Política de riscos de segurança da informação

Documento gerado em 26/11/2024 às 10h40

Metadados

Código	Origem	Elaboração	Última Revisão	Próxima Revisão
PLT.SEG.ADM.005.1	Segurança da Informação	28/05/2019	26/11/2024	26/11/2027

Ficha técnica

Etapa	Responsável	Assinatura
Elaboração	Felipe Mendonça Satito de Melo	Felipe Satito — Assinado eletronicamente por: Felipe Satito Data: 27 de novembro de 2024 11:46 GMT-3
Revisão	Antonio Sergio da Silva	Assinado eletronicamente por: Antonio Sergio da Silva Data: 27 de novembro de 2024 14:42 GMT-3
Revisão	Thamires Pedra Kemache Franco	Assinado eletronicamente por: Thamires Pedra Kemache Franco Data: 27 de novembro de 2024 17:29 GMT-3
Aprovação	Teresa Cristina Campos Mello	Teresa Cristina Campos Mello — Assinado eletronicamente por: Teresa Cristina Campos Mello Data: 29 de novembro de 2024 09:59 GMT-3

Objetivo

A Gestão de Riscos de Segurança da Informação tem como objetivo contribuir com seus processos de negócios, em consonância com as melhores práticas de segurança da informação, garantindo a monitoração contínua e eficaz dos riscos referentes à confidencialidade, integridade e disponibilidade dos ativos da informação.

Aplicabilidade

As diretrizes estabelecidas nesta política se aplicam a todos os colaboradores do Grupo Prevent Senior, incluindo sua Alta Direção.

Definições

• **Risco:** combinação de consequências que possam vir a surgir através de uma ocorrência com evento indesejado, materializando o impacto e a probabilidade de ocorrer este evento.

• **Ativo da informação:** qualquer componente ou pessoa que detém uma informação no qual tem valor para a Prevent Senior e, portanto, necessita de proteção.

• **Ameaça:** agente com potencial de prejudicar ativos da informação, bem como processos e sistemas. As ameaças podem ter sua origem de forma natural ou humana, acidentais ou deliberadas.

• **Controles:** ações as quais auxiliam na mitigação de riscos de segurança da informação.

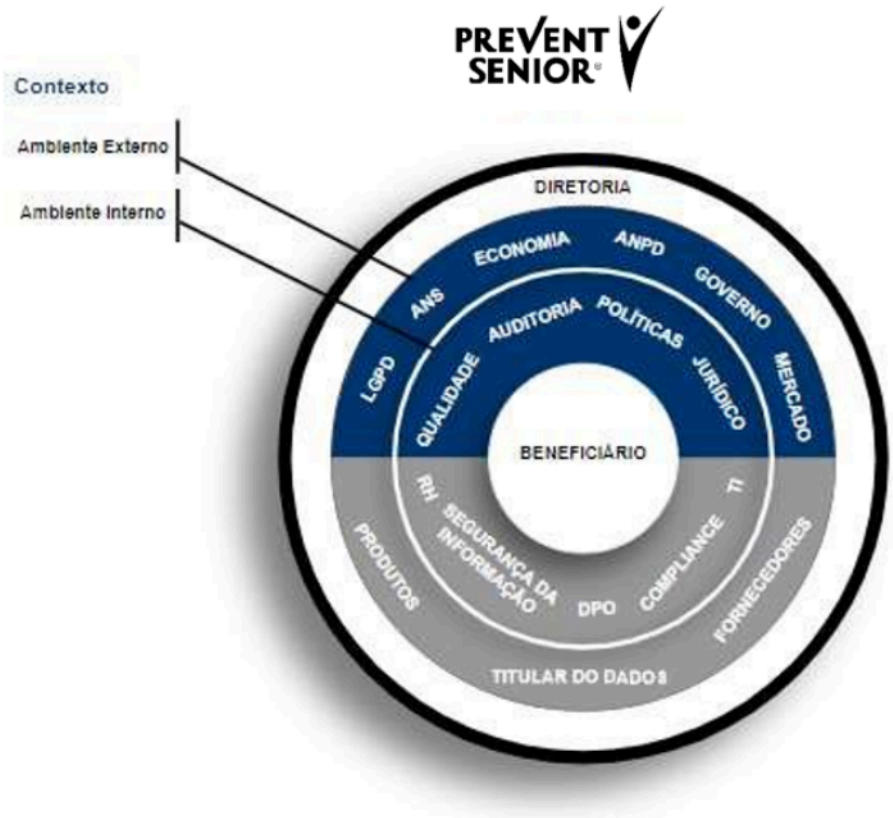
• **Consequências:** podem ser caracterizadas como perda de eficácia, condições operacionais adversas, perda de negócios, reputação, danos aos beneficiários, etc.

• **Tolerância:** quantidade, para mais ou para menos, aceita pela Prevent Senior, em face a determinado risco.

• **Evitar o risco:** significa encerrar o processo ou ativo da informação. Neste caso, essa opção deve ser aprovada pela Alta Direção.

Contexto da organização

A análise de riscos de segurança deve considerar o ambiente no qual a Prevent Senior está inserida, bem como as partes interessadas e os fatores internos e externos relevantes no contexto, conforme imagem a seguir:



Monitoração e revisão dos riscos de segurança da informação

Com o objetivo de manter o cenário de exposição atualizado, o departamento de Segurança da Informação, juntamente com as demais áreas da Prevent Senior,

deve sustentar procedimentos que corroborem com a monitoração e revisão dos riscos de segurança. Estes procedimentos podem ser sistêmicos ou por meio de controles manuais, os quais possibilitam revisar de forma periódica os níveis dos riscos em seus respectivos ativos da informação.

Papéis e responsabilidades

Alta direção

• Aprovar a Política de Riscos de Segurança da Informação.

• Aprovar a régua de impacto dos riscos de segurança.

• Aprovar a estratégia de riscos de segurança.

• Aprovar o apetite de riscos de segurança o qual a Prevent Senior está disposta a aceitar.

• Avaliar e aprovar a carta de aceitação dos riscos que estão fora da margem do apetite.

• Deliberar prioridade nas tratativas dos riscos de segurança.

• Analisar os relatórios que têm como objetivo apresentar o status dos riscos de segurança na Prevent Senior.

• Apoiar a cultura de gestão de riscos na Prevent Senior.

DPO

• Estar ciente de todos os riscos de segurança relacionados à privacidade de dados pessoais e dados pessoais sensíveis.

• Avaliar os riscos de segurança sob a ótica da privacidade de dados pessoais e dados pessoais sensíveis.

• Reportar à Alta Direção o status de tratamento dos riscos relacionados à privacidade de dados pessoais e dados pessoais sensíveis.

• Analisar e aprovar a carta de aceite dos riscos que envolvem a privacidade de dados pessoais e dados pessoais sensíveis e que estão fora da tolerância definida pela Alta Direção.

Segurança da informação

• Elaborar e manter atualizada a Política de Riscos de Segurança da Informação.

• Elaborar régua de impacto dos riscos de segurança.

• Apresentar à Alta Direção a estratégia de riscos de segurança.

• Apresentar o apetite de riscos de segurança o qual a Prevent Senior está disposta a aceitar.

• Analisar periodicamente os riscos atrelados aos ativos da informação.

• Formalizar, classificar e comunicar a análise dos riscos de segurança aos seus respectivos responsáveis.

• Aplicar a Carta de Risco para Segurança da Informação quando o responsável do risco optar por aceitá-lo.

• Reportar à Alta Direção o status dos riscos de segurança identificados na Prevent Senior.

• Comunicar ao DPO tempestivamente quando identificar um risco de segurança relacionado à privacidade de dados pessoais e dados pessoais sensíveis.

• Manter as cartas de aceite como informação documentada em local seguro e com acesso restrito.

Jurídico

• Avaliar o conteúdo da Política de Riscos de Segurança da Informação.

• Estar ciente dos riscos de segurança relacionados à privacidade de dados pessoais e dados pessoais sensíveis.

• Estar ciente das Cartas de Risco para Segurança da Informação relacionadas à privacidade de dados pessoais e dados pessoais sensíveis.

• Comunicar ao DPO tempestivamente quando identificar um risco de segurança relacionado à privacidade de dados pessoais e dados pessoais sensíveis.

Auditoria interna

• Avaliar o conteúdo da Política de Riscos de Segurança da Informação.

• Acompanhar a eficácia do processo para gestão de risco de segurança.

• Avaliar periodicamente o tratamento dos riscos de segurança.

• Comunicar ao departamento de Segurança da Informação quando identificar um risco de segurança.

• Comunicar ao DPO tempestivamente quando identificar um risco de segurança relacionado à privacidade de dados pessoais e dados pessoais sensíveis.

Qualidade

• Comunicar ao departamento de Segurança da Informação quando identificar a criação de um novo processo.

• Considerar a análise de riscos de segurança da informação na padronização estabelecida pelo departamento da Qualidade.

• Comunicar ao departamento de Segurança da Informação quando identificar um risco de segurança.

• Comunicar ao DPO tempestivamente quando identificar um risco de segurança relacionado à privacidade de dados pessoais e dados pessoais sensíveis.

Todas as áreas administrativas e operacionais

• Acompanhar a eficácia do tratamento para os riscos de segurança sob sua responsabilidade.

• Manter os riscos de segurança dentro do nível aceitável na Prevent Senior.

• Assinar a Carta de Risco para Segurança da Informação quando o responsável optar por aceitar o risco de segurança (caso o nível do risco estiver fora da tolerância estabelecida pela Prevent Senior).

• Comunicar ao departamento de Segurança da Informação quando identificar um risco de segurança.

• Comunicar ao DPO tempestivamente quando identificar um risco de segurança relacionado à privacidade de dados pessoais e dados pessoais sensíveis.

• Cumprir com o plano de ação proposto para mitigação do risco sob sua responsabilidade.

Prestadores de serviço

• Comunicar ao departamento de Segurança da Informação quando identificar um risco de segurança.

• Comunicar ao DPO tempestivamente quando identificar um risco de segurança relacionado à privacidade de dados pessoais e dados pessoais sensíveis.

• Cumprir com o plano de ação proposto para mitigação do risco sob sua responsabilidade.

• Cumprir as cláusulas estipuladas no Contrato de Prestação de Serviços.

Critério base

Atuação da gestão de riscos

Cabe à Gestão de Riscos de Segurança da Informação manter critérios básicos para um bom gerenciamento de riscos, como critérios de avaliação de riscos, de impacto, de tratativa e até critérios de aceitação dos riscos. Além disso, deve-se:

• Realizar avaliação de riscos e estabelecer um plano de tratamento para os mesmos.

• Definir e implementar políticas e procedimentos, incluindo a implementação dos controles selecionados.

• Realizar a monitoração de controles de segurança da informação.

• Realizar de forma contínua o gerenciamento de riscos à segurança da informação.

Avaliação de riscos

Os critérios para avaliação de riscos de segurança da informação devem ser desenvolvidos, considerando os seguintes tópicos:

• Valor: valor estratégico do processo de informações.

• Criticidade: criticidade dos ativos de informação envolvidos.

• Requisitos: requisitos legais, regulamentares e obrigações contratuais.

• Importância: importância operacional e ao negócio da Prevent Senior através da disponibilidade, confidencialidade e integridade da informação.

• Expectativas: expectativas, percepções dos stakeholders como consequências negativas para uma boa reputação.

Além disso, critérios de avaliação de riscos podem ser usados para especificar prioridades para o seu tratamento.

Critério de impacto

Os critérios de impacto devem ser desenvolvidos e especificados, considerando o grau de dano ou custo à organização, causado por um evento de segurança da informação, considerando:

• Nível de classificação do ativo de informação impactado.

• Violação da segurança da informação, tais como perda de confidencialidade, integridade e disponibilidade.

• Impacto nas operações (internas ou de terceiros).

• Perda de valor comercial ou financeiro.

• Interrupção de planos e prazos.

• Danos à reputação (imagem).

• Violação de requisitos legais, regulamentares ou contratuais.

Critério de aceitação de riscos

Ao realizar o tratamento de um determinado risco, o responsável pelo projeto ou processo poderá aceitar o risco, desde que este aceite que fique em consonância com os critérios estabelecidos nesta política.

Após formalizar o aceite do risco de segurança, o departamento de Segurança da Informação deverá acompanhar todo o ciclo de vida deste risco e comunicar

imediatamente as partes envolvidas, caso ocorra alguma modificação em sua característica.

Em casos os quais o nível do risco fique além do determinado pela Alta Direção, o responsável deverá manter devidamente registrado o aceite no Termo de Aceite do Risco de Segurança da Informação.

Deverão ser considerados como critérios para aceitação de risco:

• Diretrizes da Alta Direção.

• Políticas, normas e manuais da Prevent Senior.

• Metas.

• Objetivos e interesses da Prevent Senior.

Caso seja identificado risco posterior, este poderá ser aceito a qualquer momento, desde que siga as diretrizes supracitada, bem como haja a comunicação ao departamento de Segurança da Informação para conduzir a devida análise e tratamento do risco.

Caso o responsável opte por não aceitar mais o risco, o Termo de Aceite do Risco de Segurança da Informação será atualizado.

Gestão de riscos para segurança da informação

Objetivando manter a eficiência da Gestão de Riscos para Segurança da Informação, a Prevent Senior deverá considerar as seguintes ações:

• Desenvolvimento do processo de gerenciamento de riscos à segurança da informação adequado à organização.

• Identificação e análise das partes interessadas.

• Definição de papéis e responsabilidades de todas as partes, internas e externas à organização.

• Estabelecimento das relações necessárias entre o responsável pelo processo e as partes interessadas.

• Definição de critérios para escalonamento.

• Definição e descrição de registros a serem mantidos.

Descrição sobre atividade da gestão de riscos para segurança da informação

As atividades de gestão devem considerar os critérios básicos mencionados nesta política, identificando, quantificando e qualificando os descritivos, e priorizando conforme o resultado da avaliação.

A avaliação de riscos possibilitará quantificar ou descrever qualitativamente o risco, permitindo, assim, que os responsáveis priorizem de acordo com a severidade.

A avaliação consiste nas seguintes atividades:

• Identificação

• Análise

• Mensuração

A avaliação determina o valor dos ativos de informação, bem como identifica as ameaças aplicáveis e vulnerabilidades que existem (ou poderiam existir), além dos controles existentes e seus efeitos no risco e as possíveis consequências mediante o seu não tratamento.

Identificação dos riscos

Introdução para a identificação dos riscos

O objetivo da identificação de riscos é determinar o que poderá acontecer para causar uma perda potencial e obter informações sobre como, onde e por que pode ocorrer.

A identificação de riscos independe se a origem está sob o controle da Prevent Senior.

As etapas descritas nos itens a seguir informam sobre como será a coleta de informações para a atividade de análise de risco.

Identificando ativos de informação

A identificação de ativos da informação deve ser realizada em um nível adequado de detalhes e que forneça informações suficientes para a sua avaliação. O nível de detalhe influenciará a quantidade total de informações coletadas durante a sua avaliação.

O responsável do ativo deve ser identificado a fim de se fornecer responsabilidade e prestação de contas. Este não detém direitos de propriedade sobre o ativo, mas é responsável por sua produção, desenvolvimento, manutenção, uso e segurança.

Identificando ameaças

Ameaças podem afetar mais de um ativo da informação. Nestes casos, elas podem causar impactos diferentes, dependendo de quais ativos são afetados.

Identificando controles existentes

Constantemente, a equipe de Segurança da Informação deverá analisar a eficácia de um controle utilizando ferramentas para garantir a monitoração contínua (como, por exemplo, *checklist*), possibilitando a identificação da necessidade de recomendar novos controles complementares para lidar com o risco verificado.

As análises das gerências e os relatórios de auditoria também fornecem informações sobre a eficácia dos controles existentes. Um controle pode ser identificado como ineficaz, insuficiente ou justificado. Se não for justificado ou insuficiente, o controle deve ser verificado para determinar se o mesmo tem que ser removido, substituído ou se deve permanecer no local.

Identificando vulnerabilidades

A presença de uma vulnerabilidade (como, por exemplo, uma implementação incorreta, mau funcionamento ou uso incorreto do controle) em um ativo da informação não causa danos por si só, pois é necessário que haja uma ameaça presente.

Deste modo, uma vulnerabilidade que não possuir ameaça correspondente pode não exigir a implementação de um controle, mas deve ser reconhecido e monitorado para identificar eventuais mudanças. Vulnerabilidades podem ser identificadas nos seguintes locais:

• Em todas as empresas do Grupo Prevent Senior.

• Processos e procedimentos.

• Rotinas de gerenciamento.

• Pessoas.

• Ambiente físico.

• Configurações nos sistemas.

• Hardware, software ou equipamento de comunicação.

• Dependência de terceiros.

Comunicando riscos de segurança da informação

O Departamento de Segurança da Informação é o responsável por comunicar os riscos de segurança de acordo com sua criticidade, podendo chegar às seguintes partes envolvidas:

• Responsável pelo ativo da informação.

• Responsável pelo o risco de segurança.

• Responsável pelo departamento e/ou linha de negócio.

• DPO.

• Alta Direção.

• ANPD.

• ANS.

Quando um determinado risco de segurança se materializar, podem ter situações as quais será necessário um comunicado oficial através da Assessoria de Imprensa.

Identificando consequências

A identificação das consequências auxilia na mensuração de possíveis impactos, caso uma ameaça se beneficie por meio de uma vulnerabilidade. Objetivando minimizar os impactos, a Prevent Senior deve identificar as consequências e se atentar às seguintes ações:

• Tempo de investigação e reparo.

• Avaliar o tempo de trabalho perdido.

• Analisar a oportunidade perdida.

• Mensurar os danos de saúde e segurança de todas pessoas relacionadas ao impacto.

• Avaliar o custo financeiro de habilidades específicas para reparar os danos.

• Avaliar a reputação e a imagem da Prevent Senior.

Análise de riscos

Metodologia para análise de riscos

A análise de risco deve ser realizada considerando o grau de detalhes necessários que permita a verificação das consequências, levando-se em conta também a criticidade do ativo da informação e extensão do histórico de ocorrências conhecidas por identificações ou incidentes anteriores envolvendo a Prevent Senior.

Analisando consequências

Um risco poderá impactar em uma ou mais categorias. Caso identificado, o responsável pela análise deverá levar em conta sempre o pior dos cenários. A análise das consequências utilizará como base cinco categorias de impacto:

• Tecnologia.

• Financeiro.

• Legal e Regulatório.

• Operacional.

• Negócio.

• Social e humanitários.

Cada categoria de impacto terá a respectiva régua de impacto:

- Muito Baixo (valor 1).
- Baixo (valor 3).
- Médio (valor 5).
- Alto (valor 7).
- Muito Alto (valor 9).

> *Observação 1: os detalhamentos das categorias e seus respectivos impactos previstos estão disponíveis na Matriz de Impacto.*

Analisando probabilidades de incidentes

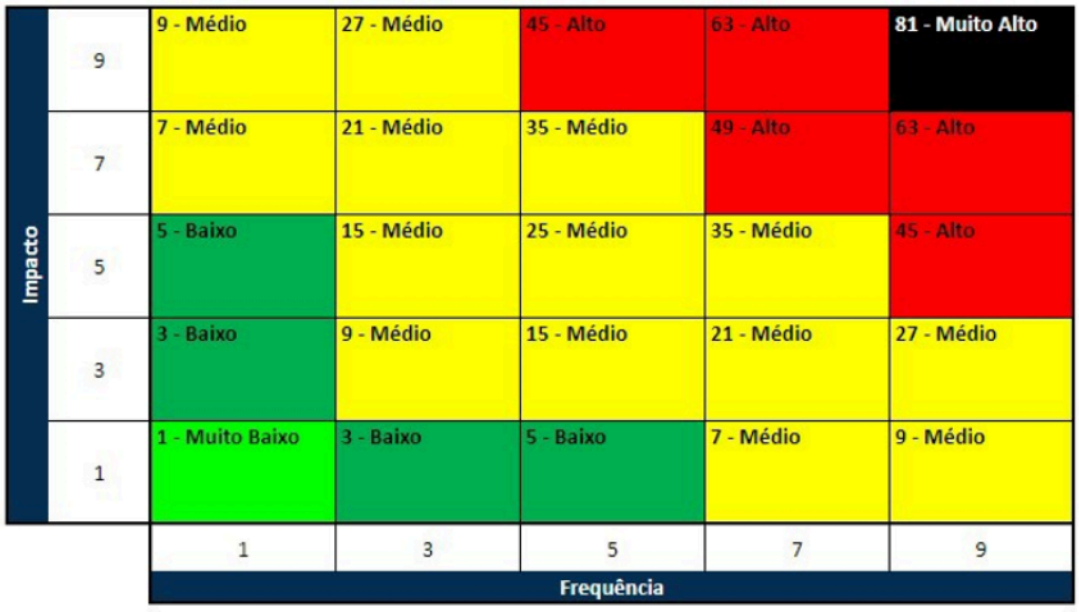
Após a identificação do impacto/consequências, o próximo passo da análise de risco é avaliar o histórico de ocorrências relacionadas ao incidente ou vulnerabilidade, através da seguinte classificação:

- **Rara** (valor 1).
- **Pouco provável** (valor 3).
- **Possível** (valor 5).
- **Provável** (valor 7).
- **Quase certo** (valor 9).

> *Observação 2: caso se identifique novamente uma vulnerabilidade, a frequência do risco aumentará.*

Níveis de riscos

Após as análises das consequências e probabilidades, é possível mensurar o nível do risco do incidente ou vulnerabilidade, conforme ilustrado a seguir:



Impacto						
	9	9 - Médio	27 - Médio	45 - Alto	63 - Alto	81 - Muito Alto
	7	7 - Médio	21 - Médio	35 - Médio	49 - Alto	63 - Alto
	5	5 - Baixo	15 - Médio	25 - Médio	35 - Médio	45 - Alto
	3	3 - Baixo	9 - Médio	15 - Médio	21 - Médio	27 - Médio
	1	1 - Muito Baixo	3 - Baixo	5 - Baixo	7 - Médio	9 - Médio
		1	3	5	7	9
		Frequência				

Avaliação dos riscos

De acordo com o nível do risco, o departamento de Segurança da Informação deverá potencializar a forma da atuação para a conclusão do plano de ação e o envolvimento das partes interessadas, podendo incluir na tratativa do risco desde somente o responsável pelo ativo da informação até a Alta Direção.

A avaliação considerará no primeiro momento o valor bruto do risco, sem considerar a efetividade dos controles atrelados para a sua mitigação.

Tratamento de riscos de segurança da informação

Descrição sobre o tratamento de riscos

O tratamento será consequência do resultado de análise do risco atrelada a sua severidade. Quanto maior o risco e a criticidade do ativo da informação, maior será o nível de comunicação e a urgência para seu tratamento, sendo estabelecidos os seguintes níveis de comunicação:

• **Risco Muito Baixo:** comunicar o responsável pelo ativo da informação.

• **Risco Baixo:** comunicar o responsável pelo ativo da informação e o seu gestor imediato.

• **Risco Médio:** comunicar o responsável pelo ativo da informação e o seu gestor imediato.

• **Risco Alto:** comunicar o responsável pelo ativo da informação e o seu gestor imediato, bem como todas as partes envolvidas e a Alta Direção.

• **Risco Muito Alto:** comunicar o responsável pelo ativo da informação, o seu gestor imediato, todas as partes envolvidas e a Alta Direção.

Nos casos os quais o incidente envolva dados pessoais e dados pessoais sensíveis, o risco deverá ser comunicado ao DPO (encarregado dos dados) para o devido tratamento.

Compartilhamento do risco

Um risco é compartilhado quando o seu nível é relativamente alto, mas a implementação de controles não apresenta custo/benefício adequado. Deste

modo, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro.

Evitar o risco

Um risco é evitado quando seu nível é classificado como “Alto” ou “Muito Alto” e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar com o risco da Prevent Senior.

Modificação do risco

A modificação ocorrerá quando houver uma alteração no nível do risco identificado. Podem ocorrer:

• **Aumento do nível do risco:** reincidência de determinado evento ou aumentando a relevância de um ativo da informação.

• **Diminuição do nível do risco:** implementação de controles, ajustes no processo, diminuição da relevância de um ativo da informação.

Retenção do risco

A retenção do risco é quando a Prevent Senior decide, com base na avaliação, aceitar o risco.

Tolerância ao risco

Toda tolerância ao risco de segurança aceito pela Prevent Senior, considerado viável para seu negócio, deve ser submetido para aprovação da Alta Direção.

Níveis de tolerância ao risco

• **Informações consideradas críticas:** consideradas vitais, de alta relevância para a Prevent Senior, que promovem impacto direto aos beneficiários e colaboradores, resultando em vazamento ou perda de informações, comprometendo, assim, sua integridade e impossibilitando de realizar a continuidade de seus negócios. A tolerância aos riscos com este perfil é baixa.

• **Informações consideradas não críticas:** referentes às atividades de suporte ao negócio da Prevent Senior, que não representam alta relevância, sendo de conhecimento. A tolerância ao risco é média.

Em caso que o responsável do risco optar em aceitar (reter) o risco, deve seguir os seguintes procedimentos:

• Quando o risco se caracterizar dentro da tolerância definida pela Prevent Senior, o aceite deverá ser avaliado formalmente pela equipe de Segurança da Informação e pelo DPO, quando constar dados pessoais ou dados pessoais sensíveis.

• Em caso o qual o nível do risco estiver além da tolerância definida pela Prevent Senior, a equipe de Segurança da Informação deverá formalizar uma **Carta de Risco para Segurança da Informação** com as seguintes informações:

• Descrição do risco.

• Ativo da informação.

• Responsável pelo risco.

• Análise de probabilidade x impacto.

• Nível do risco.

É impreterível que a carta tenha a assinatura do responsável pelo risco, do representante da Alta Direção e, em caso de envolver dados pessoal ou dado pessoal sensível, o DPO também deverá formalizar sua ciência.

Anexos

- Política de Tratamento de Dados pessoais em conformidade com LGPD.
- Política de Segurança da Informação.

Histórico de alterações conforme versionamento

Versão	Descrição da alteração	Responsável
1	Revisão do texto e reenvio devido ao prazo de vigência do documento em sistema	Felipe Satito

---

SGQ - Núcleo de Gestão de Documentos, Prevent Senior, 2024.

A work by R Markdown

UUID:45b8eeed-9ad8-4af0-89f2-98f9d56bafcf