Implementación Planes Estratégicos

Implementación de planes específicos especializados

Las distintas organizaciones pueden tener necesidades especificas relacionadas con los ámbitos de la seguridad, servicios TI, fraudes corporativos y /o continuidad operativa, ante lo cual requieren implementar planes específicos para satisfacer dichos requerimientos estratégicos.

Objetivos del Servicio

Implementar un marco de trabajo (framework) basado en buenas prácticas establecidas por normas internacionales, que permita a la organización establecer procesos de operación, monitoreo y mejora continua, que cumplan con los requerimientos específicos establecidos por la organización. Dependiendo de los objetivos y necesidades de los clientes se ofrece la implementación de los siguientes planes de implementación basados en normativas internacionales:

Plan de Continuidad del Negocio:

- **ISO/IEC 27031:2011**, Information technology, Security techniques, Guidelines for information and communication technology readiness for business continuity.

Plan de Seguridad Informática:

- **ISO/IEC 27032:2012**, Information technology, Security techniques, Guidelines for cybersecurity.

Plan de AntiFraude:

- **AS-8001:2008**, Australian Standard, Fraud and corruption control.

Descripción del Servicio

Los planes estratégicos propuestos en nuestros servicios, poseen características propias y estratégicas que son beneficiosas para cualquier organización que quiera poseer un modelo de gestión eficiente y proyectar una excelente imagen corporativa a sus clientes, entregando un valor agregado a sus servicios y/o productos. Dichos planes implementan políticas y procedimientos específicos para operar y controlar los procesos asociados a las plataformas y/o directrices de gestión propuestas

Opciones de Implementación

La implementación de cualquiera de los planes, dependerá netamente de los objetivos estratégicos de la dirección y NO del tamaño de esta, debido a que ambas arquitecturas pueden ser empleados desde pequeñas Pymes hasta organizaciones transnacionales.

Plan de Continuidad del Negocio (PCN)

El Plan de Continuidad del Negocio, corresponde a una serie de documentos, en los cuales se definen los activos críticos para la continuidad operacional de la organización, basándose en la importancia que tienen estos para los distintos procesos de negocios, además de entregar las directrices esta debe seguir para reaccionar y trabajar en contingencia ante escenarios de catástrofe (terremotos, inundaciones, pandemias, etc.) o algún otro evento que interrumpa el funcionamiento normal de dichos procesos de negocio. Adicionalmente, se definen procedimientos y programas de prueba, con el fin de mejorar el Plan, así como también mejorar la eficiencia de los procesos, plataformas tecnológicas, personal, etc. Para que no se vean afectados de manera considerable ante un hecho de contingencia. Este Plan es requisito de distintos Sistemas de Gestión, como el SGSI (ISO 27.001), SGCN (ISO 22.301), SGCS (ISO 20.000), etc.

Plan de Seguridad Informática (PSI)

El plan de seguridad tiene por objetivo implementar procesos, políticas, procedimientos y controles (normativos y técnicos) cuyo fin es mitigar los riesgos que afectan a los activos de información críticos de la organización, bajo una arquitectura de CiberSeguridad (ISO 27032), con énfasis en el intercambio de información con terceros a través de Internet y de dominios de seguridad principales (Seguridad de la Información, Seguridad de las aplicaciones, Seguridad de Servicios en Internet, Protección de Infraestructura Crítica de Información (CIIP), y Manejo de Incidentes de Seguridad). Por lo tanto, este marco de trabajo esta acotado a la relación de la organización y traspaso de información con terceros (consumidores y proveedores) en el ciberespacio, así como también a controles técnicos aplicados a la infraestructura tecnológica que la soportan.

Plan AntiFraude (PAF)

La implementación de un plan de buenas prácticas que ayude al control y gestión de los procesos que pueden verse afectados por fraudes corporativos efectuados por personas que componen la organización, es sumamente importante, debido a que su implementación permite minimizar los riesgos potenciales de que se materialicen las amenazas que conlleven a la perdida de patrimonio o que afecten a la imagen pública de su empresa. El diseño e implementación del presente plan de acción, está pensado de acuerdo a las distintas etapas que abarcan una acción ilícita, poniendo énfasis en dos elementos primordiales; el contenido mínimo requerido que debe generar la organización para la implementación del sistema y las actividades de control en el cumplimiento de las políticas implementadas, las cueles en conjunto, permiten la ejecución de controles preventivos que minimicen la probabilidad de ocurrencia.