Prime

ISF – CONTROLES ORGANIZACIONAIS

Foco da **Segurança da Informação**

Só para relembrar!

O objetivo geral da Segurança de TI é:

- ✓ "Segurança equilibrada com profundidade“;
- ✓ Implementar controles justificáveis;
- ✓ Assegurar que a Política de Segurança da Informação é aplicada;
- ✓ Que os Serviços de TI estão dentro dos parâmetros de segurança;
- ✓ Que atendam o tripé CID (Confidencialidade, Integridade e Disponibilidade).

? Normalmente, qual a melhor abordagem de uma segurança da informação?

Para muitas organizações, a abordagem é feita através de uma Política de Segurança da Informação (PSI).

? A Política de Segurança da Informação deve então ser o nosso foco?

Não! O processo de Gerenciamento da Segurança da Informação – GSI (ISMS) deve ser o ponto focal para todas as questões de Segurança de TI.

? Porque a ISMS? O que a ISMS garante?

Ela garante que uma PSI será criada, mantida e reforçada, cobrindo usos e abusos de todos os sistemas e serviços de TI.

Gerenciamento da **Segurança da Informação**

Se a ISMS é o nosso foco inicial. Como ela nos ajuda?

- A GSI precisa entender todo o ambiente de Segurança de TI e de Negócio, incluindo:
  - ✓ Política e planos de Segurança de Negócios;
  - ✓ Operação de negócios atual e seus requisitos de Segurança;
  - ✓ Planos de negócios futuros e requisitos;
  - ✓ Requisitos legais;
  - ✓ Obrigações e responsabilidades em relação à Segurança para os ANSs (SLAs);
  - ✓ Os Riscos do Negócio e da TI, e Gestão de Risco.

E o que tem dentro de uma PSI?

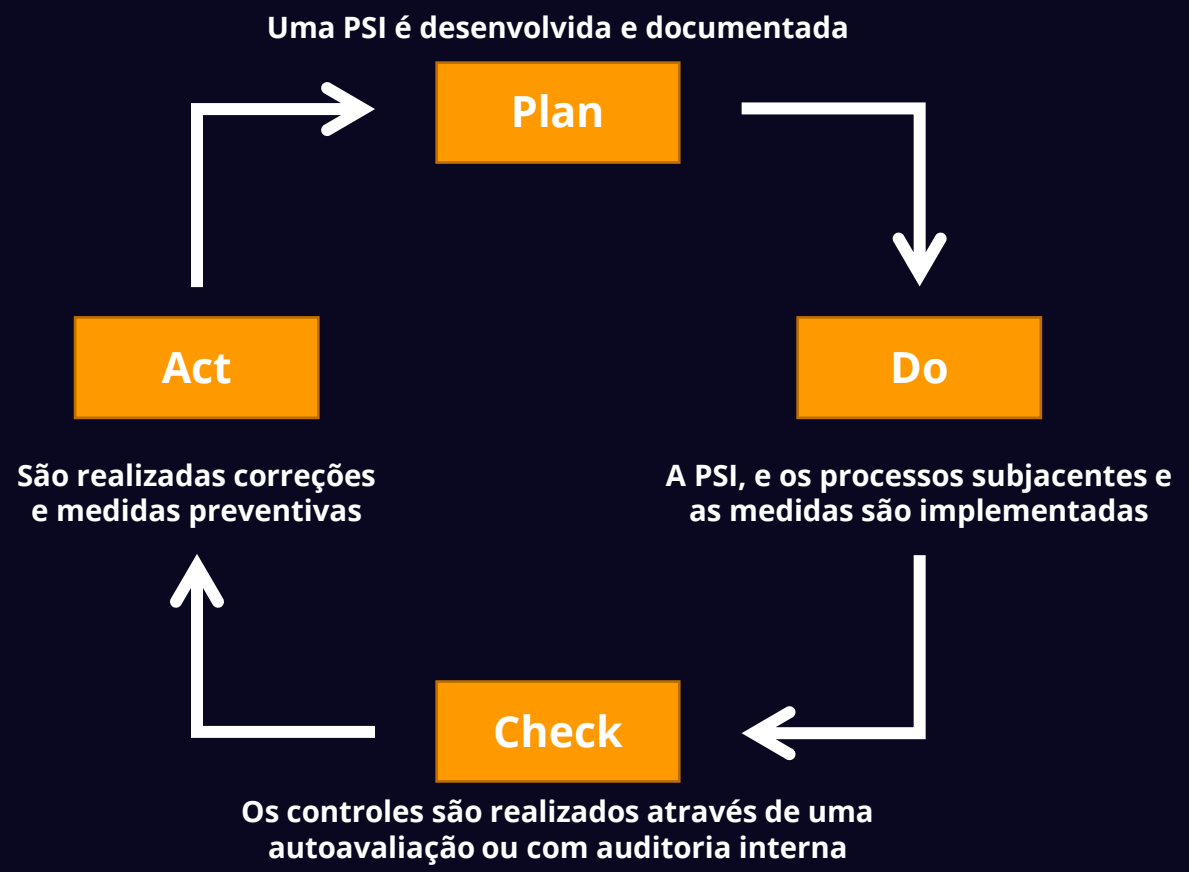
- A Política de Segurança da Informação consiste em:
  - ✓ Política geral de Segurança da Informação;
  - ✓ Política para usos e abusos dos ativos de TI;
  - ✓ Política de controle de acesso;
  - ✓ Política de controle de senha;
  - ✓ Política de e-mail;
  - ✓ Política de uso da internet;
  - ✓ Política antivírus;
  - ✓ Política de classificação da informação;
  - ✓ Política de classificação de documentos;
  - ✓ Política de acesso remoto;
  - ✓ Política sobre o acesso dos fornecedores aos Serviços de TI, informações e componentes;
  - ✓ Política de alienação de bens.

Medidas de **Segurança Organizacional**

- Medidas Técnicas estão intimamente relacionadas com Medidas Organizacionais. Medidas Técnicas executam ou forçam Medidas Organizacionais;
- O ciclo PDCA é uma forma de implementar a Segurança da Informação na organização;
- As medidas organizacionais promovem a Segurança da Informação na organização;
- Lidam com os aspectos da comunicação da Segurança da Informação;
- Lidam com os aspectos operacionais, procedimentos e gestão da Segurança da Informação, tais como:

- ✓ Política de Segurança da Informação;
- ✓ Ativos;
- ✓ Controle de Acesso;
- ✓ Direitos de Acesso;
- ✓ Gerenciamento de Incidente de Segurança;
- ✓ Evidências;
- ✓ Privacidade;
- ✓ Conformidade;
- ✓ Relacionamento com Fornecedores;
- ✓ Etc.

Modelo PDCA


Uma PSI é desenvolvida e documentada
Plan
Do
A PSI, e os processos subjacentes e as medidas são implementadas
Check
Os controles são realizados através de uma autoavaliação ou com auditoria interna
Act
São realizadas correções e medidas preventivas

Considerações sobre **Política de Segurança da Informação**

- A Política de Segurança da Informação deve ser aprovada pelo conselho administrativo e publicada a todos os interessados e envolvidos;
- Deve ser revisada continuamente ou quando ocorrerem mudanças significativas;
- Mantido na Intranet, por exemplo;
- Pode ser incluída no processo de admissão de um funcionário;
- Ter uma Política é uma coisa, cumpri-la é outra;
- Uma Política contém: Procedimento, Política de Documento, Diretrizes, etc;
- Parte de um ISMS (Information Security Management System);
- Independente do tamanho da empresa.

Controle: Política de Segurança da Informação

Objetivo:

Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Como a direção orienta?

- Ela estabelece uma política clara;
- Ela alinha com os objetivos do negócio;
- Demonstra apoio e comprometimento com a segurança da informação;
- Por meio da publicação e manutenção para toda a organização.

Como pode ser estruturada a Política de Segurança da Informação?

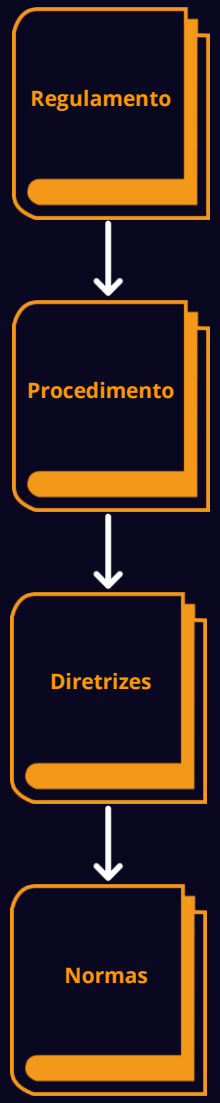
- Pode fazer parte de um documento da política geral;
- Poder ser separada;
- Se for distribuída fora da organização, cuidado para não revelar informações sensíveis.

Exemplos de Políticas de **Segurança da Informação**

Os exemplos a seguir são de níveis mais baixos, ou seja, de temas que compõem e apoiam uma política de Segurança da Informação:

- Controle de acesso;
- Classificação e tratamento da informação;
- Segurança física e do ambiente;
- Tópicos orientados aos usuários finais:
  - ✓ Uso aceitável dos ativos;
  - ✓ Mesa limpa e tela limpa;
  - ✓ Transferência de informações;
  - ✓ Dispositivos móveis e trabalho remoto;
  - ✓ Restrições sobre o uso e instalação de software;
- *Backup*;
- Transferência da informação;
- Proteção contra malware;
- Gerenciamento de vulnerabilidades técnicas;
- Controles criptográficos;
- Segurança nas comunicações;
- Proteção e privacidade da informação de identificação pessoal;
- Relacionamento na cadeia de suprimento.

Conteúdo Hierárquico de uma Política



Regulamento:

- Um regulamento é mais detalhado do que um documento de política.

Procedimento:

- Descreve a forma “como” certas medidas devem ser implementadas, e pode, às vezes, incluir instruções de trabalho.

Diretrizes:

- Fornecer orientação:
  - ✓ Descreve quais aspectos precisam ser examinados através de aspectos de segurança específicos;
  - ✓ Diretrizes não são obrigatórias, mas possuem natureza consultiva.

Normas:

- Descrevem as regras de como atingir os objetivos da organização.
- Por exemplo: Característica desejável de um software, visando a segurança, qualidade etc.

Publicando uma Política

- Primeiro, a PSI deve ser revisada em intervalos planejados ou quando ocorrerem mudanças significativas;
- Lembre-se que essa Política deve ser escrita de acordo com os requisitos do Negócio, bem como de acordo com as leis e regulamentos;
- Depois, a PSI deve ser aprovada pelo Conselho Administrativo;
- Publicada para todos os empregados e partes externas relevantes, tais como clientes e fornecedores;

Como podemos publicar a Política?

- ✓ Crie uma versão resumida da Política com os pontos principais;
- ✓ **Isso pode ser feito:**
  - ✓ Na forma de um panfleto para todos os funcionários;
  - ✓ Incluído como parte do kit introdutório aos novos empregados.
- ✓ **A versão completa pode ser:**
  - ✓ Publicada na Intranet da empresa;
  - ✓ Ou em algum outro local que seja de fácil acesso a todos os funcionários.
- ✓ Deve haver algum programa de conscientização para alcançar todos os funcionários.

Controle: Funções e Responsabilidades de Segurança da Informação

Objetivo:

As funções e responsabilidades de segurança da informação devem ser definidas e alocadas de acordo com as necessidades da organização.

De acordo com o quê deve ser definida a alocação de funções e responsabilidades?

- De acordo com a política de segurança da informação;
- E de acordo com políticas específicas da organização.

Que tipo de responsabilidade deve ser definida e gerenciada?

- Para proteção de informações e outros ativos associados;
- Para realizar processos específicos de segurança da informação;
- Para atividades de gerenciamento de riscos;
- Para todo o pessoal que usa as informações de uma organização e outros ativos associados.

A Organização da **Segurança da Informação**

- Sem uma Segurança da Informação aceita por todos, a empresa pode não sobreviver;
- Por isso a Alta Direção deve dar o exemplo;
- Apesar de todos estarem envolvidos, depende da natureza da empresa;
- Independente do porte, deve haver uma definição de responsabilidades dos envolvidos.

Funções

As funções de Segurança da Informação podem ter nomes diferentes, mas, em geral, se resumem às seguintes posições:

- O **Chief Information Security Officer - CISO** é o mais alto nível da gestão da organização e desenvolve a estratégia geral de segurança para todo o negócio;
- O **Diretor de Segurança da Informação – DSI (Information Security Officer – ISO)** desenvolve a política de segurança de uma unidade de negócios com base na política da empresa e garante que seja seguida;
- O **Gerente de Segurança da Informação – GSI (Information Security Manager – ISM)** desenvolve a política de segurança da informação dentro da organização de TI e garante que seja seguida;

- Além dessas funções que são especificamente voltadas para a segurança da informação, a organização pode ter um **Information Security Policy Officer (ISPO)** ou um **Data Protection Officer (DPO).**

O Gerente de **Segurança da Informação**

Responsável por assegurar que os objetivos da Gestão da Segurança da Informação sejam atendidos, tais como:

- ✓ Desenvolver, manter, comunicar e divulgar a PSI;
- ✓ Garantir que a PSI seja aplicada e cumprida;
- ✓ Identificar e classificar os ativos de TI e de informação, e o nível de controle e proteção exigido;
- ✓ Ajudar com Análises de Impacto nos Negócios;
- ✓ Realizar Análise de Risco de Segurança e Gestão de Risco;
- ✓ Criar controles de segurança e desenvolver planos de segurança;
- ✓ Desenvolver e documentar os procedimentos para operar e manter os controles de segurança;
- ✓ Monitorar e gerenciar todas as violações de segurança e lidar com incidentes de segurança;
- ✓ Relatórios, análises e redução do impacto e dos volumes de todos os incidentes de segurança;
- ✓ Promover educação e conscientização de segurança;

O Gerente de **Segurança da Informação**

- ✓ Garantir (no CAB) que todas as alterações sejam avaliadas em relação a seus impactos em todos os aspectos de segurança, incluindo os controles;
- ✓ Realizar testes de segurança;
- ✓ Participar em quaisquer revisões de segurança decorrentes de violações de segurança e ações corretivas;
- ✓ Assegurar que a confidencialidade, integridade e disponibilidade dos serviços sejam mantidas nos níveis acordados (ANSs) e que estejam em conformidade com todos os requisitos legais aplicáveis;
- ✓ Garantir que todo o acesso aos serviços por parceiros externos e fornecedores esteja sujeito às obrigações e responsabilidade contratuais;
- ✓ Atuar como um ponto focal para todas as questões de segurança.

Controle: Segregação de Funções

Objetivo:

Deveres conflitantes e áreas de responsabilidade conflitantes devem ser segregados.

Porque eu devo separar as funções?

- Para reduzir o risco de fraude;
- Reduzir erro;
- Minimizar desvios de controles de segurança da informação.

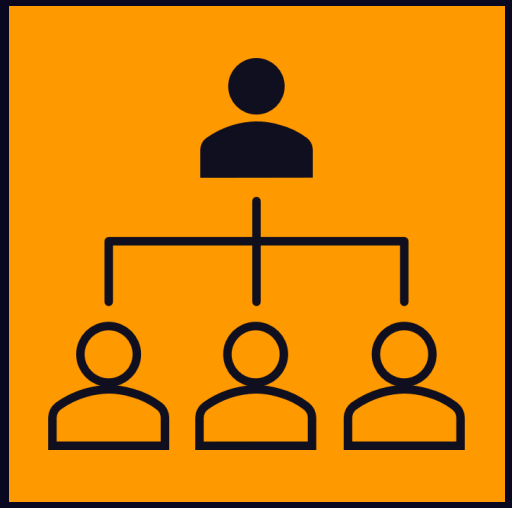
Que tipo de atividades podem ser segmentadas?

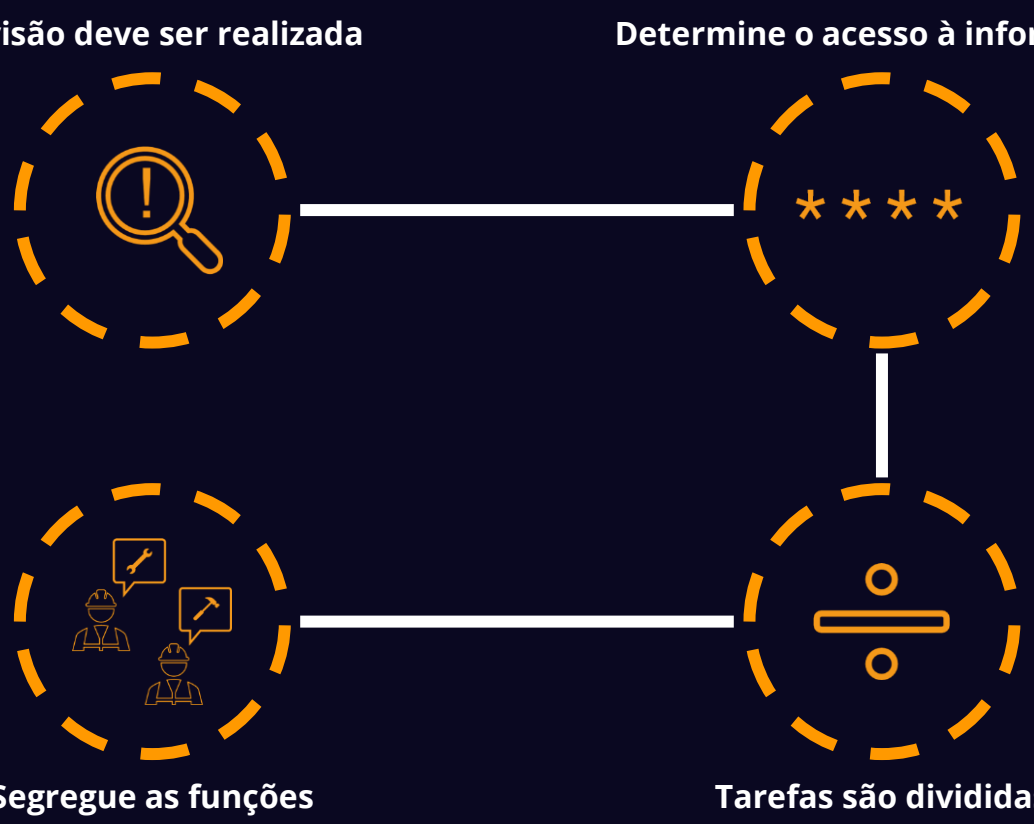
- Para iniciar, aprovar e executar uma mudança;
- Para solicitar, aprovar e implementar direitos de acesso;
- Para projetar, implementar e revisar o código;
- Para desenvolver software e administrar sistemas em produção;
- Para usar e administrar aplicativos;
- Para usar aplicativos e administrar bancos de dados;
- Para projetar, auditar e assegurar controles de segurança da informação.

- Mesmo em empresas pequenas, deve ser aplicada a separação na medida do possível.
- Cuidado com funções conflitantes!

Segregando Funções

Tarefas e responsabilidades devem ser separadas para evitar que alterações não autorizadas e não intencionais sejam executadas ou evitar o uso indevido de ativos da organização





Consideração na **Segregação dos Deveres**

- Funções e áreas de responsabilidade podem ser contraditórias;
- Segregar pode reduzir as oportunidades de modificação ou uso indevido de ativos da organização;
- As alterações podem ser não autorizadas ou não intencionais;
- O acesso sem necessidade aumenta o risco de a informação ser utilizada, alterada ou destruída, intencionalmente ou não;
- Trata-se do princípio da “necessidade de conhecer”;
- Sempre que houver dificuldade de segregação, outros controles devem ser considerados, como:
  - ✓ Monitoramento das atividades;
  - ✓ Trilhas de auditoria;
  - ✓ Supervisão da gestão.

Controle: Responsabilidades da Gestão

Objetivo:

A administração deve exigir que todo o pessoal aplique a segurança da informação de acordo com a PSI estabelecida, políticas e procedimentos específicos da organização.

Como a gestão consegue isso?

- Primeiro ela entende o seu papel na segurança da informação;
- Depois realiza ações com o objetivo de garantir que todos os funcionários:
  - ✓ Estejam cientes;
  - ✓ Cumpram suas responsabilidades de segurança da informação.

Os gestores devem garantir que o pessoal:

- Entenda suas funções e responsabilidades antes de acessarem as informações;
- Suas expectativas de segurança da informação e seu papel dentro da organização;
- Cumpra suas obrigações da PSI;
- Alcance o nível de conscientização;
- Entenda os termos e condições de trabalho, contrato ou acordo;
- Tenha as habilidades e qualificações adequadas em segurança da informação;
- Tenha um canal confidencial para denúncias de violações;
- Receba os recursos adequados para implementar os processos e controles relacionados à segurança.

Controle: Contato com as Autoridades

Objetivo:

A organização deve estabelecer e manter contato com as autoridades relevantes.

Por que manter esses contatos?

- Para garantir um fluxo de informações em relação à SI entre:
  - ✓ A organização;
  - ✓ Autoridades legais.

Que tipo de contato?

- Policiais locais;
- Autoridades supervisoras (LGPD);
- Autoridades reguladoras e de aplicação da lei;
- Pessoal de apoio de emergência, como corpo de bombeiros;
- Outros serviços públicos, água, luz etc., e de emergência;
- E ainda os provedores de serviços, como de telecomunicações e Internet.

O que fazer com estes contatos?

- Manter atualizados;
- Atrelados a procedimentos de como e quando entrar em contato;
- Atrelados a procedimentos para tomadas de ações, como continuidade do negócio;
- Mantê-los à mão, ou seja, fácil acesso.

Controle: Contato com Grupos de Interesses Especiais

Objetivo:

A organização deve estabelecer e manter contato com grupos de interesse especial ou outros fóruns especializados em segurança e associações profissionais.

Por que isso?

- Para garantir um fluxo de informações em relação a Segurança da Informação;
- Essa afiliação melhora o conhecimento de todos;
- Para obter acesso aos conselhos de especialistas destes grupos de interesse especiais;
- Receber orientação e informações de empresas sobre correções relacionadas ao hardware e ao software;
- Melhorar o conhecimento sobre as melhores práticas;
- Manter-se atualizado com as informações de segurança;
- Receber avisos antecipados de alertas, avisos e patches referentes a ataques e vulnerabilidades;
- Ter acesso a assessoria especializada em segurança da informação;
- Compartilhar e trocar informações sobre novas tecnologias, produtos, serviços, ameaças ou vulnerabilidades;
- Fornecer pontos de ligação para lidar com incidentes de segurança da informação.

Controle: Inteligência de Ameaças

Objetivo:

As informações relacionadas às ameaças à segurança da informação devem ser coletadas e analisadas para produzir inteligência sobre ameaças.

O que é Inteligência de Ameaças?

- Pode identificar e analisar as ameaças cibernéticas;
- Coleta e filtra inúmeras fontes e pacotes de pilhas de dados;
- Obtém insights relevantes para proteção contra crimes;
- Identifica padrões, hipóteses e tendências (IA);
- Examina contextualmente os dados para identificar reais problemas;
- Implementa soluções para os problemas encontrados;
- Não confundir com “dados sobre ameaças”, pois este só lista as possíveis ameaças.

As informações sobre ameaças existentes ou emergentes são coletadas e analisadas para:

- Evitar que as ameaças causem danos à organização;
- Reduzir o impacto de tais ameaças.

Atividades da **Inteligência de Ameaças**

As atividades de inteligência de ameaças devem incluir:

1. Estabelecer os objetivos da inteligência de ameaças;
2. Identificar, vetar e selecionar fontes de informações internas e externas;
3. Coletar informações de fontes selecionadas;
4. Processar informações coletadas para prepará-las para análise (por exemplo, traduzindo, formatando ou corroborando informações);
5. Analisar as informações para entender como elas se relacionam e se são significativas para a organização;
6. Comunicar e compartilhar com indivíduos em um formato que possa ser entendido.

A inteligência de ameaças deve ser analisada e usada posteriormente:

1. No gerenciamento de riscos de segurança da informação da organização;
2. Como entrada adicional para controles técnicos preventivos e de detecção, como firewalls, detecção de intrusão sistema ou soluções antimalware;
3. Como insumo para os processos e técnicas de teste de segurança da informação.

Considerações da **Inteligência de Ameaças**

A inteligência de ameaças pode ser dividida em três camadas:

Inteligência estratégica de ameaças:

- Troca de informações de alto nível sobre a mudança de cenários de uma ameaça;
- Exemplo: tipo de invasor está mudando ou o escopo dos tipos de ataques mudou.

Inteligência tática de ameaças:

- Informações sobre metodologias, ferramentas e tecnologias do invasor envolvidos.

Inteligência operacional de ameaças:

- Detalhes sobre ataques específicos, incluindo indicadores técnicos.

A inteligência de ameaças deve ser:

- Relevante (ou seja, relacionada à proteção da organização);
- Esclarecedora (ou seja, fornecer à organização uma compreensão precisa e detalhada do cenário de ameaças);
- Contextual, para fornecer consciência situacional (ou seja, adicionar contexto às informações com base no momento dos eventos, onde ocorrem, experiências anteriores e prevalência em organizações similares);
- Acionável (ou seja, a organização pode agir sobre as informações de forma rápida e eficaz).

Controle: Segurança da Informação na Gestão de Projetos

Objetivo:

A segurança da informação deve ser integrada ao gerenciamento de projetos.

Por que isso é importante?

- Para que os riscos de segurança da informação sejam abordados durante todo o ciclo de vida do projeto;
- Avaliado o quanto antes;
- Seja incluído os requisitos de segurança da informação;
- Envolvido em todos os tipos de projetos, não apenas em projetos de TI;
- Alinhado independente se é projeto em cascata ou ágil;
- Alinhado na programação segura;
- Alinhado com o DevSecOps.

OBRIGADO

ISF – CONTROLES ORGANIZACIONAIS