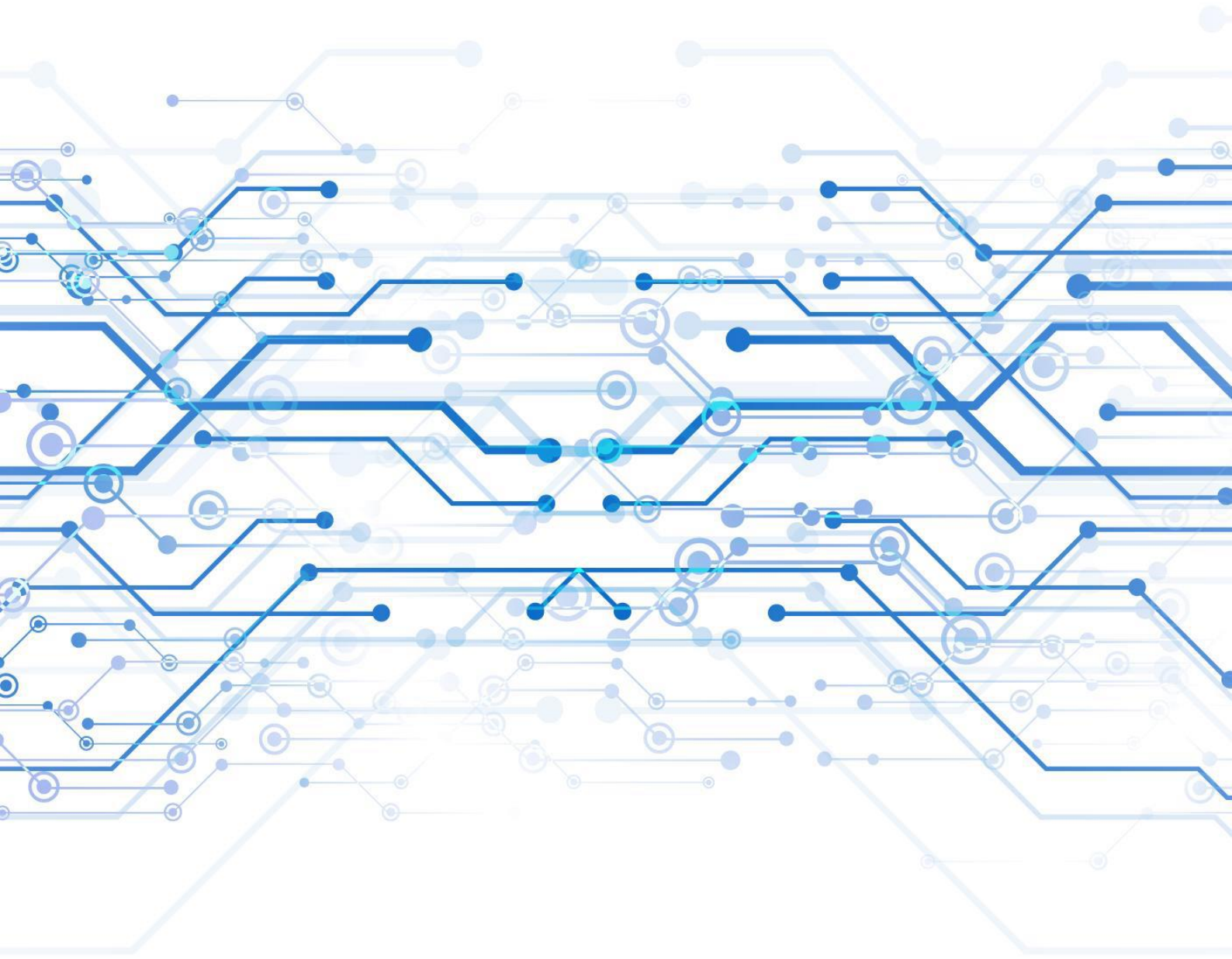
# Política de segurança da informação da Previnorte



PREVINORTE
Fundação de Previdência Complementar

# ÍNDICE

# 1. Objetivo

Definir diretrizes adequadas de Segurança da Informação, adotando-se as melhores práticas, para a correta utilização das informações. Esta Política deve ser seguida por todos os colaboradores da PREVINORTE, visando garantir a Disponibilidade, Integridade, Confidencialidade, Autenticidade e o Respeito à Privacidade e Proteção de Dados.

# 2. Conceitos

## 2.1. Ativo

Qualquer componente (seja humano, tecnológico, software e etc.) que sustente um ou mais processos de negócio da PREVINORTE.

## 2.2. Colaborador

Qualquer pessoa que contribua para o desenvolvimento das atividades da PREVINORTE. São eles empregados, diretores, conselheiros, contratados, prestadores de serviço, terceirizados, estagiários, jovens aprendizes, ou qualquer outra pessoa que atue na PREVINORTE.

## 2.3. Gestor de informação

Gerentes das áreas e titulares dos órgãos colegiados de direção superior, conforme regimento interno da PREVINORTE.

## 2.4. Incerteza

É um estado, no qual o tomador de decisões não tem como saber detalhes relacionados a um evento, tornando ineficiente a sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

## 2.5. Informação

Informação é a reunião ou o conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno.

## 2.6. Risco

Probabilidade e consequência de insucesso em um evento, em função de acontecimento eventual, em um cenário de incerteza, cuja ocorrência não depende exclusivamente da PREVINORTE, podendo causar danos, perda de informações, perda financeira, parada de serviço(s), disseminação indevida, danos a reputação e outros.

## 2.7. Segurança da Informação

É a proteção da informação contra os mais diversos tipos de ameaças para garantir a continuidade dos negócios, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio.

## 2.8. Violação

Toda e qualquer ação que desrespeite normas preestabelecidas, tanto desta política quanto dos demais instrumentos regulamentares que a complementem.

# 3. Referências

Manual de Boas Práticas em Tecnologia da Informação – ABRAPP – junho/2013.

Código das Melhores práticas de Governança Corporativa – Instituto de Governança Corporativa.

Manual de Controles Internos – ABRAPP - 2010.

Resolução CGPC/MPS nº 13 - outubro de 2004.

Código de Ética e Manual de Conduta da PREVINORTE – dezembro/2014.

Lei Geral de Proteção de Dados nº 13.709 de agosto de 2018.

# 4. Pilares

A PREVINORTE garante a segurança da informação a partir dos seguintes pilares

### 4.1. Autenticidade

Garantia de que a autoria e a origem da informação sejam sempre identificáveis.

### 4.2. Confidencialidade

Garantia de que a informação só esteja disponível para pessoa física, sistema, órgão ou entidade devidamente autorizados e credenciados.

### 4.3. Disponibilidade

Garantia de que a informação esteja acessível e utilizável por pessoa física, órgãos e entidades devidamente autorizados, através de determinado sistema ou ativo.

### 4.4. Integridade

Garantia de que a informação está íntegra, ou seja, não sofreu modificação ou foi destruída de forma não autorizada ou acidental durante se ciclo de processamento.

### 4.5. Respeito

Garantia de cumprimento à privacidade e proteção de dados, à inviolabilidade da intimidade, da autodeterminação informativa, à liberdade de expressão e de informação, de comunicação e de opinião, à honra e a imagem, ao desenvolvimento econômico, tecnológico e da inovação, em alinhamento estratégico e operacional com a Política de Proteção de Dados, normas internas de proteção de dados e programa de mitigação de riscos.

# 5. Diretrizes

## 5.1. Público-alvo

Todos os colaboradores da PREVINORTE que venham a ter acesso, de forma direta ou indireta, às suas informações e recursos corporativos.

## 5.2. Tratamento da Informação

Toda informação utilizada pela PREVINORTE deve ser gerenciada de forma adequada durante todo seu ciclo de processamento (criação, registro, classificação, acesso, manuseio, reprodução, transmissão, guarda e descarte). O acesso a esta informação deve ser permitido somente ao público adequado, devendo ser protegida de manipulação indevida, e ter o tratamento adequado

para que haja a manutenção do sigilo e da segurança de acesso, com a possibilidade de rastreabilidade da autoria e origem.

## 5.3. Propriedade Intelectual

A PREVINORTE é proprietária e detentora do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia, portanto, todas as informações sob guarda da PREVINORTE, independentemente da origem, se coletada pela entidade ou obtida através de terceiros, são consideradas propriedade intelectual da PREVINORTE, devendo os colaboradores, utilizarem única e exclusivamente para as finalidades constantes do contrato de trabalho.

Os equipamentos, meios de comunicação e sistemas estão sujeitos a monitoramento, sendo certo que eventuais informações de cunho pessoal tratadas por esses meios serão abrangidas por referido controle, pela sua indissociabilidade.

A utilização indevida de tais informações configura infração ética pelo colaborador e deverá ser encaminhada para o Comissão de Ética da entidade.

## 5.4. Classificação da informação

Com a finalidade de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a PREVINORTE, é necessário que esta receba uma classificação com base em metodologias e critérios definidos em documentos normativos internos, quanto ao seu grau de sigilo ou nível de restrição de acesso, considerando os processos e atividades nas quais estão inseridas.

## 5.5. Utilização da informação e dos recursos corporativos

Independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a sua finalidade devidamente autorizada.

Cabe ao gestor da informação autorizar os acessos, incluindo os relacionados ao sistema informatizado, levando em consideração o sigilo adequado e a necessidade de acesso para cada tipo de público.

A autorização do acesso à informação deve ser apenas para colabores que necessitem da mesma para fins relacionados ao desenvolvimento de suas atividades profissionais.

O colaborador deve acessar apenas as informações ou sistemas previamente autorizados. Qualquer ação não autorizada para burlar os controles e obter acesso a informações ou sistemas deve ser considerada uma falta disciplinar sujeita a sanções previstas no Código de Ética e Manual de Conduta da PREVINORTE.

As credenciais de acesso (nome de usuário e senha) concedidas a um colaborador devem ser de uso pessoal e intransferível e de conhecimento exclusivo.

Todos os recursos corporativos fornecidos pela PREVINORTE, inclusive o e-mail, devem ser para uso em atividades profissionais, sendo assim, o seu uso não deve violar a legislação e os normativos, nem o Código de Ética e Manual de Conduta da PREVINORTE.

Com objetivo de garantir o cumprimento desta política, a utilização dos recursos corporativos é registrada e monitorada pela PREVINORTE, não devendo o colaborador ter expectativa de sigilo em sua utilização.

## 5.6. Proteção de dados e informações

A PREVINORTE possui controles aptos a assegurar a confidencialidade da informação, através de gestão de acessos a sistemas, rede corporativa e arquivos físicos, de modo que o acesso seja realizado somente para quem possua permissão para tanto.

Todos os colaboradores devem preservar a confidencialidade e integridade de documentos, registros, cadastros e sistemas de informação, em todos os meios utilizados pela Fundação, tanto físico quanto eletrônico.

Os gestores das áreas devem proteger e controlar o acesso físico e lógico aos seus recursos de informação, compatível com o seu nível de criticidade e/ou classificação.

Todo incidente e/ou falha de segurança da informação detectados, devem ser reportados à área de Tecnologia da Informação e ao encarregado da entidade (DPO).

A PREVINORTE avalia, monitora e implementa melhorias aos riscos associados às informações que mantém sob sua guarda, como objetivo de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Também são avaliados previamente o risco e o impacto na segurança da informação no desenvolvimento de novos produtos ou reformulação de processos, bem como na contratação de fornecedores quando com estes houver a troca de informações.

## 5.7. Sigilo da informação

Nenhum colaborador deve divulgar ou fazer uso de informações privilegiadas estratégicas e confidenciais da Fundação em benefício próprio ou de terceiros, independentemente do tipo de mídia ou suporte utilizado.

## 5.8. Continuidade do uso da informação

A PREVINORTE deve manter Plano de Contingência e Plano de Resposta a Incidentes, visando a garantia absoluta da disponibilidade das informações e a continuidade do negócio, inclusive na ocorrência de incidentes ou ameaças à segurança.

## 5.9. Relacionamentos formais com terceiros

As relações formais com terceiros (contratos, convênios, dentre outros) em que houver o compartilhamento de informações da PREVINORTE e/ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos corporativos devem ser precedidos por Termos ou cláusulas de confidencialidade que tratem especificamente da Segurança da Informação.

## 5.10. Temporalidade da informação

As informações com valor comprobatório para fins de auditorias, de conformidade e judiciais devem ser preservadas pela PREVINORTE, em conformidade com normativo específico.

## 5.11. Capacitação

A PREVINORTE deve manter o assunto Segurança da Informação em seus programas de capacitação.

## 5.12. Violações e Penalidades

A PREVINORTE orienta a seus colaboradores, através do Código de Ética e Manual de Conduta, que o descumprimento de algum dos princípios éticos ou compromissos de conduta, bem como a mera tentativa de burlar as diretrizes desta política ou aos controles estabelecidos pela empresa, quando constatada, deve ser tratado como uma violação e pode resultar na adoção de sanções, que poderão partir de uma simples advertência até uma demissão ou perda de mandato, sem prejuízo da adoção

de medidas administrativas e/ou judiciais, quando se tratar, ademais de infrações contratuais e/ou legais.

## 6. Responsabilidades

**Conselho Deliberativo da PREVINORTE** – aprovar esta política e deliberar sobre as diretrizes estratégicas de segurança da informação norteando todo o processo na PREVINORTE.

**Diretoria Executiva da PREVINORTE** – aprovar esta política e os documentos normativos derivados que permitam sua implantação.

**Área de Tecnologia da Informação em conjunto com o Encarregado da PREVINORTE (DPO)** – coordenar o tratamento de incidentes de Segurança da Informação e, consequentemente, acompanhar as investigações e as avaliações dos danos decorrentes da quebra de segurança, apoiar a gestão dos riscos de Segurança da Informação, definindo controles adequados, em conjunto com os gestores das áreas, gerir a matriz corporativa de classificação da informação quanto à restrição de acesso e apoiar a execução das ações para garantir a Segurança da Informação.

**Comitê de Segurança da Informação da PREVINORTE** – manter as diretrizes desta política, monitorar as ações necessárias para o seu cumprimento, manter os documentos normativos desdobrados desta política e promover a cultura de Segurança da Informação por meio de treinamentos e conscientizações na PREVINORTE, bem como apoiar a gestão dos riscos de Segurança da Informação, definindo controles adequados, em conjunto com os gestores das áreas.

**Gestores das áreas** – zelar pelas informações produzidas por sua equipe, realizando sua adequada classificação e autorização de acesso e contingência, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta política.

**Colaboradores** – cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas pela PREVINORTE.

**Áreas de gestão de pessoas** – promover ações de treinamento e desenvolvimento referentes à segurança da informação, incluindo aspectos técnicos, normativos e comportamentais.

## 7. Disposições Gerais

Esta política deve ser lida e considerada em conjunto com outras normas e procedimentos aplicáveis e relevantes adotados pela PREVINORTE. Além disso, ela deve se desdobrar em outro(s) documento(s) normativo(s) específico(s), sempre alinhados às diretrizes e princípios aqui estabelecidos.

As diretrizes aqui estabelecidas devem nortear a atuação de todas as áreas da PREVINORTE, contribuindo para uma visão única e integrada.

A PREVINORTE deve assegurar que esta política seja amplamente divulgada a todos os seus colaboradores, devendo ser disponibilizada a todos que se relacionam com a Fundação e que, direta ou indiretamente, são impactados.

A PREVINORTE deve manter um programa de atualização periódica desta política e dos demais instrumentos regulamentares subordinados a ela, visando garantir que

todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente e alinhados com as estratégias organizacionais.