

INDUSTRY-STANDARD SECURITY FRAMEWORK GAP ANALYSIS

Avalie o nível de segurança de acordo com padrões mundialmente adotados

BENEFÍCIOS

- ◆ Conhecimento do nível de segurança e evolução no tempo
- ◆ Entendimento dos riscos relacionados
- ◆ Informações disponíveis para a melhor tomada de decisão
- ◆ Demonstração de diligência na condução dos negócios perante terceiros
- ◆ Avaliação independente das ações realizadas, processos implementados e tecnologias utilizadas
- ◆ Preparação para certificação da empresa

CONTRATOS



On Demand



Managed Services



Umbrella



Retainer

Visão geral

O primeiro passo para a tomada de boas decisões é ter informação de qualidade. Em cybersecurity não é diferente: um bom plano de ação depende de uma avaliação abrangente do nível atual de segurança.

E para entender, de forma precisa e com metodologia independente e reconhecida globalmente, o mercado utiliza padrões definidos por organizações independentes, como a ISO, o NIST e a Cloud Security Alliance.

O serviço INDUSTRY-STANDARD SECURITY FRAMEWORK GAP ANALYSIS foi desenvolvido para atender essa demanda crescente e recorrente do mercado, utilizando metodologia e técnicas consagradas mundialmente.

Para quem é indicado

Empresas que necessitam avaliar ou reavaliar o seu nível de segurança, ou o de terceiros, de acordo com frameworks de cybersecurity definidos pela indústria, para embasar tomada de decisões ou para fins de compliance.

Produtos finais

- ◆ Relatório de Gap Analysis em relação ao(s) framework(s) selecionado(s);
- ◆ Relatório evolutivo, se contratado no modelo Managed Services, ou se houver relatório anterior para o mesmo framework;
- ◆ Plano de ação para compliance com o framework (opcional).

Industry-standard Security Frameworks

O Serviço INDUSTRY-STANDARD SECURITY FRAMEWORK GAP ANALYSIS pode ser executado tendo como referência qualquer framework do mercado, tais como:

- ◆ National Institute of Technologies (NIST) Cybersecurity Framework (CSF)
- ◆ NIST Special Publication (SP) 800-82 Guide to Industrial Control Systems (ICS) Security
- ◆ MITRE ATT&CK
- ◆ International Office of Standardization (ISO) 27001
- ◆ Center for Internet Security (CIS) Controls
- ◆ Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- ◆ Control Objectives for Information Technology (COBIT)
- ◆ Payment Card Industry Data Security Standard (PCI DSS)
- ◆ Cybersecurity and Infrastructure Security Agency (CISA) Transportation Systems Sector (TSS) Cybersecurity Framework
- ◆ National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)
- ◆ Cybersecurity Maturity Model Certification (CMMC)
- ◆ European Telecommunications Standards Institute (ETSI)
- ◆ European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework
- ◆ Factor Analysis of Information Risk (FAIR) Cyber Risk Framework
- ◆ HITRUST Cybersecurity Framework (CSF)
- ◆ International Society of Automation (ISA/IEC 62443)
- ◆ International Telecommunications Union (ITU) National Cybersecurity/ Critical Information Infrastructure Protection (CIIP)
- ◆ Internet of Things (IoT) Cybersecurity Alliance (IOTCA)
- ◆ Internet of Things (IoT) Security Foundation (IoTSF) Security Compliance Framework

Além destes, qualquer outro framework pode ser eleito como baseline para a realização do serviço. Para maiores informações sobre escopo de cada um deles, visite nosso site ou solicite informações conforme instruções no rodapé deste documento.

Mais informações em www.safontreis.com

SAFONT REIS

Av. Cauaxi, 370, Unid. 161 | Alphaville
Barueri/SP | CEP: 06454-020
info@safontreis.com.br
+55 11 97657-6777

Sobre nossa empresa

Somos independentes. Não trabalhamos com vendedores, mas com advisors. Não representamos ou estamos comprometidos com fabricantes, produtos ou soluções. Estamos do lado do cliente, somos os olhos do cliente. Entendemos o negócio e as necessidades, avaliamos a situação, e recomendamos os próximos passos, baseados em uma equipe com 25 anos de experiência, trabalhando com os maiores clientes e projetos do Brasil.