Avaliação de Segurança Cibernética Baseada no CSF 2.0

Objetivo: Avaliar o nível de maturidade da organização em relação à segurança cibernética, com base no framework CSF 2.0.

Público-alvo: Todos os colaboradores da empresa.

Identificar

Gestão de Ativos (id.am)

- A organização possui um inventário completo de seus ativos de informação?
- Os ativos de informação são classificados de acordo com sua criticidade?
- Os riscos aos ativos de informação são identificados e avaliados?
- Controles de acesso adequados são implementados para proteger os ativos de informação?

Avaliação de Riscos (id.ra)

- A organização possui um processo formal para avaliação de riscos?
- Os riscos de segurança cibernética são identificados, analisados e priorizados?
- Os impactos potenciais dos riscos de segurança cibernética são quantificados?
- Planos de ação para mitigar os riscos de segurança cibernética são desenvolvidos e implementados?

Melhoria (id.im)

- A organização possui um processo formal para gerenciar as melhorias contínuas na segurança cibernética?
- As lições aprendidas com incidentes de segurança cibernética são documentadas e compartilhadas?
- As melhores práticas de segurança cibernética são identificadas e implementadas?
- A organização possui um programa de treinamento em segurança cibernética para seus colaboradores?

Proteger

Gerenciamento de Identidade, Autenticação e Controle de Acesso (pr.aa)

- A organização possui uma política de gerenciamento de identidade e acesso?
- Os acessos aos sistemas e dados da organização são controlados por meio de mecanismos de autenticação e autorização adequados?
- As senhas dos usuários são fortes e complexas?
- O acesso privilegiado é controlado e monitorado?

Conscientização e Treinamento (pr.at)

- A organização possui um programa de conscientização em segurança cibernética para seus colaboradores?
- Os colaboradores são treinados sobre os riscos de segurança cibernética e as melhores práticas para se protegerem?
- Os colaboradores são treinados sobre como reportar incidentes de segurança cibernética?

Segurança de Dados (pr.ds)

- A organização possui uma política de segurança de dados?
- Os dados confidenciais são criptografados?

- Os dados confidenciais são armazenados de forma segura?
- A organização possui um processo para backup e recuperação de dados?

Segurança da Plataforma (pr.ps)

- Os sistemas da organização são atualizados com os últimos patches de segurança?
- Os sistemas da organização são configurados de forma segura?
- A organização possui um processo para monitorar e detectar atividades maliciosas em seus sistemas?

Resiliência da Infraestrutura Tecnológica (pr.ir)

- A organização possui um plano de contingência para lidar com interrupções no serviço?
- A organização possui um plano de recuperação de desastres?
- A organização testa regularmente seus planos de contingência e recuperação de desastres?

Observações:

- As respostas às perguntas acima devem ser documentadas e analisadas para determinar o nível de maturidade da organização em relação à segurança cibernética.
- A auto auditoria deve ser realizada periodicamente para verificar se a organização está continuamente aprimorando sua postura de segurança cibernética.
- É recomendável que a auto auditoria seja realizada por um profissional qualificado em segurança cibernética.