BASE4 SECURITY

Ajudando a construir um ecossistema digital mais seguro.

Security Risk and Compliance

DATA SHEET

Aspectos gerais da área

Trabalhamos na área de forma integrada e sistêmica para tratar da governança, risco e conformidade (GRC) da Segurança da Informação.

Os serviços da BASE4 Security visam garantir ações eticamente corretas de acordo com o nível de risco aceitável para a organização (apetite de risco), levando em conta suas políticas internas, regulamentações externas e estruturas de conformidade tomadas como referência.

Isto é conseguido alinhando a estratégia corporativa e de segurança cibernética, os processos, a tecnologia e as pessoas.

Princípios de GRC

- Atingimento dos objetivos comerciais por todas as partes interessadas trabalhando em conjunto.
- Informações oportunas, confiáveis e úteis para os implementadores sobre riscos, incentivos e responsabilidades.
- Melhorar a cultura organizacional, promovendo responsabilidade, integridade, confiabilidade e comunicação.
- Aumento da confiança das partes interessadas.
- Organização preparada para gerenciar riscos.
- Detecção, prevenção e redução de situações adversas ou fraquezas.

- Motivação e inspiração para encorajar o comportamento desejado, especialmente diante de novos desafios.
- Permanente estado de alerta para novas oportunidades.
- Melhor resposta e eficiência como uma vantagem competitiva.
- Maximizar o retorno econômico e a geração de valor.

A Cybersecurity Governance compreende a estrutura, princípios, estruturas, processos e melhores práticas que estabelecem a direção, o monitoramento e o desempenho da Segurança da Informação.

Governança e gestão

- Virtual CISO (VCISO)
- Aconselhamento no desenvolvimento de um Plano Diretor de Segurança Cibernética (Estratégia SI)
- Análise GAP (Determinação do Nível de Maturidade da Segurança da Informação)
- Elaboração de um “Road Map” (ações corretivas e oportunidades de melhoria a curto, médio e longo prazo)
- Documentação e revisão das políticas e procedimentos da SI (controles oposicionistas)
- IS ferramentas de gestão estratégica (Plano Operacional Anual. Métricas e indicadores)
- Alinhamento às estruturas de conformidade, normas internacionais e melhores práticas do SI (ISO, CIS, PCI, SOX, COBIT, BCRA, NIST, outros)
- Sistema de Gestão de Segurança da Informação (ISO 27001)
- Sistema de Gestão da Continuidade de Negócios (ISO 22301)
- Cyber Resilience: Contingency Planning / BCP (Business Continuity Plan) / DRP (Disaster Recovery Plan)
- Assessoria na implementação da Assinatura Digital
- Segurança Industrial - OT
- Elaboração de relatórios executivos para a gerência
- Conscientização e Treinamento em Segurança da Informação

Avaliação e Gerenciamento de Riscos é o processo pelo qual a

probabilidade de ocorrência de uma situação e suas possíveis conseqüências são analisadas. Além disso, são tomadas decisões apropriadas para reduzir o risco a um nível aceitável (apetite de risco).

Risk

- Avaliação, gerenciamento e tratamento dos riscos operacionais e de TI (ISO 27005 / ISO 31001 / COBIT 5 / Magerit / COSO / BCRA / Outros).
- Preparação da Matriz de Risco associada aos projetos.
- Inventário de Ativos de Informação (CMDB).
- Metodologias de classificação e rotulagem dos ativos de informação (ISO 27002).
- Análise BIA (Bussiness Impact Analysis).
- Auditorias de conformidade.
- Projeto de controles de SI (Anexo A – ISO 27001 / CIS Critical Security Controls).
- Métricas e indicadores de risco.
- Elaboração de relatórios executivos para a administração.
- Pensamento baseado no risco (ISO 9001), ações corretivas e oportunidade de melhoria

A conformidade é uma função independente que identifica, aconselha, alerta, monitora e relata riscos de conformidade nas organizações, ou seja, o risco de ser sancionado por não conformidade legal ou regulamentar, sofrer perda financeira ou dano à reputação devido ao não cumprimento das leis, regulamentos, códigos de conduta e padrões de boas práticas aplicáveis..

Conformidade

- GAP ISO.
- Auditorias de conformidade: ISO, SWIFT, PCI, SOX, BCRA.
- Primeira (interna) e segunda parte (partes interessadas) auditorias.

De acordo com as diretrizes da ISO 19011.

- Estrutura legal: lei de dados pessoais, privacidade, assinatura digital, crimes cibernéticos.
- Relatório de auditoria com conclusões e opinião sobre a razoabilidade do cumprimento das exigências da estrutura.

Serviços

Criação de políticas

Preparação e revisão das políticas e procedimentos de Segurança da Informação, levando em conta as exigências documentais estabelecidas pelas normas internacionais.

GAP Análise regulatória

Preparação e revisão das políticas e procedimentos de Segurança da Informação, levando em conta as exigências documentais estabelecidas pelas normas internacionais.

Plano Diretor de Segurança da Informação

Assessoria na preparação de um Plano Diretor de Segurança Cibernética (Estratégia SI). Elaboração de um “Road Map” (ações corretivas e oportunidades de melhoria a curto, médio e longo prazo).

vCISO

É um serviço de consultoria que ajuda executivos, equipes de TI e Segurança de TI a proteger os ativos de informação, ao mesmo tempo em que apóia suas operações sem perder o foco no negócio principal. BASE4 Security ajuda a projetar a melhor estratégia de Segurança da Informação, levando em conta as características particulares de sua organização.

Gerenciamento de risco

Identificar, avaliar, gerenciar e tratar os riscos e oportunidades operacionais e de TI (ISO 27005 / ISO 31001 / COBIT 5 / Magerit / COSO / BCRA / Otros)

BASE4
SECURITY

www.base4sec.com