Si bien las TI son una herramienta poderosa para el desarrollo de los negocios, también son el origen de nuevos riesgos que se deben administrar, lo que conlleva a que cada día las empresas tienen mayor exposición a incidentes de seguridad.

Dependiendo de la necesidad del cliente PMO360 ofrece un servicio de consultoría especializada, enfocada en los procesos y en la arquitectura TI, usando como referencia las buenas prácticas, la experiencia y las definiciones del negocio.

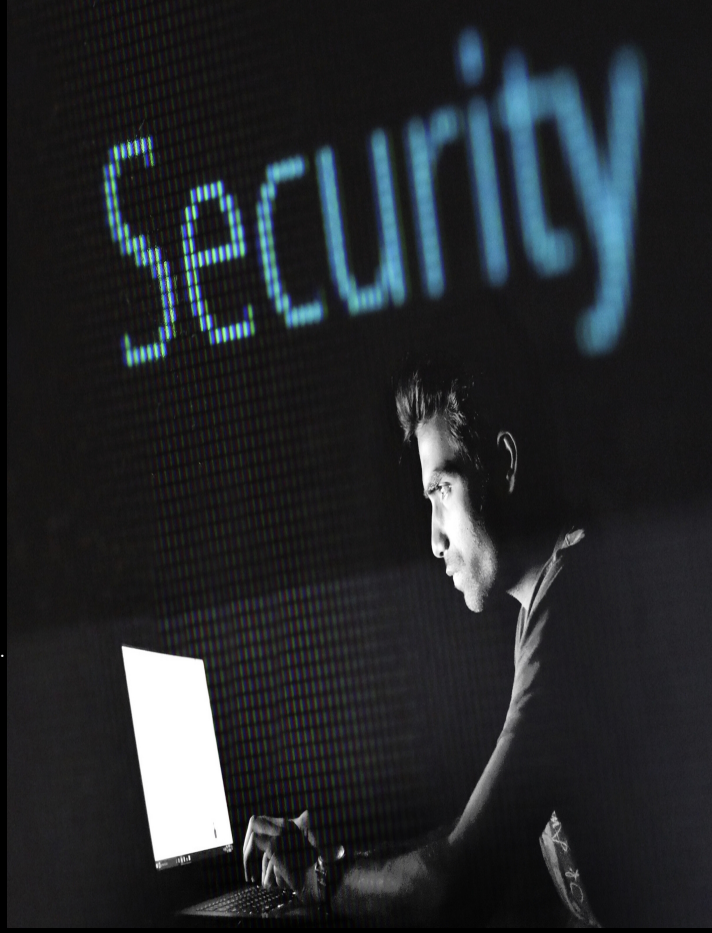
CONTÁCTANOS

+56939122872

Nueva Tajamar 481 WTC torre sur, of 1403. Las Condes.
Av. Nueva Providencia 1881, of 1201,Providencia.
Av. Nueva Providencia 1881, of 2110, Providencia.
San Antonio 19, of 702, Santiago Centro.

CONTACTO@PMO360.CL

PMO 360
Resiliencia para TI



SEGURIDAD DE LA INFORMACIÓN

WWW.PMO360.CL

OBJETIVOS

- Evaluar las condiciones de seguridad de la organización, según estándares regulatorios, corporativos o locales, nacionales o internacionales y apoyar en la adopción y cumplimiento de esos cuerpos normativos.

- Ayudar a la organización en el establecimiento, evaluación y gestión de los riesgos que enfrentan sus procesos y activos de información.

- Apoyar en la implementación efectiva de controles de seguridad que permitan establecer,formalizar, proteger, monitorear y dar respuesta ante amenazas a la seguridad.

LEVANTAMIENTO ESCENARIO ACTUAL

En esta fase se realiza el levantamiento de la situación actual incluyendo los procesos críticos del negocio y la plataforma TI y de instalaciones que la soporta, para hacer un diagnóstico de la situación de seguridad de la información de la organización.

GAP ANALYSIS

Un análisis de brecha o GAP Analysis permite conocer el estado del arte real de la Seguridad de la Información al interior de la organización, detectando aquellos elementos que presenten problemas o eventuales riesgos para la operación.

El análisis usa como referencia las buenas prácticas y normas de la ISO 27001 y/o CIS (Center for Internet Security).

EVALUACIÓN DE IMPLEMENTACIÓN

Evaluar los resultados de la implementación del Plan y formular recomendaciones de mejora, diseñar el Programa de Seguimiento a partir de las recomendaciones formuladas e implementar los compromisos establecidos en el Programa de Seguimiento.

PLAN DE IMPLEMENTACIÓN

Determinar una lista priorizada de iniciativas que puedan ser implementadas en el cliente con su respectivo análisis de impacto. Construir una “hoja de ruta” (roadmap) que sirva como guía para la implementación futura de la arquitectura y el modelo propuestos.

IMPLEMENTACIÓN DEL PLAN

Registrar y controlar los resultados de la implementación del programa de trabajo considerando actividades, dificultades, grado de avance en el cierre de las brechas, holguras detectadas, las acciones de difusión, sensibilización y capacitación y las modificaciones realizadas según lo programado.

VALOR PARA EL NEGOCIO

- Disponer de una mirada estratégica en la relación de TI y la seguridad de la información con el Negocio.
- Contar con una hoja de ruta para establecer su programa de ciber defensa y generar un plan director de ciberseguridad.
- Concientizar de todas las dimensiones del cambio que ciberseguridad requiere en una organización.
- Mejorar la competitividad en el mercado.