Aula 11 — Segurança em Recursos Humanos (RH)

1. O Fator Humano na Segurança da Informação

A segurança da informação não depende apenas de tecnologias avançadas, firewalls ou criptografia — ela depende, principalmente, de pessoas.

Estudos na área, como os abordados por Peixoto (2006), mostram que uma parcela significativa (estimativas geralmente apontam para mais de 70%) dos incidentes de segurança têm origem em falhas humanas, seja por descuido, desconhecimento ou má conduta.

1. O Fator Humano na Segurança da Informação

O papel da Segurança em Recursos Humanos (RH) é garantir que todos os colaboradores — internos, terceirizados ou prestadores de serviço — compreendam e pratiquem comportamentos seguros, alinhados à Política de Segurança da Informação (PSI) da organização.

Essa segurança deve acompanhar todo o ciclo de vínculo do colaborador:

- Antes da contratação
- Durante o vínculo
- Após o desligamento

Cada etapa exige controles e políticas específicas.

2. Segurança Antes da Contratação (Prevenção)

A prevenção começa antes mesmo de o colaborador iniciar suas atividades. O objetivo é minimizar o risco de empregar pessoas que possam comprometer a segurança organizacional.

Principais práticas:

- Verificação de antecedentes: Inclui checagem de histórico profissional, referências anteriores e, quando permitido pela legislação, antecedentes criminais.
- Análise de perfil de confiabilidade: Avalia a adequação do candidato a funções críticas, como acesso a informações sensíveis ou financeiras.

2. Segurança Antes da Contratação (Prevenção)

Principais práticas:

- Assinatura de termo de confidencialidade (NDA): Documento legal que formaliza o compromisso do colaborador com a proteção de informações sigilosas.
- Treinamento de integração (onboarding seguro): Introduz o novo colaborador à PSI da empresa, normas de conduta, canais de denúncia e práticas básicas de segurança digital.

Exemplo prático:

- Uma empresa de tecnologia exige que todo novo colaborador assista a um treinamento sobre boas práticas de senha e uso de dispositivos corporativos antes de receber acesso a qualquer sistema.

3. Segurança Durante o Vínculo (Conscientização e Controle)

Durante a relação de trabalho, é essencial garantir conscientização contínua, acessos controlados e auditoria de atividades.

Medidas principais:

- Treinamentos periódicos de conscientização: Devem abordar temas como engenharia social, phishing, políticas de senha e manuseio de dados pessoais.
- Segregação de funções: Evita que uma única pessoa tenha controle total de processos críticos, reduzindo o risco de fraude interna.
- Princípio do menor privilégio: Cada colaborador deve possuir apenas os acessos necessários para executar suas tarefas.

3. Segurança Durante o Vínculo (Conscientização e Controle)

Medidas principais:

- Monitoramento e auditoria: Registros de acesso, logs de sistemas e alertas ajudam a identificar comportamentos suspeitos.
- Papéis e responsabilidades claros: O colaborador precisa compreender seu papel na proteção da informação, sabendo o que é permitido e o que constitui violação.

Exemplo prático:

- Um analista de suporte técnico não deve ter acesso à base de dados de clientes, a menos que seja estritamente necessário para uma demanda autorizada.

4. Segurança Após o Desligamento (Revogação e Fechamento)

O processo de desligamento é uma fase crítica e, quando negligenciada, pode resultar em vazamentos de dados e perdas financeiras.

Ações essenciais:

- Revogação imediata de acessos: Desativação de contas em sistemas, e-mail corporativo, redes internas e VPNs.
- Devolução de ativos: Recolher notebooks, tokens, crachás, pendrives e quaisquer equipamentos corporativos.

4. Segurança Após o Desligamento (Revogação e Fechamento)

Ações essenciais:

- Assinatura de termo de desligamento seguro: Reforça o compromisso com a confidencialidade mesmo após o fim do contrato.
- Comunicação interna eficiente: As áreas de TI, segurança e gestão de pessoas devem ser notificadas simultaneamente sobre o desligamento.

Exemplo prático:

- Um colaborador com acesso a informações financeiras é desligado e seu acesso ao sistema ERP é bloqueado imediatamente pela equipe de TI — evitando risco de manipulação de dados.

5. Cultura Organizacional e Conscientização em Segurança

A segurança da informação não depende apenas de políticas ou tecnologias: ela é sustentada por uma cultura organizacional voltada à segurança, onde todos — da alta direção aos estagiários — compreendem seu papel na proteção de ativos e dados.

Segundo Whitman e Mattord (2021), a cultura de segurança é construída quando os valores da organização estão alinhados com práticas seguras, e quando o comportamento ético é reforçado por treinamento, comunicação e exemplo da liderança.

5.1. Conscientização e Educação Contínua

A conscientização em segurança da informação é um processo contínuo de educação dos colaboradores sobre riscos e boas práticas.

- De acordo com a ISO/IEC 27002 (2022), programas de treinamento devem ser atualizados regularmente e adaptados à função e ao nível de acesso de cada colaborador.
- Segundo Peixoto (2006), ações educativas reduzem drasticamente a eficácia de golpes de engenharia social, pois tornam o colaborador um elo de defesa — e não uma vulnerabilidade.

5.2. Liderança e Responsabilidade Compartilhada

A cultura de segurança deve ser promovida de cima para baixo (“top-down”).

- A ISO/IEC 27001 (2022) reforça que o comprometimento da direção é essencial para o sucesso do Sistema de Gestão da Segurança da Informação (SGSI), devendo incluir o apoio à definição de políticas e a garantia de recursos.
- O NIST SP 800-50 (2003) recomenda que a conscientização não seja apenas punitiva, mas motivacional, reforçando atitudes seguras e a cooperação entre departamentos.

6. Aspectos Legais e Éticos

A segurança em RH não é apenas uma boa prática — é também uma exigência legal e ética que permeia o ciclo de vida do colaborador.

- LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018): Determina que todos os colaboradores devem tratar dados pessoais de clientes e usuários de forma responsável e segura.
- CLT e Normas Trabalhistas: O empregador deve garantir um ambiente de trabalho seguro, inclusive em termos de informação e privacidade.
- Ética profissional: A integridade e o sigilo são pilares da reputação corporativa.
- Responsabilidade civil e criminal: Em casos de vazamento intencional, fraude ou espionagem corporativa, o colaborador pode ser responsabilizado judicialmente.

7. Exemplos Reais de Falhas Humanas

Tipo de Falha	**Consequência**	**Prevenção**
Phishing – funcionário clicou em *e-mail* falso	Invasor obteve acesso ao *e-mail* corporativo	Treinamentos e simulações de *phishing*
Senha compartilhada em planilha	Vazamento de dados confidenciais	Política de senhas e autenticação multifator
Cópia de base de clientes antes do desligamento	Perda de vantagem competitiva	Revogação imediata de acessos e cláusulas contratuais
Técnico desligou servidor crítico sem autorização	Indisponibilidade de serviços	Procedimentos padronizados e dupla verificação

8. Atividade em Grupo

Desafio: Simular um processo completo de segurança em Recursos Humanos para uma empresa fictícia.

Tarefas:

- 1. Elaborar um checklist de segurança antes da contratação.
- 2. Criar exemplos de políticas de segurança durante o vínculo (com foco em cultura).
- 3. Definir um plano de desligamento seguro, com etapas e responsáveis.
- 4. Discutir os riscos e impactos caso alguma dessas etapas seja ignorada.

Objetivo: Compreender como práticas de segurança se integram à gestão de pessoas, reduzindo vulnerabilidades organizacionais.