



Prime

**ISF – SEGURANÇA DA
INFORMAÇÃO EM
RECURSOS HUMANOS**

Segurança dos Recursos Humanos

Dentro do domínio Segurança dos Recursos Humanos é tratado:



Responsabilidades dos colaboradores pela SI;



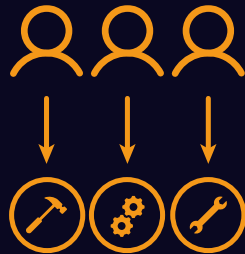
Contrato e Código de Conduta;



Acordos de Confidencialidade e Não-Divulgação.



Antes



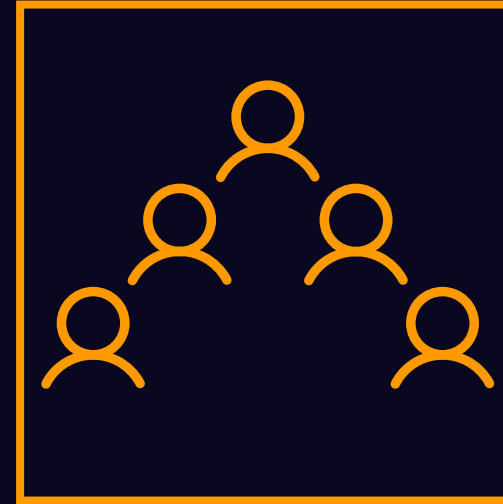
Durante



Depois

Pessoal

- Patrimônio da empresa;
- Todos são responsáveis pela Segurança da Informação;
- O manual dos funcionários deve conter um código de conduta, junto com as sanções;
- O gerente é responsável pela correta descrição dos cargos e da SI;
- Pode ser indicada a pesquisa de antecedentes;
- Rigorosos procedimentos de desligamento.



A Organização da Segurança da Informação



- Deve ser aceita por todos;
- Conselho Administrativo deve dar exemplo;
- A forma como será gerenciada depende da natureza e porte da empresa;
- Independente do tamanho, a definição de responsabilidades é essencial;
- Todos que manuseiam a informação precisam assegurá-la.

Controle: Triagem



Objetivo:

Garantir que todo o pessoal seja elegível e adequado para as funções para as quais é considerado e permaneça qualificado e adequado durante seu emprego.

O que é feito antes da contratação?

- Verifica-se os antecedentes de todos os candidatos a se tornarem funcionários;
- Geralmente apresenta-se também um atestado de boa conduta;
- A verificação deve ser realizada antes de ingressar na empresa e de forma contínua;
- A verificação deve seguir as leis, regulamentos e ética, e os requisitos do negócio;
- Garantir que todo o pessoal seja elegível e adequado para as funções;



Controle: Triagem



O que é feito antes da contratação?

- Um processo de triagem deve ser realizado para todo o pessoal, incluindo funcionários:
 - ✓ Em tempo integral;
 - ✓ Meio período;
 - ✓ Temporários;
 - ✓ Contratados por meio de fornecedores (incluídos nos acordos e contratos).

Considerações sobre a Triagem

A verificação deve levar em consideração:

- A privacidade dos dados;
- A proteção da PII (Informação pessoalmente identificável);
- A legislação vigente – lesão moral;
- O quão profunda é a verificação vai depender do nível de confidencialidade:
 - ✓ Específica de profissionais de segurança da informação;
 - ✓ Que envolve o manuseio e processamento de dados e informações confidenciais.
- A triagem pode custar muito;
- Existem organizações que podem conduzir tal triagem.

Controle: Termos e Condições de Emprego



Objetivo:

Garantir que o pessoal entenda suas responsabilidades de segurança da informação para as funções para as quais são considerados.

Os contratos de trabalhos ou acordos contratuais de trabalho devem:

- Indicar as responsabilidades do pessoal;
- Indicar as responsabilidades da organização pela segurança da informação;
- Considerar a política de segurança da informação;
- Ser concordados antes da contratação;
- Ser concordados após uma mudança nas políticas;
- Ser revistos quanto às leis, regulamentações e políticas;
- Continuar validados até o término do contrato de trabalho.



A ideia é garantir que entendam suas responsabilidades de segurança da informação para as funções para as quais são considerados.

Código de Conduta

Um código de conduta pode ser usado para as responsabilidades de:

- Segurança da Informação;
- Em relação à confidencialidade;
- Proteção da PII;
- Ética;
- Uso apropriado das informações da organização e outros ativos;
- Bem como práticas confiáveis esperadas pela organização.



Conscientização, Educação e Treinamento



Sensibilização



Cursos



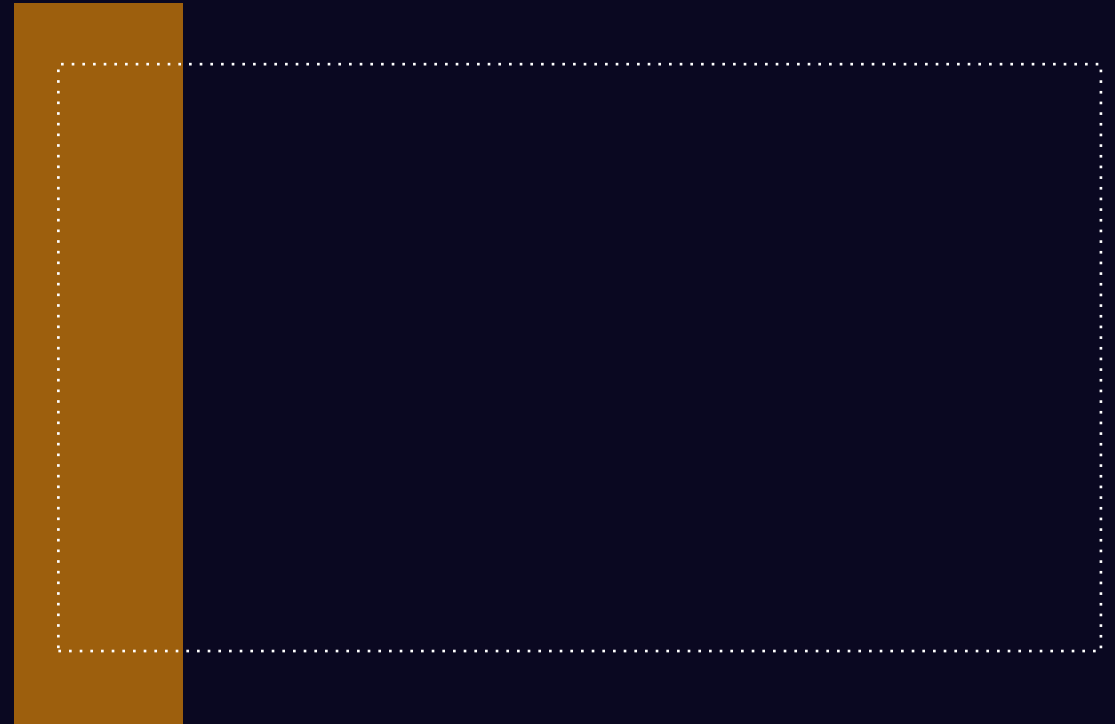
Documentação



**Conscientes da
Importância**



**Proteção contra
Engenharia Social**



Controle: Conscientização, Educação e Treinamento em Segurança da Informação



Objetivo:

Garantir que o pessoal e as partes interessadas relevantes estejam cientes e cumpram suas responsabilidades de segurança da informação.

Como, quando e por que usar a conscientização?

- Uma das medidas mais eficazes é um curso de conscientização de segurança quando estiver entrando no emprego;
- Pode ser parte do treinamento de admissão;
- Pode usar vários meios, como folhetos, mensagens em telas de computador, mousepads, boletins informativos, vídeos e cartazes;
- Diferentes conteúdos para diferentes públicos-alvo;
- Focados em ameaças específicas;
- Devem estar disponíveis para todos na organização.



Cuidados ao Evitar Vazamento de Informações



Cuidado com:

- Informações da empresa divulgadas em redes sociais, clubes, fórum, restaurantes etc.;
- Informação facilmente compartilhada em uma atmosfera relaxada;
- Engenharia social para extração de informações de uma vítima não voluntária.

Controle: Processo Disciplinar

Objetivo:



Garantir que o pessoal e outras partes interessadas relevantes entendam as consequências da violação da política de segurança da informação, para dissuadir e lidar adequadamente com o pessoal e outras partes interessadas relevantes que cometeram a violação.

Como usar um processo disciplinar?



- Um processo disciplinar é usado para quem viola a política de segurança da informação;
- Deve ser formalizado e comunicado com as partes interessadas relevantes;
- Garantir que entendam as consequências da violação da política de SI.

Considerações sobre o Processo Disciplinar

Considerações:

- O processo disciplinar não deve ser iniciado antes da coleta de provas;
- Se for demonstrado excelente comportamento, pode ser recompensado para:
 - ✓ Promover a segurança da informação;
 - ✓ Incentivar o bom comportamento.
- O processo disciplinar leva em consideração fatores como:
 - ✓ A natureza (quem, o quê, quando, como);
 - ✓ Gravidade da violação e suas consequências;
 - ✓ Se a ofensa foi intencional (dolosa) ou não intencional (acidental);
 - ✓ Se trata ou não de uma primeira infração ou reincidência;
 - ✓ Se o infrator foi ou não devidamente treinado.
- A resposta deve levar em consideração os requisitos legais, regulamentos etc.



Controle: Responsabilidades Após Rescisão ou Mudança de Emprego

Objetivo:



- Proteger os interesses da organização como parte do processo de mudança ou rescisão de contrato de trabalho.
- Visa a proteção do conhecimento;
- Processo que garante a revogação dos direitos quando alguém deixa a organização;
- Processo que garante a devolução de todos os ativos à organização.

Considerações: Responsabilidades Após Rescisão ou Mudança de Emprego

Considerações:

- Analise se as responsabilidades e deveres de segurança da informação devem permanecer válidos após a rescisão ou mudança de emprego;
- Pode incluir confidencialidade, propriedade intelectual e outros conhecimentos obtidos;
- O processo de rescisão ou mudança de emprego também deve ser aplicado ao pessoal externo (ou seja, fornecedores);
- Em muitas organizações, o RH geralmente é o responsável pelo processo geral de desligamento e trabalha em conjunto com o gerente supervisor da pessoa em transição;
- No caso da parte externa esse processo de rescisão é realizado pela parte externa de acordo com o contrato.



Controle: Contratos de Confidencialidade ou Não Divulgação



Objetivo:

Mantêm a confidencialidade das informações acessíveis ao pessoal ou a terceiros;

Como aplicar?

- São aplicáveis às partes interessadas e ao pessoal da organização;
- Para uma função que envolva confidencialidade, deve ter validade mesmo após o término do emprego;
- O gerente é responsável por documentar regras especiais para funções específicas;
- Em todos os casos, toda pessoa com função que envolva confidencialidade deve assinar um acordo de não divulgação (Non-Disclosure Agreement – NDA);
- Devem assinar antes de ter acesso a informações e outros ativos associados.



Controle: Contratos de Confidencialidade ou Não Divulgação

Como aplicar?

■ Leva-se em consideração:

- ✓ O tipo de informação que será tratada;
- ✓ Seu nível de classificação;
- ✓ Seu uso;
- ✓ O acesso permitido pela outra parte.



Em trabalhos que exigem confidencialidade, exige-se um NDA assinado



Controle: Trabalho Remoto



Objetivo:

Garantir a segurança das informações quando o pessoal estiver trabalhando remotamente.



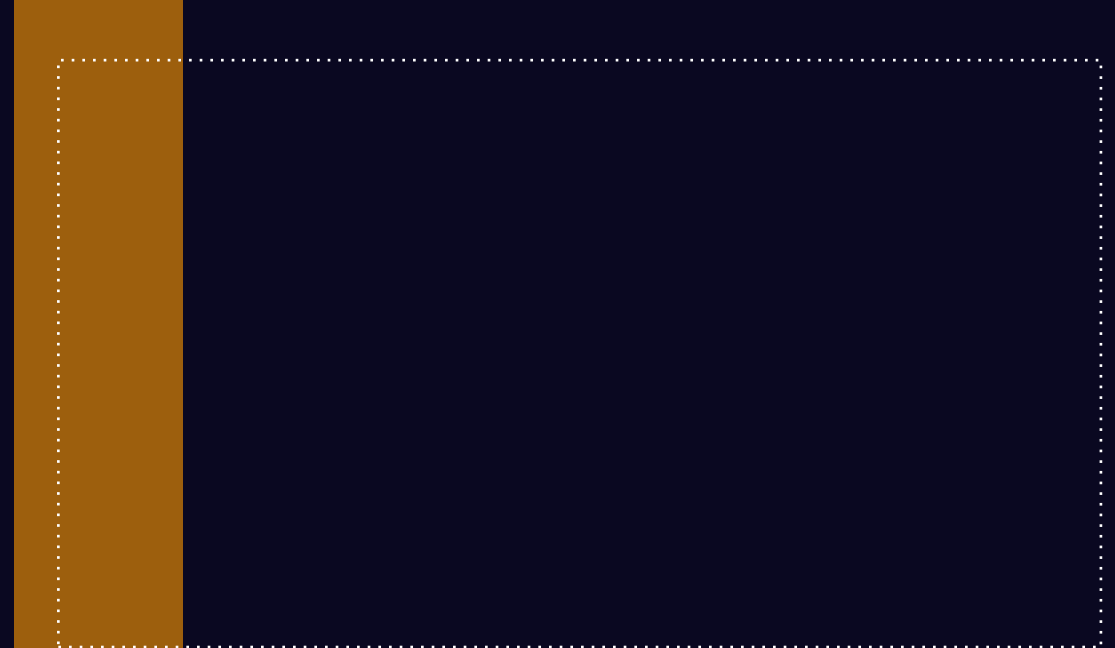
- Referido também como “teletrabalho”, “local de trabalho flexível”, “ambientes virtuais de trabalho” e “manutenção remota”.
- É possível que nem todas as recomendações possam ser aplicadas devido à legislação e regulamentos locais em diferentes jurisdições.
- Organizações que permitem atividades de trabalho remoto devem emitir uma política específica com tópicos sobre trabalho remoto.

Política de Trabalho Remoto

Emita uma política específica que contemple:



- Segurança física do local e do ambiente local;
- Regras e mecanismos de segurança para o ambiente físico remoto;
- Requisitos de segurança das comunicações;
- Uso de acesso remoto;
- Acesso não autorizado a informações por família e amigos, por exemplo;
- Uso de redes domésticas e redes públicas;
- Uso de medidas de segurança, como firewalls e proteção contra malware;
- Mecanismos seguros de autenticação.



Política de Trabalho Remoto

Emita uma política específica que contemple:

- Utilização de equipamento privado sob controle da organização;
- Classificação das informações que podem ser mantidas e acessadas;
- Contratação de seguros;
- Procedimentos de backup e continuidade de negócios;
- Auditoria e monitoramento de segurança;
- Revogação de autoridade, direitos de acesso e devolução de equipamentos quando encerrados os trabalhos.



Controle: Relatórios de Eventos de Segurança da Informação



Objetivo:

Apoiar relatórios de eventos de SI que possam ser identificados pelo pessoal;

O que esperar deste controle?

- A organização deve fornecer mecanismos para o pessoal relatar eventos de SI;
- Eventos suspeitos devem ser relatados o mais breve possível;
- Os eventos de SI incluem incidentes, violações e vulnerabilidades.



Controle: Relatórios de Eventos de Segurança da Informação

Relatórios de eventos de segurança da informação incluem:

- Controles ineficazes de segurança da informação;
- Violação da confidencialidade, integridade ou disponibilidade das informações;
- Erros humanos;
- Descumprimento da política de segurança da informação, outras políticas ou normas;
- Violação das medidas de segurança física;
- Alterações que não passaram pelo processo de gerenciamento de mudanças;
- Violações de acesso;
- Vulnerabilidades;
- Suspeita de infecção por malware.



OBRIGADO



**ISF – SEGURANÇA DA
INFORMAÇÃO EM
RECURSOS HUMANOS**