs).
- Procesos administrativos vinculados al manejo de información sensible (nóminas, facturación, soporte al cliente).
- Políticas internas de acceso, contraseñas y gestión de credenciales.

Limitaciones:

- Presupuesto asignado por la dirección para el ejercicio 2025.
- Recursos humanos limitados en el área de seguridad (actualmente absorbida por desarrollo).
- Dependencia parcial de servicios externos.

Supuestos:

- Colaboración total de todas las áreas de la empresa.
- Disponibilidad de herramientas de auditoría y capacitación digital.
- Apoyo ejecutivo y comunicación continua con los directores técnicos y comerciales.

Lista de Actividades Estratégicas

Nombre de la actividad	Descripción y propósito	Recursos requeridos	Área responsable	Riesgo operativo asociado	Objetivo al que contribuye
1. Programa de Capacitación en Cultura de Ciberseguridad	Diseño e implementación de talleres y micro cursos sobre higiene digital, phishing y buenas prácticas de manejo de información.	Humanos: área de TI, RH y consultores externos. Técnicos: LMS interno, material audiovisual. Financieros: presupuesto anual de formación.	Dirección de TI y RH	Falta de sensibilización del personal ante amenazas sociales.	Incrementar el nivel de conciencia y reducir incidentes por error humano.
2. Implementación del Comité de Seguridad de la Información (CSI)	Creación de un órgano colegiado que coordine políticas, auditorías y decisiones estratégicas de ciberseguridad.	Humanos: directivos, CISO, área jurídica. Técnicos: herramientas colaborativas y dashboards de KPIs. Financieros: apoyo de la alta dirección.	Dirección General / CISO	Falta de gobernanza y seguimiento de indicadores.	Fortalecer el liderazgo corporativo en seguridad y asegurar gobernanza institucional.
3. Evaluación y Certificación ISO 27001	Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) con miras a obtener certificación internacional.	Humanos: equipo TI, auditor líder, consultores. Técnicos: documentación SGSI, software de cumplimiento. Financieros: inversión inicial en auditoría externa.	Dirección TI / Compliance	Riesgo de incumplimiento normativo o pérdida de confianza de clientes.	Alinear operaciones a estándares internacionales de seguridad y gestión de riesgos.

Vinculación Actividad-Objetivo

Actividad	Objetivo vinculado
Capacitación en Cultura de Ciberseguridad	Desarrollar competencias y hábitos preventivos en todo el personal.
Comité de Seguridad de la Información	Consolidar el liderazgo ejecutivo y la toma de decisiones estratégicas en materia de seguridad.
Certificación ISO 27001	Elevar la madurez tecnológica y asegurar la confianza de los clientes y socios.

Recursos y Actores Involucrado

Tipo de recurso	Detalle / Actor responsable
Humanos	CISO, Director General, equipo TI, RH, consultor externo ISO.
Técnicos	Plataforma de capacitación LMS, software SGSI, panel de indicadores, infraestructura TI.
Financieros	Presupuesto anual de seguridad asignado al área TI y aportaciones de dirección general.

Cronograma Tentativo

Fase / Mes	Actividad principal	Entregable / Hito	Responsable
Mes 1–2	Lanzamiento del Programa de Capacitación	Cursos y test de diagnóstico aplicados	RH / TI
Mes 3–4	Creación del Comité de Seguridad de la Información	Acta constitutiva y plan de sesiones mensuales	Dirección General
Mes 5–7	Implementación del SGSI bajo ISO 27001	Manuales, políticas y auditoría interna	CISO / Consultor
Mes 8–9	Auditoría externa y certificación ISO 27001	Certificado de cumplimiento y plan de mejora continua	Dirección General / Auditor

Riesgos operativos y mitigación

Riesgo	Impacto	Estrategia de mitigación
Resistencia del personal al cambio	Medio	Comunicación y capacitación constante.
Falta de presupuesto sostenido	Alto	Integrar seguridad al plan estratégico anual.
Retrasos en certificación ISO	Medio	Acompañamiento continuo del consultor externo.

Cronograma de actividades

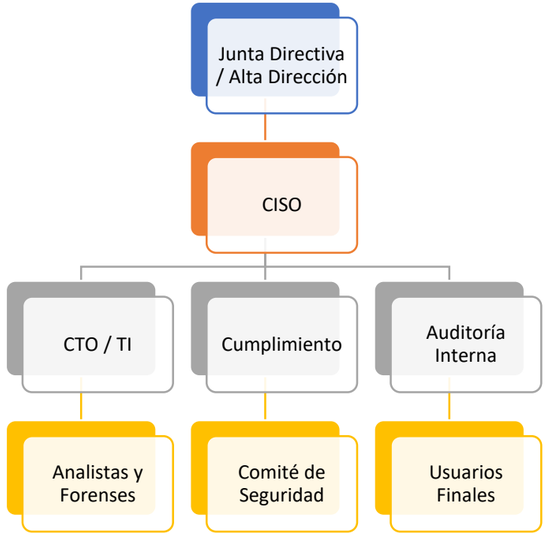
Cronograma tipo Gantt - Programa de Liderazgo en Seguridad Cibernética (FastNom)

Cronograma tipo Gantt - Programa de Liderazgo en Seguridad Cibernética (FastNom) PDF

Identificación de Actores y Roles Clave

Rol / Puesto	Funciones específicas dentro del programa	Responsabilidades directas	Nivel jerárquico	Relación con otros actores
Alta Dirección (CEO / Junta Directiva)	Define lineamientos estratégicos y aprueba presupuesto.	Asegurar recursos financieros y cumplimiento regulatorio.	Nivel 1 – Estratégico	Supervisa al CISO y recibe reportes ejecutivos.
CISO (Chief Information Security Officer)	Dirige la estrategia de ciberseguridad, coordina políticas y planes de respuesta a incidentes.	Gestionar riesgos, supervisar auditorías y liderar el comité de seguridad.	Nivel 2 – Ejecutivo	Reporta al CEO y coordina con CTO y auditores.
CTO / Equipos Técnicos	Implementan controles de seguridad, gestionan infraestructura, redes y sistemas.	Ejecución de medidas técnicas, actualizaciones y monitoreo.	Nivel 3 – Operativo	Reportan al CISO y colaboran con analistas y forenses.
Equipo de Cumplimiento y Auditoría Interna	Verifican la adherencia a políticas, normativas y estándares (ISO, GDPR, PCI).	Evaluar controles, detectar desviaciones y emitir reportes de mejora.	Nivel 3 – Operativo	Trabajan en conjunto con CISO y alta dirección.
Usuarios Finales / Personal Interno	Aplican políticas y procedimientos de seguridad.	Cumplimiento diario de las normas de uso y buenas prácticas.	Nivel 4 – Táctico	Reciben capacitación y supervisión del área TI.

Organigrama Funcional del Programa



Relaciones funcionales clave:

- El CISO funge como nodo central del programa, coordinando entre la alta dirección y las áreas operativas.
- Los equipos técnicos ejecutan las políticas definidas.
- Los usuarios finales son el eslabón de cumplimiento cotidiano.
- Las auditorías garantizan la transparencia y mejora continua.

Indicadores Estratégicos de Desempeño

Indicador	Fórmula de cálculo	Fuente de datos	Frecuencia de medición	Meta esperada	Responsable	Objetivo estratégico asociado
Índice de Cumplimiento de Políticas de Seguridad (ICPS)	(Usuarios que cumplen políticas / Total de usuarios) × 100	Reportes de auditoría interna	Trimestral	≥ 95%	CISO / Auditoría Interna	Fortalecer la cultura de cumplimiento y control interno.
Tiempo Medio de Respuesta a Incidentes (MTTR)	Σ tiempo total de respuesta / número de incidentes	Sistema SIEM / SOC	Mensual	≤ 2 horas	CTO / CISO	Reducir el impacto operativo ante incidentes críticos.
Nivel de Madurez del SGSI	Puntuación promedio obtenida en auditorías ISO 27001	Informes de auditoría externa	Semestral	≥ 4/5	CISO / Comité de Seguridad	Aumentar la madurez organizacional en gestión de riesgos.
Porcentaje de Personal Capacitado en Ciberseguridad	(Empleados capacitados / Total de empleados) × 100	RH / Registros de LMS	Trimestral	≥ 90%	Recursos Humanos / CISO	Desarrollar cultura de ciberseguridad en toda la organización.
Número de Incidentes Críticos Recurrentes	Conteo de incidentes de nivel alto / mes	Reporte del SOC	Mensual	0	CISO / CTO	Mantener continuidad operativa y control de amenazas.

Conclusión

La Fase 3 consolida la visión operativa y de gobernanza del programa de seguridad, al definir quién hace qué, cómo se supervisa y cómo se mide el éxito.

La articulación entre alta dirección, CISO, equipos técnicos y usuarios garantiza una estructura sólida basada en liderazgo, comunicación y mejora continua.

Asimismo, la incorporación de indicadores estratégicos medibles permite evaluar el progreso de manera objetiva, fomentando la transparencia, rendición de cuentas y sostenibilidad del programa.

De esta forma, la organización no solo gestiona riesgos, sino que también fortalece su madurez digital y resiliencia corporativa frente a las amenazas cibernéticas emergentes.