ADV Management

Programa de Privacidade e Segurança da Informação

para escritórios de advocacia de pequeno e médio portes

Valter Araujo
Diretor Executivo I CISO

COMPONENTES DE UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Ativos de Informação

Tudo que tem valor

Ameaça

Potencial causa de um incidente

Vulnerabilidade

Fragilidade de um ativo

Risco

Probabilidade de impacto ao negócio

Incidente

Evento indesejado

Dano

Perda ou prejuízo

Recuperação

Restabelecimento das operações

Medidas de Segurança

Combater e minimizar a perda de ativos de informação devido a ação de uma ameaça.

REDUTIVA

Reduzir a probabilidade de uma ameaça.

PREVENTIVA

Proteger contra o surgimento de uma ameaça.

DETECTIVA

Detectar o incidente o mais breve possível.

REPRESSIVA

Minimizar as consequências ou conter o incidente.

CORRETIVA

Reparar o que foi danificado.

Sistema de Gestão de Segurança da Informação – SGSI

AVALIAÇÃO DO AMBIENTE

Levantamento da situação atual e identificação dos pontos críticos que serão necessários endereçar para alcançar um nível de segurança ideal.

Entender as potenciais ameaças e suas consequências a fim de implementar medidas de controle e mitigação eficazes.

Serve como um mapa que valida os controles de segurança da informação que são relevantes e aplicáveis no ambiente.

CONTROLES ORGANIZACIONAIS

Políticas, diretrizes e práticas estabelecidas para garantir que as pessoas, parceiros de negócios e processos estejam alinhados com a estratégia e os objetivos de segurança da informação.

CONTROLES TECNOLÓGICOS

Medidas implementadas por meio de hardware e software projetadas para proteger, prevenir, detectar, monitorar e responder a ameaças e vulnerabilidades tecnológicas.

CONTROLES DE PESSOAS

Estratégia projetada para garantir que os indivíduos que interagem com os ativos de informação o façam de maneira segura e em conformidade com as políticas e procedimentos estabelecidos.

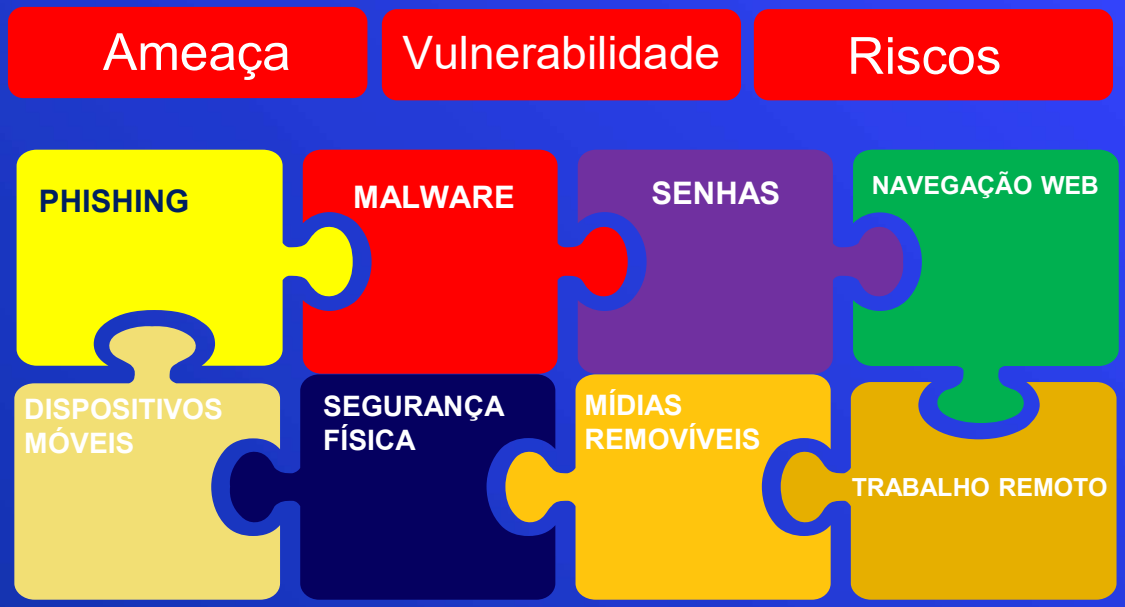
CONTROLES FÍSICOS

Métodos e dispositivos implementados para proteger fisicamente instalações, equipamentos, dados e pessoas de acessos não autorizados, danos, roubo ou qualquer tipo de ameaça física.

MELHORIA CONTÍNUA

Aprimoramento constante das defesas e dos procedimentos de segurança de forma que se mantenham eficazes diante da evolução das ameaças e das mudanças no ambiente tecnológico.

Treinamento em Conscientização em Segurança da Informação e Segurança Cibernética



BENEFÍCIOS

- Conformidade com a norma ISO 27001
- Compatibilidade com clientes e fornecedores
- Desenvolvimento da cultura de segurança
- Identificação de riscos e vulnerabilidades
- Revisão de políticas e procedimentos
- Impedir vazamento de dados sensíveis
- Evitar problemas de má reputação

ADV
Management

advmanagement.com.br