# Cultura Organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

MONACO
PALESTRANTE

monaco
Coaching em Governança de TI

PRISMA
SECURITY

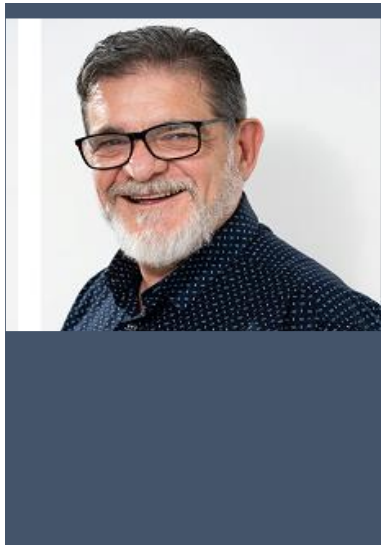
HÉLIO ABREU
helioabreu.adv.br
(41) 9 9976-1166

Atualizado em:
13/07/2023

ISO 27001:2022

ISO 27002:2022

ISO 27005:2018



# CURRÍCULO RESUMIDO

## Wellington Antonio Monaco

- ❑ **Chief Compliance Officer | Head de Governança de Privacidade e Proteção de Dados**
- ❑ **Palestrante | Coaching & Instrutor – Governança Corporativa, Governança de TI e Governança de Privacidade - EXIN DPO**

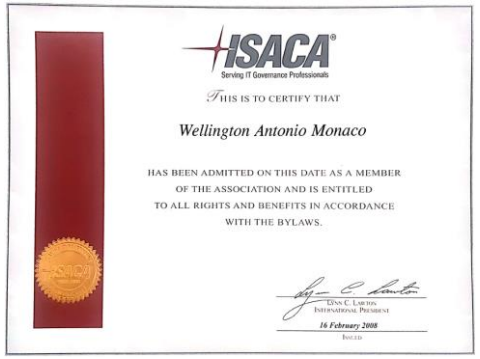
- Compliance e Governança Corporativa
- Jornada de Adequação e de Sustentação à LGPD
- Implementação de Soluções de Segurança da Informação
- Implementação de Gerenciamento e Tratamento de Incidentes de Segurança da Informação.
- Implementação da Privacidade desde a Concepção e Privacidade por Padrão
- Auditor Interno - ISO 27001
- Diretor de Serviços Gerenciados e Central de Serviços Compartilhados:

- Implementação de Serviços Gerenciados nos cliente no foco de Redução de Custo e Melhoria de Desempenho
- Operacional.
- Consultor Estratégico em Governança de TI e Governança Corporativa

- FASP | Bacharel em Administração de Empresas e Analise de Sistemas
- FIAP | Pós-Graduação em Gestão de Projetos
- UNINOVE | Mestrado Gestão da Tecnologia da Informação e Gestão do Conhecimento.


**WhatsApp:** +55 11 99222-4396
**LinkedIn:** https://www.linkedin.com/in/wmonaco
**Youtube:** palestrantemonaco
**Instagran**: @monacowellington
**Email:** monaco@palestrantemonaco.com.br
**Site:** www.palestrantemonaco.com.br







# Cultura organizacional em Segurança da Informação

Forbes

Início / Forbes Tech / Gartner afirma que a segurança cibernética precisa ser reformulada

## Gartner afirma que a segurança cibernética precisa ser reformulada

Com riscos indo além das áreas de TI, líderes de cibersegurança devem garantir que divisões de negócios também tenham recursos para tomar decisões defende instituto

Andressa Barbosa

16 de março de 2022 Atualizado

Compartilhe esta publicação:

# Cultura organizacional em Segurança da Informação

Forbes

Início / Forbes Tech / Gartner afirma que a segurança cibernética precisa ser reformulada

## Gartner afirma que a segurança cibernética precisa ser reformulada

- A Gartner, empresa de pesquisa e consultoria para empresas, alertou, por meio de um novo estudo global, que os líderes de segurança cibernética precisam adotar novas práticas, já que a responsabilidade sobre os riscos cibernéticos estão avançando para além das áreas de TI.
- “Os líderes de segurança cibernética estão esgotados, sobrecarregados e no modo ‘sempre ativo’”, alerta Sam Olyaei, diretor de pesquisa do Gartner.
- “Este é um reflexo direto de quão elástico o papel desse especialista se tornou na última década, devido ao crescente das expectativas entre as partes interessadas dentro de suas organizações.”, finaliza.
- Em uma pesquisa realizada pelo Gartner, cerca de 88% dos conselhos consideram a segurança cibernética como um risco comercial e não apenas um problema técnico de TI. E 13% dos entrevistados responderam que as empresas deveriam criar comitês específicos de segurança cibernética supervisionados por um diretor.
- O Gartner prevê que pelo menos 50% dos C-Levels terão requisitos de desempenho relacionados ao risco e gestão de segurança cibernética incorporados em seus contratos de trabalho até 2026. Isso afeta a pontualidade e a qualidade das decisões de risco das informações, que estão sendo cada vez mais tomadas por partes interessadas e fora da linha de visão da TI ou da segurança.

# Cultura organizacional em Segurança da Informação

## Referências

A proposta de atuação está consolidada à partir dos seguintes frameworks e legislação de mercado:

- Lei n.13.709 de 14/08/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), alterada pela Lei n. 13.853 de 08/07/2019 (criação da Autoridade Nacional de Proteção de Dados e outras providências).
- Lei de Acesso à Informação - LAI (Lei Federal nº 12.527/11)
- Marco Civil da Internet Lei n° 12.965/2014
- NBR ISO/IEC 27001:2022 - Sistemas de Gestão da Segurança da Informação
- NBR ISO/IEC 27002:2022 - Código de Prática para Controles de Segurança da Informação
- NBR ISO/IEC 27005 - Gestão de Riscos de Segurança da Informação
- NBR ISO/IEC 27701 - Gestão da Privacidade da Informação

# Cultura organizacional em Segurança da Informação

## Referências

- **ANPD | Regulamentos e Guias Orientativos (todos relatados abaixo, para simples informação):**
  - Resolução CD/ANPD Nº 1, de 28 de outubro de 2021 | Regulamento do Macro Processo de Fiscalização e do Macro Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.
  - Resolução CD/ANPD Nº 2, de 27 de janeiro de 2022 | Regulamento de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de Tratamento de pequeno porte.
  - Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público | Versão 1.0 | Jan. 2022
  - Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte | Versão 1.0 Jan. 2022
  - Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado | Versão 2.0 | Abril/2022
  - Cartilha de Segurança para Internet: Fascículo de Vazamento de Dados e Fascículo de Proteção de Dados
  - Guia Orientativo Cookies e proteção de dados pessoais | out / 2022
  - Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023 Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

# Cultura organizacional em Segurança da Informação

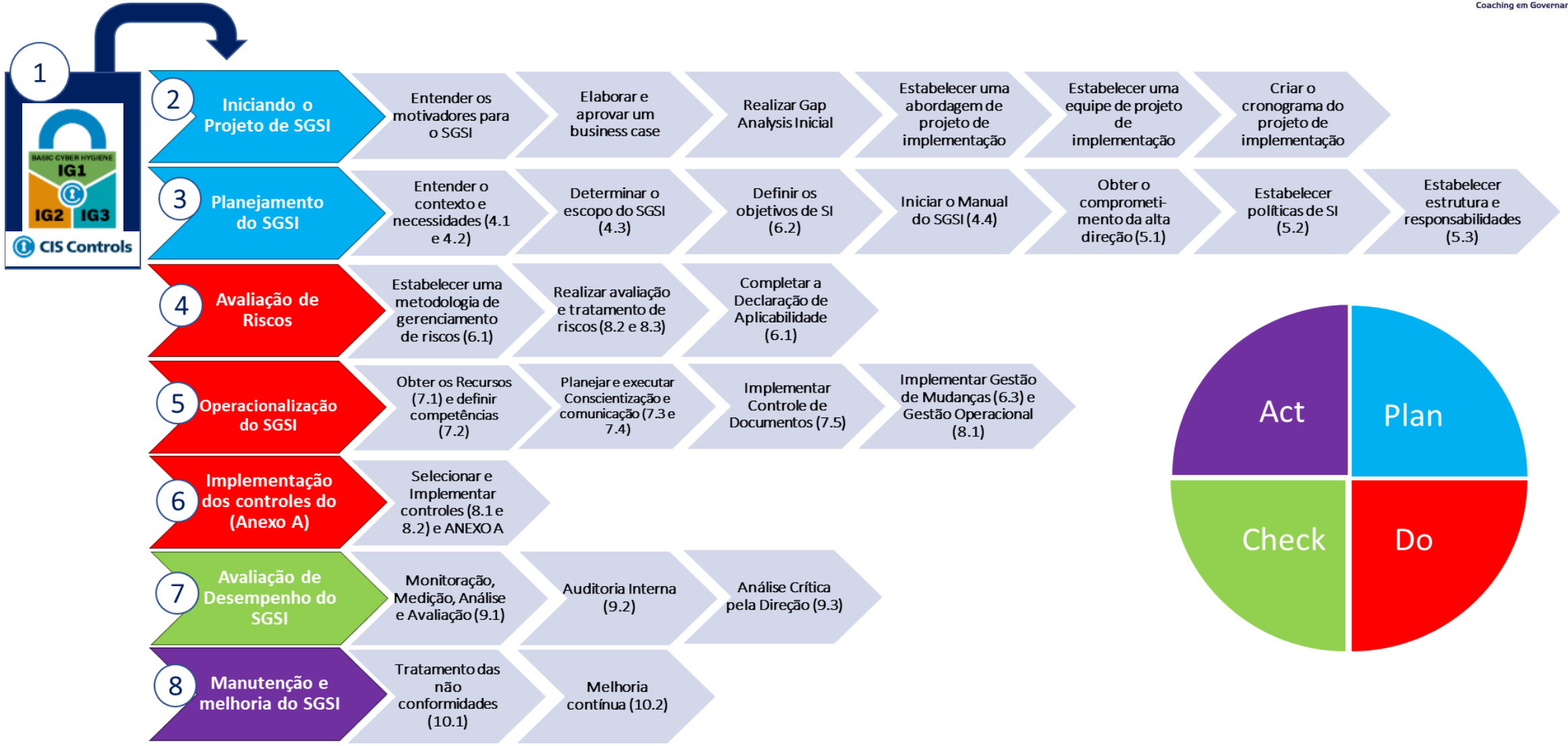
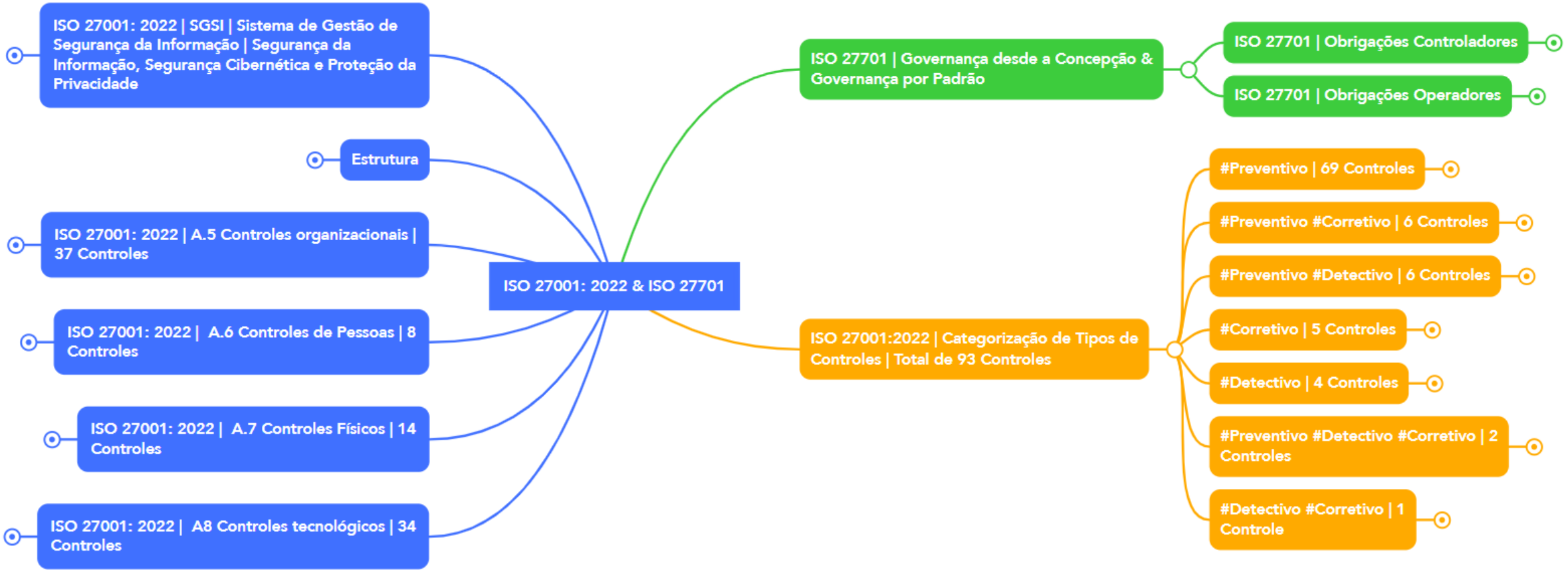



**Ilustração: TIEXAMES**

# Cultura organizacional em Segurança da Informação



# Cultura organizacional em Segurança da Informação

Ciclo de Vida dos Dados

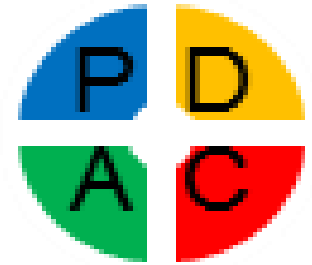
**Rastreabilidade**

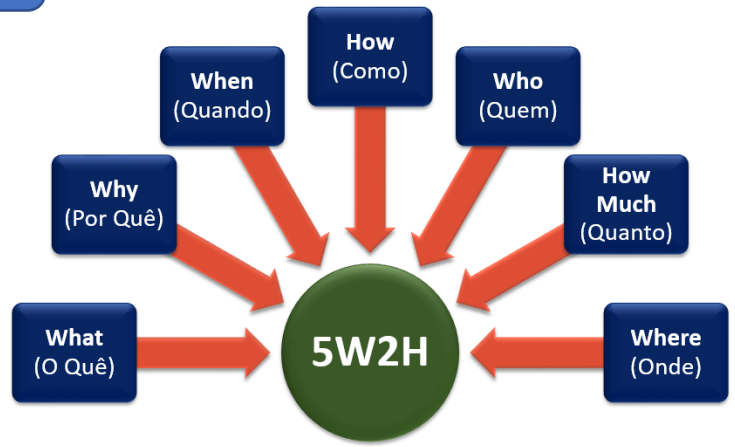
| Gerar / Coletar | Armazenar | Usar | Compartilhar | Arquivar | Excluir |
|---|---|---|---|---|---|
| Crescimento | Identificar<br>Classificar<br>Armazenar<br>Preservar<br>Proteger<br>Visibilidade<br>Dark Data | Transformar<br>Mover<br>Hierarquizar<br>Anonimizar<br>Pseudonimizar<br>Controle de Acesso<br>Comportamento | Direitos de Acesso<br>Fuga de Dados<br>Risco de Acesso | Backup<br>Criptografia<br>Reter<br>Recuperar<br>Preservar<br>Auditar | Expirar<br>Deletar<br>Destruir |

**Geração ou Coleta de dados** | **Estrutura de Permissões de Acessos** | **Regras de Retenção / Exclusão**

**Ativos:** tudo aquilo que tem importância e valor para o contexto Corporativo.

**Ativos de Informação:** tudo aquilo onde temos informações armazenadas temporária ou definitivamente.



# Cultura organizacional em Segurança da Informação

Hoje melhor que ontem..., sempre

- Indicadores
- Auditoria
- Análise Crítica
- Plano de Ação
- Acompanhamento
- Registro

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Ao contratar um fornecedor que se utiliza de um Email pessoal (@gmail, @hotmail, @terra, etc.) e não de um Email corporativo (com domínio corporativo específico) no dia-a-dia corporativo, a empresa assume uma série de riscos significativos que podem colocar em perigo sua segurança, conformidade, continuidade dos serviços e gestão de pessoal, podendo resultar em consequências graves e prejudiciais para a reputação da empresa, dos quais destacamos:

**(1) Segurança da Informação:** Ao permitir que fornecedores utilizem e-mails pessoais, a empresa está abrindo as portas para possíveis ataques cibernéticos, vazamento de informações confidenciais e acesso não autorizado a dados corporativos. É como convidar hackers para aproveitar-se das vulnerabilidades.

**Exemplo:** Um colaborador do fornecedor recebe um Email pessoal comprometido, resultando em um ataque de phishing bem-sucedido que concede acesso a informações confidenciais da empresa.

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Ao contratar um fornecedor que se utiliza de um Email pessoal ....., podendo resultar em consequências graves e prejudiciais para a reputação da empresa, dos quais destacamos:

**(2) Conformidade com regulamentações**: Ao ignorar a importância de um email corporativo, a empresa mostra desprezo flagrante pelas regulamentações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD – Artigo 50) e outras normas setoriais. Essa negligência pode levar a multas exorbitantes e manchar a reputação da empresa.

- **Exemplo:** A empresa é auditada e descobre-se que fornecedores que usam Email pessoais estão em desacordo com as regulamentações, resultando em multas pesadas e perda de confiança dos clientes.

**(3) Continuidade dos serviços:** problemas de continuidade dos serviços, especialmente mediante uma situação de desligamento de colaboradores nos fornecedores contratados, mantendo em poder do desligado, todas as informações e documentos corporativos tratados, dificultando a transferência de responsabilidades e possíveis interrupções nos serviços contratados..

- **Exemplo:** O colaborador do fornecedor que se utiliza de um Email pessoal decide sair repentinamente, deixando a empresa sem acesso aos arquivos e informações cruciais para a continuidade dos serviços, causando atrasos significativos e prejuízos financeiros.

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Ao contratar um fornecedor que se utiliza de um Email pessoal ....., podendo resultar em consequências graves e prejudiciais para a reputação da empresa, dos quais destacamos:

**(4) Rastreabilidade e responsabilidade:** O uso de um Email pessoal dificulta a rastreabilidade das comunicações e a atribuição de responsabilidades. Isso cria um ambiente perfeito para práticas inadequadas e impunidade, como o compartilhamento irresponsável de informações sensíveis.

- **Exemplo:** Um colaborador do fornecedor compartilha inadvertidamente informações confidenciais com um terceiro, mas como o Email utilizado é pessoal, é impossível identificar o responsável pelo vazamento, resultando em danos reputacionais e legais para a empresa.

**(5) Vazamento de informações sensíveis**: Ao permitir que os colaboradores dos fornecedores compartilhem informações confidenciais através de e-mails pessoais, a empresa está praticamente concedendo um convite aberto para o vazamento de dados valiosos.

- **Exemplo:** Um colaborador do fornecedor envia acidentalmente um email contendo informações confidenciais para um destinatário errado, resultando em uma violação de dados significativa que expõe informações pessoais e financeiras dos clientes da empresa.

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Ao contratar um fornecedor que se utiliza de um Email pessoal ....., podendo resultar em consequências graves e prejudiciais para a reputação da empresa, dos quais destacamos:

**(6) Compartilhamento de credenciais:** A utilização de Email pessoais pode incentivar o compartilhamento de credenciais de acesso a sistemas e plataformas, comprometendo a segurança dos dados. Isso pode levar a acessos não autorizados e tornar difícil a responsabilização individual por ações realizadas..

- **Exemplo:** Um colaborador do fornecedor compartilha inadvertidamente informações confidenciais com um terceiro, mas como o Email utilizado é pessoal, é impossível identificar o responsável pelo vazamento, resultando em danos reputacionais e legais para a empresa.

**(7) Imagem corporativa:** A utilização de emails pessoais em vez de emails corporativos mina a imagem corporativa da empresa, transmitindo uma sensação de amadorismo e falta de profissionalismo. Isso prejudica a confiança dos clientes, parceiros e stakeholders, afastando-os em direção a concorrentes mais competentes.

- **Exemplo:** Os clientes percebem que os colaboradores dos fornecedores usam Email pessoais durante a comunicação, levando a questionamentos sobre a confiabilidade da empresa e resultando em uma perda significativa de negócios.

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Ao contratar um fornecedor que se utiliza de um Email pessoal ....., podendo resultar em consequências graves e prejudiciais para a reputação da empresa, dos quais destacamos:

**(8) Gerenciamento de contatos:** Com a mudança de colaboradores no fornecedor, o uso de emails pessoais dificulta a gestão e atualização dos contatos. Isso pode resultar em lacunas de comunicação e problemas na transição de informações e responsabilidades.

- **Exemplo:** O colaborador responsável pelos serviços é substituído e a empresa descobre que não possui as informações de contato atualizadas, causando atrasos nas comunicações e dificuldades na conclusão dos projetos além de, continuar tratando informações confidenciais e sensíveis da empresa, com um colaborador já desligado do fornecedor.

**(9) Monitoramento e auditoria:** A falta de emails corporativos dificulta o monitoramento e a auditoria das comunicações e atividades relacionadas ao fornecedor. Isso cria uma névoa de incerteza sobre as ações realizadas, abrindo espaço para fraudes e abusos.

- **Exemplo:** Durante uma auditoria, a empresa não consegue rastrear adequadamente as comunicações e as atividades realizadas pelos fornecedores, deixando brechas para a ocorrência de práticas ilegais ou não de não conformidades.

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Ao contratar um fornecedor que se utiliza de um Email pessoal ....., podendo resultar em consequências graves e prejudiciais para a reputação da empresa, dos quais destacamos:

**(10) Resposta a incidentes:** A falta de rastreabilidade e identificação clara dos responsáveis dificulta de forma alarmante a resposta a incidentes de segurança ou violações de dados. Isso resulta em uma resposta lenta e inadequada, agravando os danos causados pela violação.

- **Exemplo:** Após uma violação de segurança, a empresa não consegue determinar rapidamente qual colaborador do fornecedor foi responsável pela ação, resultando em atrasos na mitigação do incidente e perda de confiança dos clientes..

# Cultura organizacional em Segurança da Informação

## Reveja a relação com Fornecedores que se utilizam de E-mail pessoal

- Para mitigar esses riscos, é essencial que a empresa estabeleça Políticas e Diretrizes claras sobre o Uso de Email Corporativo nos contratos com fornecedores.
- Definir cláusulas contratuais que estipulem a obrigatoriedade do fornecedor em utilizar e-mails corporativos, bem como informar prontamente a empresa sobre qualquer mudança de colaboradores ou contato responsável pelos serviços prestados.
- Essas medidas ajudam a garantir a segurança dos dados, a conformidade com regulamentações e a continuidade dos serviços de forma adequada.

# Proposta de Atuação
# Identificar “onde estamos”

# Cultura organizacional em Segurança da Informação

monaco
Coaching em Governança de TI

**Oferta-1 | Diagnóstico Inicial: técnico**

- Análise de Vulnerabilidade
- Pentests
- **Investimentos: consulte-nos**

**Oferta-2 | Avaliação de Contratos no contexto LGPD (Jurídico)**

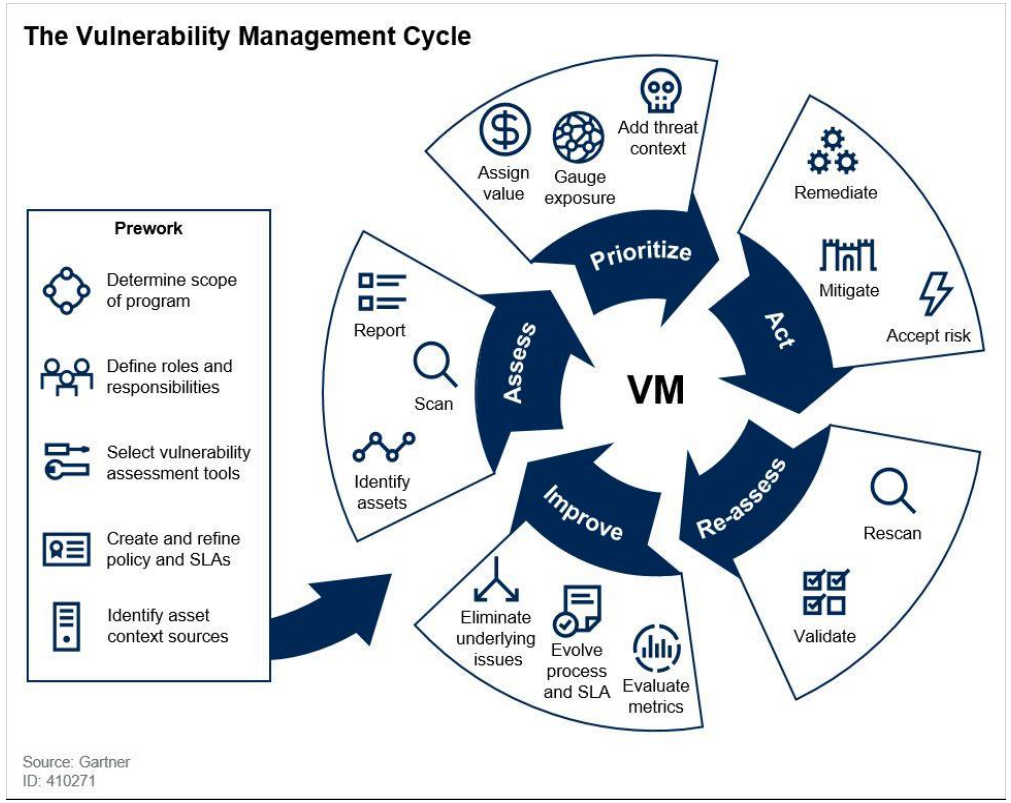
- 4 Contratos ou Tipos de Contratos
- 1 reunião de consolidação e direcionamento das propostas de alterações
- **Investimentos: consulte-nos**

**Oferta-3 | Avaliação da cultura corporativa em Segurança da Informação (ISO 27001:2022)**

- Identificação de Atividades de Tratamento de Dados nos Departamentos: RH, Jurídico, Marketing, Comercial e TI
- Consolidação do Sistema de Gestão de Segurança da Informação
- Consolidação dos atuais Controles de Segurança da Informação
- Consolidação da atual Gestão de Aplicabilidade
- Consolidação de Gaps
- Plano de Ação – alto nível de detalhamento

**Requisitos obrigatórios:**

- Áreas corporativas envolvidas como **"perímetro de segurança mínimo":**
  - ✓ Sites Web Corporativos
  - ✓ RH | Jurídico | Marketing | TI
  - ✓ no mínimo de 2 Colaboradores por departamento
- **Investimentos: consulte-nos**



MONACO
PALESTRANTE

# Obrigado!

## Wellington Monaco


+55 11 99222-4396
https://www.linkedin.com/in/wmonaco
palestrantemonaco
@monacowellington
monaco@palestrantemonaco.com.br

www.palestrantemonaco.com.br