Prof. esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp

- **Professor (contratado):**
- **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor (Efetivado):**
- **Graduação:** Todo núcleo de T.I. - Wyden Facimp
- **Tech Lead na Motoca Systems**

Redes sociais:

- **Linkedin:** https://www.linkedin.com/in/thalles-canela/
- **YouTube:** https://www.youtube.com/aXR6CyberSecurity
- **Facebook:** https://www.facebook.com/axr6PenTest
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** https://github.com/ThallesCanela
- **Github:** https://github.com/aXR6
- **Twitter:** https://twitter.com/Axr6S

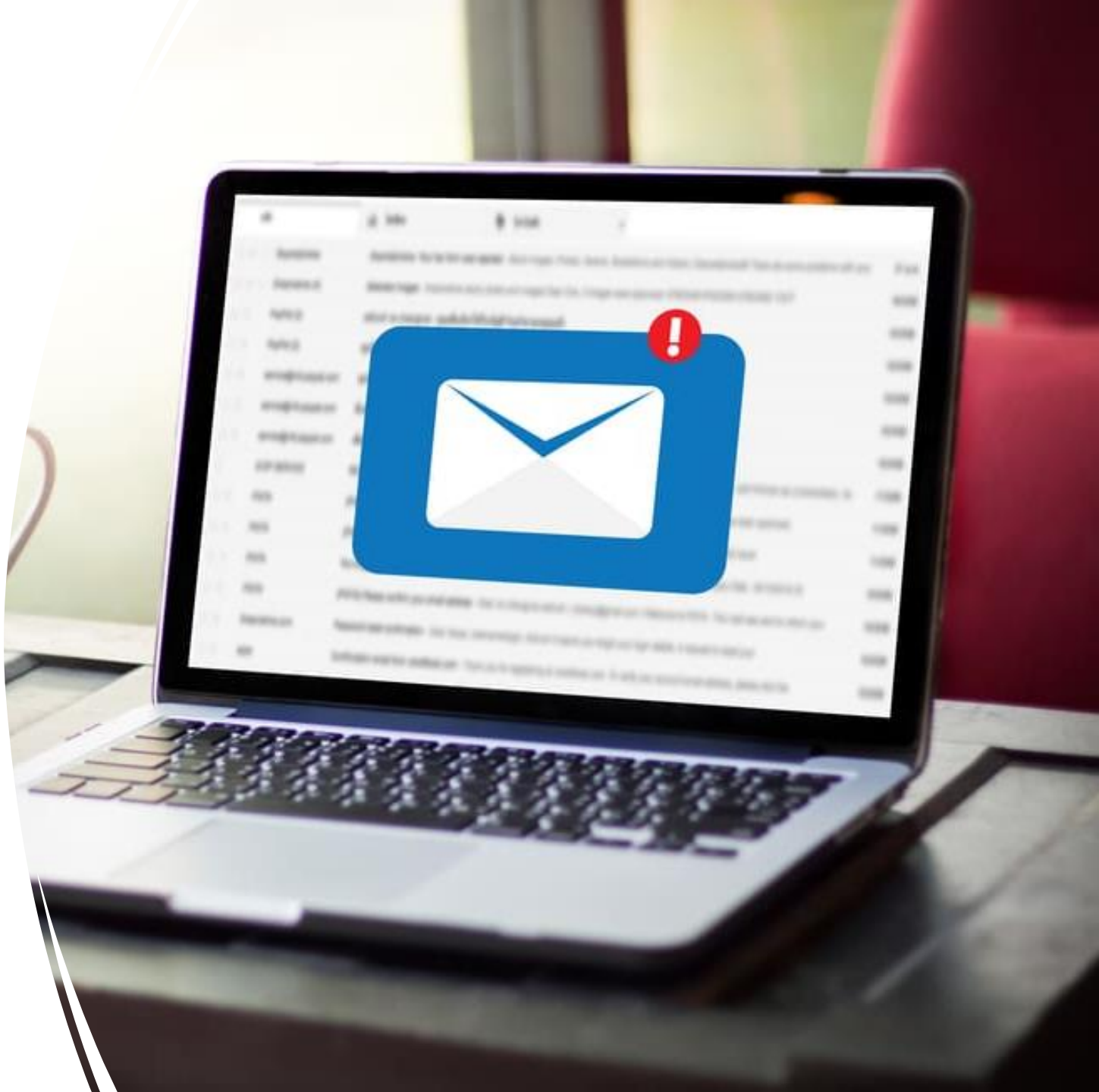
INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

NORMAS DE SEGURANÇA AMEAÇAS E VULNERABILIDADES

Compreendendo o problema

- **Situação:** você deixou seu programa de e-mail aberto, e alguém clicou em um link de uma mensagem estranha que estava em sua caixa de entrada.

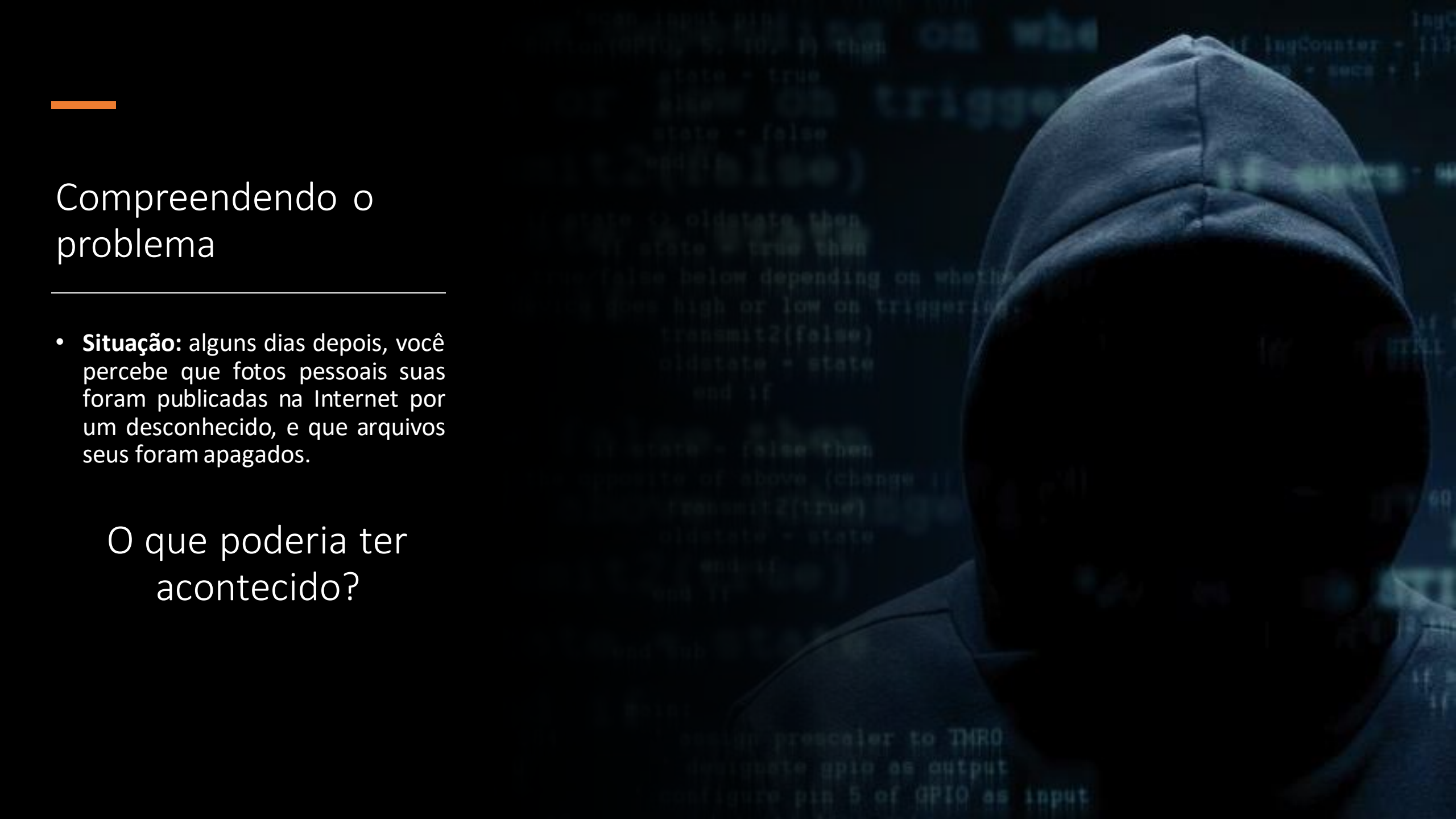
Qual a gravidade disso?



Compreendendo o problema

- **Situação:** alguns dias depois, você percebe que fotos pessoais suas foram publicadas na Internet por um desconhecido, e que arquivos seus foram apagados.

O que poderia ter acontecido?



Compreendendo o problema

- **Situação:** alguns dias depois, você percebe que fotos pessoais suas foram publicadas na Internet por um desconhecido, e que arquivos seus foram apagados.

Como proceder?

Prisão por Furto de Fotos

G1 RIO DE JANEIRO

/12 23h18 - Atualizado em 14/05/2012 10h11

uspeitos do roubo das fotos de Carolina Dieckmann são descobertos

Roubo foi feito por hackers do interior de Minas e São Paulo, via e-mail. O Fantástico acompanhou com exclusividade a investigação.

Do G1, com informações do Fantástico

FACEBOOK

A polícia encontrou quatro suspeitos de terem roubado fotos íntimas do computador de Carolina Dieckmann em março e depois as terem divulgado na internet, em 7 de maio, após tentativa de extorsão. De acordo com a investigação, acompanhada de perto com exclusividade pelo Fantástico neste domingo (13), hackers do interior de Minas Gerais e São Paulo invadiram o e-mail da atriz e pegaram as imagens. Isso descarta a suspeita inicial sobre funcionários de uma

ssistência técnica no Rio de Janeiro onde Dieckmann havia deixado o laptop para

Objetivos

- Tomar contato com as normas e as leis brasileiras de segurança.
- Compreender os conceitos de risco, ameaça, vulnerabilidade e desastre
- Compreender como lidar com os riscos de segurança na empresa

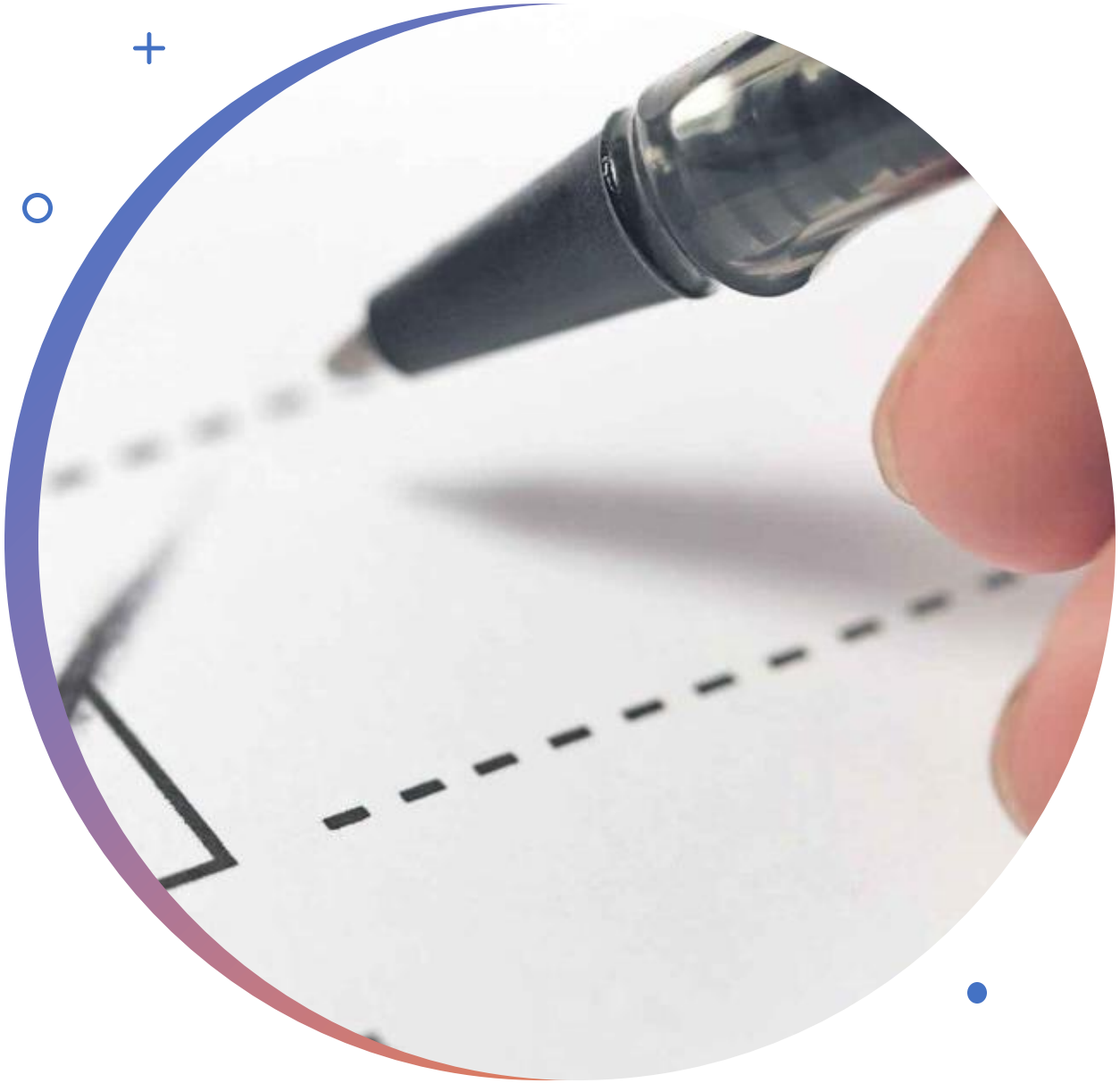
IMPORTÂNCIA DA INFORMAÇÃO

Importância da Informação

- Informações são um ativo da empresa
  - Devem ser protegidas!
    - Garantir continuidade dos negócios
    - Maximizar o retorno de investimentos/oportunidades
    - Minimizar transtornos.

Informação é Essencial

- O mundo mudou muito nas últimas décadas
  - Documentos e processos são digitais: nuvem
  - Todos os dispositivos “sempre online”!



Como proteger a informação?

- Guias gerais
  - Normas
  - Leis

- Cada empresa refina:
  - Política de Segurança da Informação
  - Plano de Continuidade de Negócios
  - Plano de Contingências

NOÇÕES:

- NORMAS NBR ISO/IEC 27001
- E ISO/IEC 27002

Norma ISO/IEC 17799:2005

- Diretrizes e princípios para melhorar...
  - Gestão de Segurança da Informação da empresa
  - Internacionalização da BS 7799.
- Objetivo:
  - Controles a implementar em função de...
  - requisitos levantados em uma Análise de Risco.
- Norma pode servir como um guia prático
  - Desenvolvimento dos procedimentos de segurança
  - E a elaboração de políticas
- Foi incorporada à ISO/IEC 27002.

Norma ISO/IEC 27002

- Código de Prática para a GSI
  - Gestão de Segurança da Informação
- Objetivo
  - Estabelecer diretrizes e princípios iniciais para:
    - Iniciar, implementar e melhorar a GSI da organização
  - Ou seja: proteger informações importantes...
    - para a continuidade dos negócios.

Norma ISO/IEC 27002 - Tópicos

- Política de Segurança da Informação
  - Formalizada em documento e comunicada claramente; deve ser revisada periodicamente
- Organizando a Segurança da Informação
  - Deve haver uma estrutura gerencial envolvendo representantes estratégicos de diversas áreas. Importante estabelecer acordos de sigilo.
- Gestão de Ativos
  - Manter e proteger ativos – identificar, classificar, catalogar etc. de maneira estruturada.

Norma ISO/IEC 27002 - Tópicos

- Política de Segurança da Informação
  - Formalizada em documento e comunicada claramente; deve ser revisada periodicamente
- Organizando a Segurança da Informação
  - Deve haver uma estrutura gerencial envolvendo representantes estratégicos de diversas áreas. Importante estabelecer acordos de sigilo.
- Gestão de Ativos
  - Manter e proteger ativos – identificar, classificar, catalogar etc. de maneira estruturada.

Norma ISO/IEC 27002 - Tópicos

- Segurança em Recursos Humanos
  - Descrições de cargos e termos de contratação devem ser explícitos no que tange às responsabilidades de Segurança da Informação.
  - Candidatos: análise minuciosa!
    - Especial: manuseio de informações sigilosas.
  - Todos: estar cientes das ameaças
    - E de suas responsabilidades e obrigações.
- Segurança Física e do Ambiente
  - Controle rigoroso, com proteção de equipamentos

Norma ISO/IEC 27002 - Tópicos

- Gestão das Operações e Comunicações
  - Procedimentos e responsabilidades operacionais
  - Diretrizes para gerenciamento de terceirizados
  - Diretrizes para segurança em redes e comunicações
- Controles de Acessos
  - Mecanismos do controle e responsabilização
  - Aspectos sobre computação móvel e teletrabalho
  - Passam por políticas e gerenciamento de privilégios

Norma ISO/IEC 27002 - Tópicos

- Aquisição, Desesenv. e Manut. de Sist. de Infor.
  - Definição de requisitos para aplicações
  - Uso de controles criptográficos
  - Diretrizes de segurança de arquivos e desenvolv.
- Gestão de Incidentes de Segurança da Inform.
  - Gestão e comunicação de fragilidades
  - Coleta de evidências e mecanismos de análise

Norma ISO/IEC 27002 - Tópicos

- Gestão da Continuidade do Negócio
  - Diretrizes para prevenir interrupção do negócio
  - Recuperação e retomada em tempo mínimo
- Conformidade
  - Orientações para evitar violações legais
  - Diretrizes para identificar a legislação vigente:
    - Proteção de registros e direitos de P.I.
    - Proteção de dados e inform. pessoais
    - Prevenção de mau uso dos recursos
    - Regulamentação de criptografia

Norma ISO/IEC 27001

- Requisitos para um SGSI
  - Sistema de Gestão de Segurança da Informação
  - Compatível com ISO 9001:2000 e ISO 14001:2004
- Em que se baseia um SGSI?
  - Abordagem de riscos de negócio
- Norma: sugere abordagem de processos
  - Identificar e gerenciar os processos do SGSI
- Ciclo PDCA
  - Plan, Do, Check, Act

Norma ISO/IEC 27001

Ciclo PDCA na implantação do SGSI

Norma ISO/IEC 27001

- Objetivo: requisitos para quê?
  - Estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria de um SGSI
- Se aplicam a que tipo de empresas?
  - Quaisquer, independente de tipo, tamanho ou natureza
- Ajuda a proteger ativos de informação
- Única norma auditável para esse fim

Norma ISO/IEC 27001

- Significado da Certificação
  - Requisitos de governança e continuidade de negócios são atendidos
  - Leis e regulamentos aplicáveis são observados
  - Segurança da informação é de suma importância
  - Riscos são corretamente identificados, avaliados e gerenciados
  - Comprometimento da alta gestão
  - Auditorias regulares: melhoria contínua

ASPECTOS LEGAIS

Leis Envolvendo Redes e Segurança

- Três são especificamente relevantes:
  - Lei Carolina Dieckman
    - Lei Federal 12.737 de 30 de Novembro de 2012
    - Tipificação criminal
    - http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
  - Marco Civil da Internet
  - Lei Geral de Proteção de Dados (LGPD)

Marco Civil da Internet

- Lei Federal 12.965 de 24 de Abril de 2014
- Uso da Internet
  - Essencial ao exercício da cidadania
- Delimita direitos e deveres
  - Liberdade de expressão
  - Privacidade
  - Direitos do consumidor
  - Livre concorrência

Marco Civil da Internet

- Exemplos de pontos relevantes:
  - Neutralidade da Rede
  - Privacidade
    - Registros de acesso de controle: conexão e aplicação
      - Data, hora, quem, IP.
      - Aplicação: só por seu fornecedor!
  - Responsabilizar autores do conteúdo
    - Provedor de conexão?
    - Provedor de aplicação: fornece espaço x publica conteúdo
- **Não aborda:** Tipificação criminal e direitos autorais

Lei Geral de Proteção de Dados

- Lei Federal 13.709 de 2018
  - Unifica diversas leis especiais
  - Influenciada pela GDPR Europeia
  - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm
- Regula o tratamento de dados pessoais
  - Nome, RG, CPF, profissão, escolaridade etc...
  - Toda operação realizada com dados pessoais
    - Dados coletados ou tratados no Brasil
    - Ou com propósito de aplicação do Brasil

Lei Geral de Proteção de Dados

- Conceito de dado sensível
  - Pode ocasionar vulnerabilidade ou discriminação

"dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"

- Exemplificativo, não taxativo

Lei Geral de Proteção de Dados

- A quem se aplica?
  - Pessoas jurídicas (público ou privado)
  - Pessoas físicas: com uso não particular ou com finalidade econômica
- Proteger privacidade dos usuários
  - Regras claras sobre dados
    - Como coletar, armazenar e compartilhar
  - Exige consentimento explícito do titular
    - Consentimento específico para o uso que se pretende
    - Pode ser revogado a qualquer tempo

Lei Geral de Proteção de Dados

- Palavra-chave: Transparência
- Cuidados exigidos:
  - Conhecer os dados que coleta
  - Gerenciar as informações: quem acessa?
  - Utilizar medidas de segurança corretas
  - Documentas os dados coletados
  - Manter-se atualizado.
- Fiscalização: ANPD
  - Autoridade Nacional de Proteção de Dados

O CERT.BR

CERT.BR

- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  - Mantido pelo NIC.Br
  - Do Comitê Gestor da Internet no Brasil (CGI.Br)
  - https://cert.br/
- Missão
  - Aumentar os níveis de segurança...
  - E de capacidade de tratamento de incidentes...
  - Das redes conectadas à internet no Brasil.

CERT.BR

- Público
- Qualquer rede que use recursos administrados pelo NIC.br (endereços IP, por exemplo) no Brasil
- Oferece apoio para CSIRTs
  - Computer Security Incident Reponse Team
    - Grupos de Reposta a Incidentes de Segurança
  - Serviços, cursos, documentação...
- É um CSIRT de último recurso
  - Quando não se sabe quem contatar

DISCUSSÃO DE CASO PRÁTICO

Compreendendo o problema

- **Situação:** Uma grande empresa contratou uma empresa especializada em espionagem industrial para obter informações sobre seus concorrentes. O crime foi descoberto porque um dos detetives foi encontrado revirando lixo de uma das concorrentes.

Como se proteger disso?

PREMISSAS BÁSICAS :

- DEFININDO E PRIORIZANDO AÇÕES DE SEGURANÇA

Ameaça, vulnerabilidade e desastre

- Conceitos via exemplos
  - Ameaças
  - Existência de potenciais invasores com interesse nas informações que mantemos
  - Funcionários insatisfeitos com acesso ao banco de dados
- Vulnerabilidades
  - Uma versão antiga de webserver com falha conhecida
  - Código PHP mal elaborado que permita injection
- Desastres
  - Furto de informações confidenciais do banco de dados
  - Deleção do banco de dados como um todo

Terminologia

- Ameaça
  - Circunstância, ação ou evento que pode levar à quebra de segurança
- Vulnerabilidade
  - Fragilidade nos ativos que os expõem a ameaças
- Incidente ou ataque
  - Uma tentativa ou sucesso de uma ameaça em explorar uma vulnerabilidade
- Desastre
  - Resultado do sucesso de um ataque
- E risco?

O que é Risco?

- Risco é uma probabilidade de...
  - Ameaças e vulnerabilidades...
  - Levarem a desastres
- Em geral, define-se risco como:
  - $risco = ameaças \,.\, vulnerabilidades$
- Em outras palavras...
  - Se não houvesse ameaças ou vulnerabilidades...
  - ... Não haveria riscos.
- Em segurança da informação...
  - O risco considera a magnitude do desastre

Determinação do Risco

- Avaliar:
  - A possibilidade de exploração da vulnerabilidade
  - O impacto ao negócio devido a evento adverso
  - Efetividade de controles para reduzir os riscos.
- Tabela conforme ABNT (notas 0 a 8)

	PROBABILIDADE DO CENÁRIO DE INCIDENTE	MUITO BAIXA (MUITO IMPROVÁVEL)	BAIXA (IMPROVÁVEL)	MÉDIA (POSSÍVEL)	ALTA (PROVÁVEL)	MUITO ALTA (FREQUENTE)
IMPACTO NO NEGÓCIO	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Inevitabilidade dos Riscos

- Riscos são inevitáveis
  - Investidores comprando ações
  - Cirurgiões realizando operações
  - Engenheiros projetando pontes
  - Empresários abrindo negócios
  - Etc...
- Mas gerenciá-los é estratégico!
  - Já que não temos como eliminá-los totalmente...
  - Precisamos lidar com eles!

LIDANDO COM RISCOS

Abordagens de Segurança

- Há dois tipos principais de abordagem:
  - Reativa
  - Proativa

Abordagem Reativa

- Agir quando ocorre um incidente
  - Sempre que ocorrer um incidente...
  - Verificar e agir para não voltar a acontecer
- Envolve:
  - Auditoria
  - Análise e pesquisa
  - Documentação
  - Implementação de medidas.

Abordagem Proativa

- Agir para que não haja incidentes
  - Prática diária, agir antes de acontecer
  - Para evitar que incidentes venham a acontecer
- Envolve:
  - Pesquisa de falhas
  - Análise de logs
  - Documentação
  - Implementação de medidas

Abordagens de Segurança

- Há dois tipos principais de abordagem:
  - Reativa
  - Proativa
- Não são excludentes!
- Ambas: mitigação de riscos futuros
  - Proativa é efetiva também para o presente
  - Reativa “pura” tende a ser mais cara
  - Ao menos no longo prazo!

Lidar com os Riscos

- Mitigar?
- É impraticável eliminar os riscos...
  - Priorizar... em função de quê?
  - Custos.
- Objetivo geral:
  - Implementar controles para...
  - Reduzir os riscos a nível aceitável...
  - Com mínimo impacto sobre os recursos e metas
- Significa que vamos aceitar riscos?

Aceitação de Riscos

- Há custos para mitigar riscos
- Há custos por eventuais desastres
- E se mitigar for mais caro que o desastre?
  - Podemos aceitar o risco!
- Custo “certo” x custo “duvidoso”
  - Mais fácil aceitar riscos baixos: custo “duvidoso”

	PROBABILIDADE DO CENÁRIO DE INCIDENTE	MUITO BAIXA (MUITO IMPROVÁVEL)	BAIXA (IMPROVÁVEL)	MÉDIA (POSSÍVEL)	ALTA (PROVÁVEL)	MUITO ALTA (FREQUENTE)
IMPACTO NO NEGÓCIO	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Mitigação de Riscos

- Etapas
  - Priorizar
  - Analisar
  - Avaliar
  - Implementar controles.

"Isso se aplica inclusive a projetos de software! Prazos, Resultados!"

Atividade

- Grupos – 15 minutos
  - Conforme canais do Teams
- Leia o caso que tem o mesmo número de seu grupo, do texto disponível em: https://tinyurl.com/23vserhb
- Discuta com seu grupo e identifique UMA medida que o grupo considera que seria a mais eficaz para prevenir o problema
- Quando chegar a vez do grupo, explique a ocorrência e a medida levantada.