RGM
TECNOLOGIA

Workshop LGPD

Como gerenciar o nível de Confiabilidade dos ativos de informação (CID da Informação)

Agenda

- Incidentes de segurança da informação
- Confiabilidade da informação
- Os padrões e boas práticas

RGM
TECNOLOGIA

Adilson Taub Junior

CIO/CTO
DPO certified

20+ years of experience, helping companies solve problems with the right tools

Contatos

/in/ataubjr/

adilsontj@rgm.com.br

Acadêmico

Master of Business Administration (MBA)
Gestão Estratégica de Negócios

Formação Executiva
Compliance Empresarial (FGV)

Pós-graduação
Engenharia de Software

Graduação
Processamento de Dados

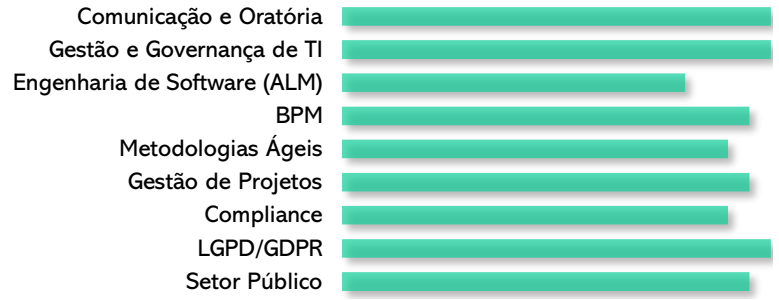
Certificações

Privacy & Security Management
Data Protection Officer (DPO)
Privacy and Data Protection Practitioner
Privacy and Data Protection Foundation
Information Security (ISO/IEC 27.001)

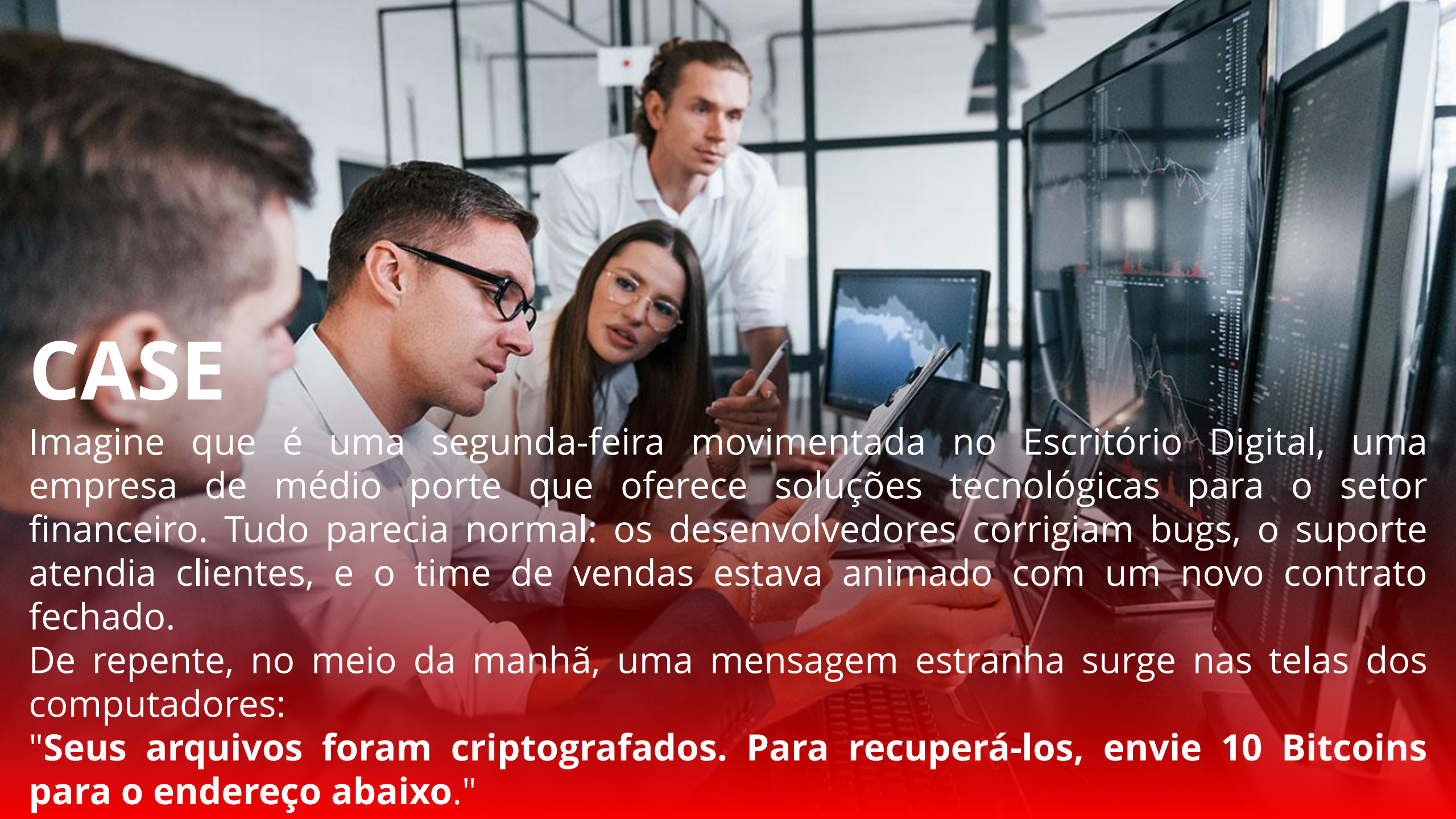
IT Governance and Service Management
IT Service Management (ISO/IEC 20.000)
ITIL V3 Fdn. Certified
COBIT 4.1 Fdn. Certified
ITIL V2 Fdn. Certified

Software Engineering
Professional Scrum Product Owner (PSPO I)
Professional Scrum Master (PSM I)
Certified Scrum Professional
Certified ScrumMaster
Kanban Foundation KIKF
IBM Certified Solution Designer (RUP)
Certified Expert in BPM

Mapa de habilidades




ALERTA



CASE

Imagine que é uma segunda-feira movimentada no Escritório Digital, uma empresa de médio porte que oferece soluções tecnológicas para o setor financeiro. Tudo parecia normal: os desenvolvedores corrigiam bugs, o suporte atendia clientes, e o time de vendas estava animado com um novo contrato fechado.

De repente, no meio da manhã, uma mensagem estranha surge nas telas dos computadores:

"**Seus arquivos foram criptografados. Para recuperá-los, envie 10 Bitcoins para o endereço abaixo**."

CAOS!

Em questão de minutos:

- Todos os arquivos dos servidores estavam inacessíveis, incluindo contratos com clientes e dados financeiros;
- O sistema de atendimento parou completamente, deixando clientes irritados;
- Um backup recente que poderia salvar a situação? Também estava comprometido.

A empresa foi vítima de um ataque de **ransomware**. E agora, sem acesso às suas informações críticas, cada minuto parado custa **milhares de reais.**

O que são incidentes de segurança da informação

De acordo com a literatura

- Um incidente de segurança da informação é um único evento ou uma série de eventos indesejados ou inesperados que têm uma probabilidade significativa de comprometer as operações de negócios e ameaçar a segurança das informações.

(ISO/IEC 27035-1:2016)

- Um incidente de segurança da informação é a violação de uma política de segurança explícita ou implícita, como acesso não autorizado, uso indevido de sistemas ou interrupções intencionais na disponibilidade de serviços.

(NIST SP 800-61 Rev. 2)

Podemos então definir...

- Incidentes de segurança da informação são eventos ou ações que comprometem a confidencialidade, integridade ou disponibilidade de informações ou sistemas de uma organização. Esses incidentes podem ocorrer devido a ataques maliciosos (como invasões e malware), falhas técnicas, erros humanos, ou desastres naturais, e geralmente representam uma violação das políticas ou medidas de segurança estabelecidas.

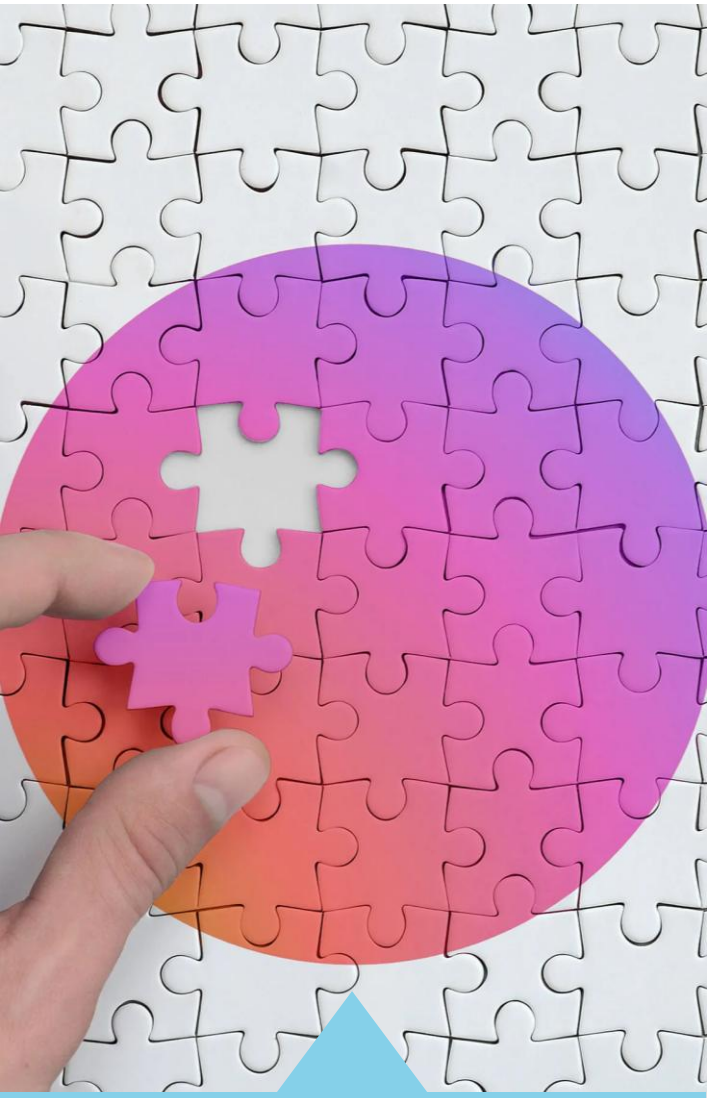
- *Exemplos:*
  - Acesso não autorizado a dados
  - Roubo ou perda de dispositivos contendo informações sensíveis.
  - Divulgação acidental de informações confidenciais.
  - Ataques de ransomware ou negação de serviço (DDoS)

RGM TECNOLOGIA

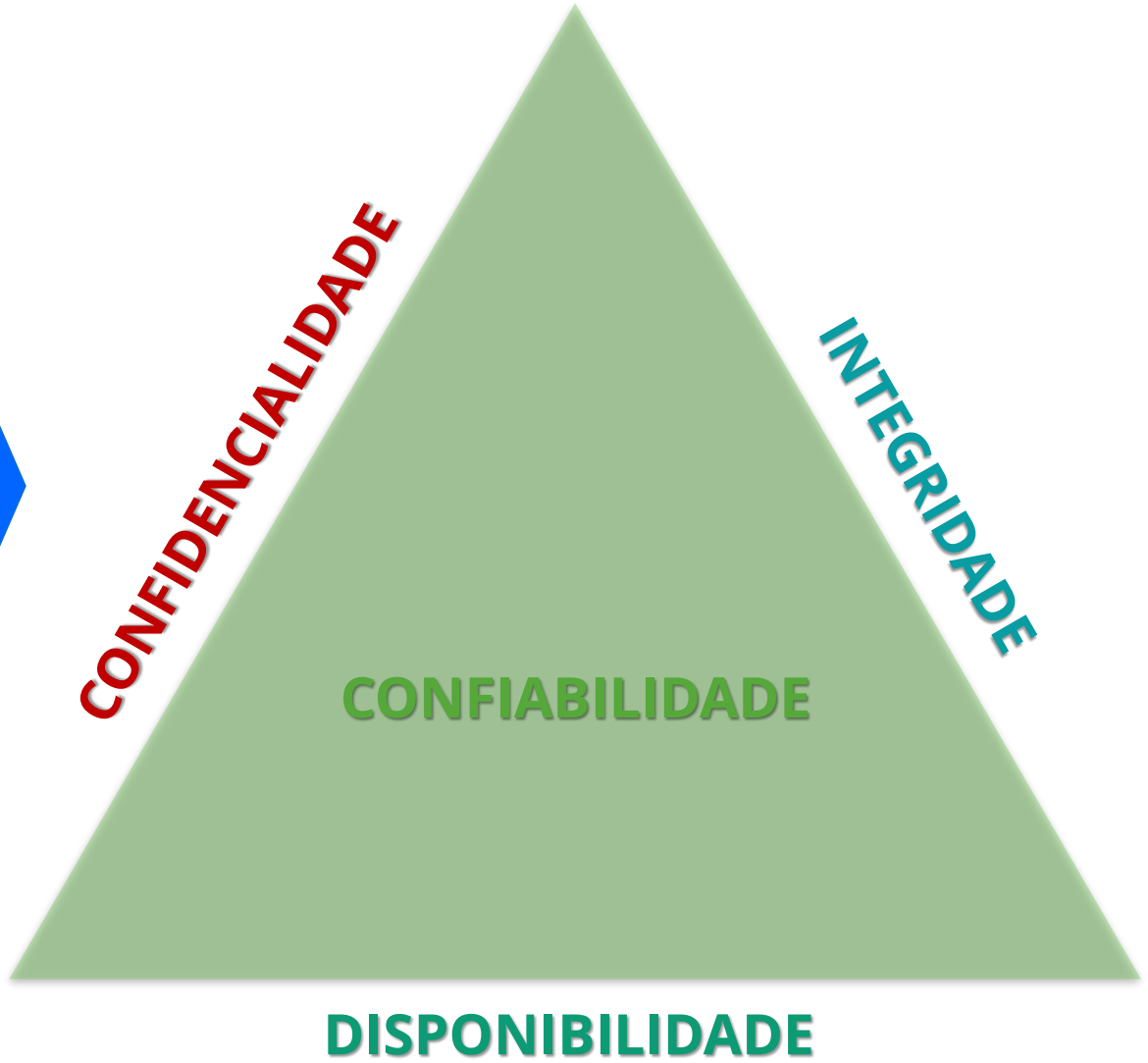
A PRIVACIDADE E A PROTEÇÃO DE DADOS

RGM
TECNOLOGIA

O TRIÂNGULO DA CID (CIA TRIAD)



As melhores práticas de mercado estabelecem a formação da confiabilidade da informação como um triângulo



Medidas de segurança por parâmetro

Medidas de **Confidencialidade**

- Criptografia de dados
- Estrito controle de acesso físico e lógico: *Assegurar o nível de acesso apropriado e somente para as pessoas autorizadas*
- Classificação de dados: *Definir a que público os dados podem ser comunicados (Públicos? Sensíveis? Confidenciais?)*
- Treinamento de pessoal
- Segregação de funções: *Evitar que funções conflitantes sejam executadas pela mesma pessoa*
- Política de "mesa limpa"

Sigilo

Medidas de **Integridade**

- Padronizar caminho de acesso: *Por exemplo, não permitir atualização de dados "diretamente na Base de Dados"*
- Gravação de logs de usuários: *Garantir que possa ser determinado quem modificou a informação*
- Segregação de Função, posições e autoridade: *Ao menos duas pessoas serão necessárias para realizar mudanças que tenham graves consequências*
- Mudanças em sistemas e dados devem ser são autorizadas
- Padronizar terminologia: *Por exemplo, um incidente é sempre chamado de "incidente", logo, o termo "chamado" não pode ser inserido na base de dados*

Exatidão

Medidas de **Disponibilidade**

- Implementação de uma robusta solução de *backup* e *restore*
- Realizar rotinas de teste de restauração de ambientes
- Políticas de armazenamento gerenciado de dados: *Por exemplo, não permitir o armazenamento de dados em máquinas pessoais, dar preferência a sistemas de armazenamento centralizados, como servidores em rede interna ou cloud*
- Implementação do Gerenciamento de Disponibilidade da ITIL

Prontidão

RGM TECNOLOGIA

Ativos de informação

- O uso e o processamento de informações acontece sempre se fazendo uso de um ATIVO DE INFORMAÇÃO.
- ATIVOS DE INFORMAÇÃO são tudo o que possui valor para uma organização e é onde fazemos uso de dados
  - Ativos eletrônicos: Softwares, Aplicativos, Sistemas
  - Ativos físicos: Armários, Hardware
- As medidas técnicas de segurança são sempre implementadas nos ATIVOS DE INFORMAÇÃO, visando maximizar o nível de CONFIABILIDADE desses ativos.

RGM TECNOLOGIA

Os padrões e boas práticas de segurança da informação

RGM TECNOLOGIA

Norma ISO/IEC 27.001

- **Propósito**
  - Estabelecer os requisitos para implementar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).
- **Escopo**

  Define os requisitos gerais para a gestão da segurança da informação, incluindo:
  - Análise de contexto
  - Gerenciamento de riscos
  - Definição de políticas
  - Planejamento e implementação de controles
  - Monitoramento e melhoria contínua
- **Foco**
  - Norma certificável
  - Orienta o "o que" deve ser feito para implementar um SGSI eficaz.

RGM TECNOLOGIA

Norma ISO/IEC 27.002

- **Propósito**
  - Fornecer diretrizes detalhadas para implementar os controles de segurança da informação mencionados no Anexo A da ISO 27001.
- **Escopo**

  Apresenta controles de segurança organizacionais, físicos, tecnológicos e humanos, agrupados em categorias como:
  - Controle de acesso
  - Gestão de ativos
  - Segurança física e ambiental
  - Gestão de incidentes
- **Foco**
  - Norma não-certificável, mas apoia na certificação ISO 27.001
  - Explica o "como" implementar os controles recomendados.

RGM TECNOLOGIA

Framework NIST CSF

- **Propósito**
  - O NIST Cybersecurity Framework (CSF) É um conjunto de diretrizes flexíveis para melhorar a segurança cibernética, criado para ser aplicável a organizações de qualquer porte e setor.
- **Escopo**

  Estabelece critérios e boas práticas para 5 funções de segurança:
  - **Identify**: Identificação de ativos e riscos (contexto organizacional)
  - **Protect**: Implementação de controles para proteger ativos e serviços
  - **Detect**: Monitoramento para identificar eventos de segurança
  - **Respond**: Respostas a incidentes de segurança
  - **Recover**: Planejamento de recuperação e resiliência após incidentes
- **Foco**
  - Apoia na definição de controles, orientando o "o que" fazer

RGM TECNOLOGIA

Modelo de planilha da CID

Demonstração prática

RGM
TECNOLOGIA

Obrigado!

Adilson Taub Jr.

https://www.linkedin.com/in/ataubjr/

RGM Tecnologia

www.rgm.com.br

SCAN ME