BASE4 SECURITY

Ayudando a construir un ecosistema digital más seguro.

Security Risk and Compliance

DATA SHEET

Aspectos generales del área

Se trabaja en el área de un modo integrado y sistémico para abordar la gobernanza, el riesgo y el cumplimiento (GRC) de la Seguridad de la Información.

Los servicios de BASE4 Security buscan garantizar un accionar éticamente correcto y conforme al nivel de riesgo aceptable por la organización (apetito al riesgo), teniendo en cuenta sus políticas internas, la normativa externa y los marcos de cumplimiento tomados como referencia.

Ello se consigue a través de un alineamiento de la estrategia corporativa y de ciberseguridad, los procesos, la tecnología y las personas.

Principios del GRC

- Logro de los objetivos del negocio mediante un trabajo conjunto de todos los involucrados.
- Información oportuna, confiable y útil para los responsables de la ejecución sobre riesgos, incentivos y responsabilidades.
- Mejora de la cultura organizacional promoviendo la responsabilidad, integridad, confiabilidad y comunicación.
- Aumento de la confianza de los interesados.
- Organización preparada para gestionar el riesgo.
- Detección, prevención y reducción de situaciones adversas o de debilidad.

- Motivación e inspiración para fomentar la conducta deseada, especialmente ante nuevos desafíos.
- Estado de alerta permanente para nuevas oportunidades.
- Mejora en las respuestas y eficiencia como ventaja competitiva.
- Maximización del retorno económico y la generación de valor.

El Gobierno de Ciberseguridad comprende el marco, los principios, las estructuras, los procesos y las buenas prácticas que establecen la dirección, el monitoreo y el desempeño de Seguridad de la Información.

Gobierno y gestión

- Virtual CISO (VCISO)
- Asesoramiento para la confección de un Plan Director de Ciberseguridad (Estrategia de SI)
- GAP análisis (Determinación del nivel de madurez de Seguridad de Información)
- Elaboración de un “Road Map” (acciones correctivas y oportunidades de mejora a corto, mediano y largo plazo)
- Documentación y revisión de políticas y procedimientos de SI (controles por oposición)
- Herramientas de gestión estratégica de SI (Plan Operativo Anual. Métricas e indicadores)
- Alineación a marcos de cumplimiento, estándares internacionales y buenas prácticas de SI (ISO, CIS, PCI, SOX, COBIT, BCRA, NIST, otros)
- Sistema de Gestión de Seguridad de la Información (ISO 27001)
- Sistema de Gestión de Continuidad de Negocios (ISO 22301)
- Ciber resiliencia: Plan de Contingencias / BCP (Plan de continuidad del negocio) / DRP (Plan de recuperación ante desastres)
- Asesoramiento para la implementación de Firma Digital
- Seguridad Industrial – OT
- Elaboración de informes ejecutivos para la dirección
- Capacitación y concientización de Seguridad de la Información

La Evaluación y Gestión del Riesgo es el proceso por el cual se analiza la probabilidad de ocurrencia de una situación y sus posibles

consecuencias. Además, se toman decisiones adecuadas para reducir el riesgo a un nivel aceptable (apetito de riesgo).

Riesgo

- Evaluación, gestión y tratamiento de riesgos operacionales y de TI (ISO 27005 / ISO 31001 / COBIT 5 / Magerit / COSO / BCRA / Otros).
- Confección de Matriz de Riesgos asociadas a proyectos.
- Inventario de activos de Información (CMDB).
- Metodologías de clasificación y rotulado de activos de información (ISO 27002)
- Análisis BIA (Bussiness Impact Analysis).
- Auditorías de cumplimiento.
- Diseño de controles de SI (Anexo A – ISO 27001 / CIS Critical Security Controls).
- Métricas e indicadores de riesgo.
- Elaboración de informes ejecutivos para la dirección.
- Pensamiento basado en riesgos (ISO 9001), acciones correctivas y oportunidad de mejora.

El Cumplimiento (compliance) es una función independiente que identifica, asesora, alerta, monitorea y reporta los riesgos de cumplimiento en las organizaciones, es decir, el riesgo de recibir sanciones por incumplimientos legales o regulatorios, sufrir pérdidas financieras o daños a la reputación por fallas de cumplimiento con las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas.

Cumplimiento

- GAP ISO.
- Auditorías de cumplimiento: ISO, SWIFT, PCI, SOX, BCRA.
- Auditoría de primera (interna) y segunda parte (partes interesadas). Según directrices de ISO 19011.
- Marco legal: ley de datos personales, privacidad, firma digital, delitos informáticos.
- Informe de auditorías con hallazgos y opinión sobre la

razonabilidad en el cumplimiento de los requisitos exigidos por el marco de referencia.

Servicios

Creación de Política

Confección y revisión de políticas y procedimientos de Seguridad de la Información, teniendo en cuenta requisitos documentales establecidos por estándares internacionales.

GAP Análisis Normativo

Confección y revisión de políticas y procedimientos de Seguridad de la Información, teniendo en cuenta requisitos documentales establecidos por estándares internacionales.

Plan Director de Seguridad de la información

Asesoramiento para la confección de un Plan director de Ciberseguridad (Estrategia de SI). Elaboración de un “Road Map” (acciones correctivas y oportunidades de mejora a corto, mediano y largo plazo)

vCISO

Es un servicio de consultoría que ayuda a los ejecutivos, equipo de TI y de Seguridad Informática a proteger los activos de información, mientras se respaldan sus operaciones sin que deban desenfocarse del “core” de negocio. BASE4 Security ayuda a diseñar la mejor estrategia de Seguridad de la Información, teniendo en cuenta las características particulares de su organización.

Gestión de Riesgo

Identificación, evaluación, gestión y tratamiento de riesgos y oportunidades operacionales y de TI (ISO 27005 / ISO 31001 / COBIT 5 / Magerit / COSO / BCRA / Otros)

BASE4
SECURITY

www.base4sec.com