



# **Política** **Segurança da** **Informação**

---

## SUMÁRIO

OBJETIVO.....	3
PÚBLICO-ALVO .....	3
INTRODUÇÃO .....	3
DIRETRIZES .....	3
PAPÉIS E RESPONSABILIDADES .....	4
PROCESSOS DE SEGURANÇA DA INFORMAÇÃO .....	5
DOCUMENTOS RELACIONADOS.....	12
APROVAÇÃO.....	12
RESPONSÁVEIS PELO DOCUMENTO .....	12
ATUALIZAÇÃO E VIGÊNCIA.....	12
GLOSSÁRIO .....	12
ANEXOS .....	13

---

## OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da Fundação Itaú Unibanco – Previdência Complementar (“Fundação”), dos participantes, assistidos e demais públicos de relacionamento, observando as melhores práticas de mercado e regulamentações aplicáveis, bem como orientar o comportamento dos colaboradores e membros dos órgãos estatutários em relação à promoção da segurança da informação e proteção dos ativos da Fundação.

---

## PÚBLICO-ALVO

Esta política aplica-se aos colaboradores e membros dos órgãos estatutários da Fundação Itaú Unibanco – Previdência Complementar (Fundação).

---

## INTRODUÇÃO

### PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações da Fundação, dos participantes, assistidos e público em geral está fundamentado nos seguintes princípios:

- I. Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas;
- II. Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- III. Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos;
- IV. Autenticidade: garantir a identificação da informação e registro dos acessos e modificações.

---

## DIRETRIZES

A informação é o principal ativo de uma organização. Assim, a Fundação define a estratégia de segurança da Informação para proteger a integridade, disponibilidade e confidencialidade da informação.

Data de publicação: 10/12/2024

Esta estratégia está alinhada às diretrizes da Patrocinadora, que é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética.

Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, em todo o seu ciclo de vida, desde a coleta até o descarte.

A Política de Segurança da Informação deve estar disponível em local acessível aos colaboradores e protegida contra possíveis violações. A Política de Segurança da Informação deverá ser revisada pelo menos anualmente pela Fundação.

A adesão à essa Política e eventuais desvios, são monitorados inclusive por informações da Patrocinadora e seus comitês superiores sempre que o suporte tecnológico for compartilhado.

A informação deve ser utilizada de forma transparente, de acordo com a sua finalidade, grupos de interesse e com a legislação vigente.

As diretrizes e eventuais exceções serão levadas para avaliação dos órgãos estatutários da Fundação.

---

## **PAPÉIS E RESPONSABILIDADES**

As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionadas com o suporte da Patrocinadora, através da Diretoria de Segurança Corporativa e discutidos nos Comitês das áreas da Fundação e/ou no Comitê de Tecnologia e Segurança da Informação e no Comitê de Privacidade.

### **5.1. AUDITORIA INTERNA**

Os papéis e responsabilidades da Auditoria Interna estão descritos na Política de Auditoria Interna (Global).

### **5.2. CONTROLES INTERNOS**

A equipe de Controles Internos e Compliance, em parceria com as equipes de Segurança da Informação da Patrocinadora, é responsável por gerenciar e acompanhar as atividades que se referem ao risco em Tecnologia e Segurança da Informação, bem como realizar a interlocução entre as áreas da Fundação e equipes de SI da Patrocinadora.

### **5.3. SEGURANÇA CORPORATIVA**

As atividades listadas abaixo serão desenvolvidas com o apoio da estrutura de Segurança da Informação da Patrocinadora, em especial quanto a estratégia, objetivos e ações necessárias para a mitigação dos riscos dos processos de segurança da informação, e a

Data de publicação: 10/12/2024

manutenção do parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

- I. Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;
- II. Proteger a informação de ameaças buscando garantir a continuidade dos processos e minimizar os riscos;
- III. Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação (SGSI).
- IV. Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação.
- V. Estabelecer e disseminar uma cultura de segurança da informação.
- VI. Definir as políticas de segurança da informação a serem aplicadas nos processos e tecnologias.

#### **5.4. COMITÊ DE AUDITORIA DA FUNDAÇÃO**

Os papéis e responsabilidades do Comitê de Auditoria da Fundação estão descritos no seu Regulamento Interno, bem como no Manual de Governança da Fundação.

#### **5.5. ÁREAS DA FUNDAÇÃO**

Proteger as informações sob sua responsabilidade.

Em relação aos prestadores de serviços, cabe ao gestor responsável pela contratação monitorar o cumprimento, através do contrato de prestação de serviços firmado entre as partes. Adicionalmente, é responsabilidade da área contratante seguir o fluxo de Avaliação de Riscos em Segurança da Informação em caso de contratação de fornecedores de sistemas, conforme descrito no capítulo “PROCESSOS DE SEGURANÇA DA INFORMAÇÃO” item “e” deste documento e na Política de Contratações e Pagamentos da Fundação.

---

### **PROCESSOS DE SEGURANÇA DA INFORMAÇÃO**

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Fundação adota os seguintes processos:

#### **a. Informação**

Toda informação que a Fundação considerar como relevante, desde tecnológicas (p.ex. software e hardware) como não tecnológicas (p.ex. informações em suporte físico, pessoas, processos e dependências físicas) relacionadas à proteção da informação.

Data de publicação: 10/12/2024

A informação deve ser identificada, inventariada, mantida atualizada, possuir um proprietário e ser protegida contra acessos indevidos. A proteção pode ser, física (p.ex. ambiente com acesso controlado) e lógica (p.ex. configurações de blindagem ou hardening, patch management, autenticação e autorização).

As informações da Fundação, dos participantes e assistidos e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida.

## **b. Classificação da Informação**

As informações devem ser classificadas de acordo com a confidencialidade:

- Acesso amplo, quando se tratar de informações públicas ou tornadas manifestamente públicas pelo titular da informação, que não estão sujeitas a restrição de acesso e compartilhamento, resguardados os direitos do titular dos dados e os princípios estabelecidos na Política Privacidade e Proteção de Dados da Fundação;
- Acesso restrito, quando se tratar de informações coletadas ou disponibilizadas para o cumprimento de contrato e seus procedimentos preliminares ou para o cumprimento de obrigação legal ou regulatória;
- Acesso específico, quando se tratar de informações confidenciais, sigilosas, inclusive dados sensíveis de saúde.

Para isso, devem ser consideradas as necessidades relacionadas aos processos, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

Independentemente de classificação, todas as informações da Fundação somente poderão ser utilizadas para fins profissionais e institucionais, e somente poderão ser compartilhadas a terceiros que estejam diretamente relacionados aos processos a que se referem as informações compartilhadas e mediante lastro contratual (outros colaboradores da Fundação ou da Patrocinadora, fornecedores contratados ou autoridades fiscalizadoras).

## **c. Gestão de Acessos**

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos da Fundação.

As credenciais de login e senha relativas a um colaborador atribuem responsabilidade pelo acesso às informações e ações sobre estas, vale, como assinatura eletrônica e são de uso pessoal, intransferível, vedada a sua exposição, compartilhamento ou acesso por

Data de publicação: 10/12/2024

terceiros, ainda que colaboradores da Fundação. Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

Para tanto, credenciais, suportes tecnológicos ou físicos deverão ser usados para fins profissionais apenas, não devendo o colaborador ter expectativa de sigilo sobre a sua utilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

#### **d. Gestão de Riscos**

Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, identificação de vulnerabilidades, análise de probabilidades e impactos sobre os ativos da Fundação, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nos fóruns apropriados.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, segundo condições de mercado, independentemente de estarem dentro da infraestrutura da Fundação, parceiros ou prestadores de serviços.

As tecnologias em uso pela Fundação devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas de acordo com os processos de gestão de patches.

Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios definidos pela gestão.

#### **e. Gestão de Riscos em Prestadores de Serviços**

Os prestadores de serviços contratados pela Fundação devem ser classificados considerando alguns critérios, conforme documento de Avaliação de Riscos em Segurança da Informação da Patrocinadora.

De acordo com a classificação, o prestador de serviços passará por avaliação de risco, que pode incluir a validação in loco dos controles de Segurança da Informação, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços.

Os prestadores de serviços devem informar os incidentes relevantes, relacionados às informações da Fundação armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares, conforme previsão contratual.

#### **f. Tratamento de Incidentes de Segurança da Informação**

O monitoramento de segurança do ambiente tecnológico da Fundação é feito utilizando-se a estrutura e o suporte da Patrocinadora analisando os eventos e alertas com o objetivo de identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação aos seus respectivos impactos, de acordo com os critérios previamente estabelecidos e o comprometimento de dados. Incidentes classificados como relevantes devem ser comunicados às instâncias de governança da Fundação e ao titular do dado quando envolver dados pessoais e dados pessoais sensíveis que possam causar dano relevante, independentemente das medidas a serem adotadas pelas áreas técnicas. Para tanto, todos os incidentes deverão passar por um processo de tratamento e comunicação, onde são registrados os detalhes pertinentes aos incidentes como causa, impacto, classificação etc.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a gerência de Controle Interno e Compliance da Entidade e na mitigação dos riscos relacionados à segurança da informação.

Eventuais incidentes de vazamentos ou riscos de exposição de dados pessoais tratados pela Fundação deverão ser reportados ao DPO ([dpo\\_fiu@itau-unibanco.com.br](mailto:dpo_fiu@itau-unibanco.com.br)) com a máxima brevidade possível.

#### **g. Conscientização em Segurança da Informação**

A Fundação coordena programas relacionados a disseminação, conscientização, capacitação e fortalecimento dos princípios e diretrizes de Segurança da informação.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, e-learning, e em mídias.

#### **h. Governança com as áreas da Fundação e Tecnologia**

Os Projetos e iniciativas das áreas da Fundação devem estar alinhados com os princípios e diretrizes de segurança da informação.

#### **i. Segurança Física do Ambiente**

O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes.

Os colaboradores deverão manter documentos físicos (papel, pen drive, CD ou outro suporte físico), inclusive pastas, formulários e dados pessoais seus e de terceiros,

Data de publicação: 10/12/2024

participantes e assistidos, em local de acesso restrito, preservado de fácil visualização, acesso ou cópia.

#### **j. Segurança nos Sistemas**

Os sistemas utilizados pela Fundação devem ser estruturados de forma a proteger os dados, principalmente dados pessoais e sensíveis, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, atendendo aos padrões de boas práticas e de governança e aos princípios gerais estabelecidos em Lei.

Em caso de aquisição de novos sistemas, os mesmos deverão ser homologados seguindo o padrão de segurança estabelecido pela Patrocinadora, e conforme a legislação em vigor.

#### **k. Gravação de LOGs**

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

Essas informações devem ser protegidas contra modificações e acessos não autorizados.

#### **l. Programa de Segurança da Informação**

O Programa de Cyber Security definido pela Patrocinadora e praticado na Fundação é norteado pelos seguintes fatores:

- I. Regulamentações vigentes;
- II. Melhores práticas;
- III. Cenário mundiais;
- IV. Análises de risco da própria Entidade.

Conforme sua criticidade, o programa divide-se em:

- I. **Críticas** - Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- II. **Sustentação** - Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Fundação e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- III. **Estruturantes** - Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos.

### **m. Proteção de perímetro**

Para proteção da infraestrutura da Fundação contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de indisponibilidade DDoS, Spam, Phishing, APT/Malware, invasão de dispositivos de rede e servidores, ataques a aplicação além de processos de scan de vulnerabilidades externos e internos e testes de penetração.

Para mitigação do risco de vazamento de informações, a Fundação utiliza ferramentas preventivas da Patrocinadora, instaladas em dispositivos móveis, estações de trabalho e servidores, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares não gerenciados ou não homologados.

**Proteção interna:** Para proteção da infraestrutura contra ataques internos, a Fundação compartilha os processos com a Patrocinadora que utiliza ferramenta de Antimalware homologada contra ameaças cibernéticas. O antimalware é responsável pela detecção, proteção e mitigação dessas ameaças.

## **6.1. PROPRIEDADE INTELECTUAL**

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Pertencem exclusivamente à Fundação todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criadas ou realizadas pelo colaborador da Fundação, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho, de estágio ou trabalhos desenvolvidos por fornecedores contratados pela Fundação, cujas normas de direito de propriedade intelectual estejam disponíveis em contrato. Quaisquer informações e conteúdos cuja propriedade intelectual pertença a Fundação, ou tenham sido por ele disponibilizado, inclusive informações e conteúdo que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da Fundação não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa da Fundação.

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual da Fundação.

## 6.2. DECLARAÇÃO DE RESPONSABILIDADE

Pela confirmação de aceitação e ciência da presente Política, os colaboradores e membros dos órgãos estatutários da Fundação consideram-se formalmente comprometidos a agir segundo os critérios e definições descritas neste documento, bem como a adotar as medidas indicadas, quando aplicável.

Os contratos firmados entre terceiros e a Fundação devem possuir cláusula que assegure a confidencialidade das informações.

## 6.3. SANÇÕES DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas na legislação e nos procedimentos da Fundação.

## 6.4. CANAIS DE COMUNICAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- **Suspeitas de incidentes de segurança da informação?**

Encaminhe e-mail para: [monitoracao\\_soc@itau-unibanco.com.br](mailto:monitoracao_soc@itau-unibanco.com.br) ou [Fundacao\\_CICompliance@correio.itau.com.br](mailto:Fundacao_CICompliance@correio.itau.com.br)

- **Recebeu um e-mail suspeito e deseja enviá-lo para análise?**

Encaminhe e-mail para: [emailsuspeito@itau-unibanco.com.br](mailto:emailsuspeito@itau-unibanco.com.br)

- **Está com dúvida sobre como solicitar, excluir ou alterar um acesso?**

Fale com a Unidade de Relacionamento de Segurança através do Assistente Virtual (Chat) no IU Conecta.

Acesse: <http://pms.itau> > Solicitação de Acessos > Solicitar Acessos > Descrição de Acesso > DÚVIDAS

- **Precisa de uma avaliação de risco de segurança?**

Fale com a Gerência de Avaliação de Risco Segurança da Informação.

Acesse: IU Digital > Avaliação de Riscos de Segurança da Informação (link: [https://itau.service-now.com/tech?id=sc\\_cat\\_item&sys\\_id=290337911bc078d41941dca0f54bcbcf](https://itau.service-now.com/tech?id=sc_cat_item&sys_id=290337911bc078d41941dca0f54bcbcf))

Data de publicação: 10/12/2024

Esta Política Corporativa de Segurança da Informação é complementada por procedimentos específicos de Segurança da Informação da Patrocinadora, em conformidade com os aspectos legais e regulamentares e aprovadas nos fóruns competentes da Fundação.

---

## DOCUMENTOS RELACIONADOS

Lei nº 13.709/2019 (Lei Geral de Proteção de Dados Pessoais).

---

## APROVAÇÃO

Esta Política foi aprovada pela Diretoria Executiva da Fundação em 30/07/2020 e teve sua última atualização realizada em 11/11/2024

---

## RESPONSÁVEIS PELO DOCUMENTO

ETAPA	NOME	DATA
ELABORAÇÃO	Gerência de Controles Internos e Compliance	29/10/2024
APROVAÇÃO	Diretoria Executiva	11/11/2024

---

## ATUALIZAÇÃO E VIGÊNCIA

Esta Política entra em vigor imediatamente após deliberação pela Diretoria Executiva da Fundação. Sempre que houver necessidade de atualizações decorrentes de exigências de legislação ou do órgão regulador, estas serão devidamente comunicadas a todos que se submetem a esta Política.

---

## GLOSSÁRIO

**APT (Advanced Persistent Threat)** – ataques avançados persistentes.

**Cyber Security** – é o termo que designa o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição de informações.

**Interoperabilidade** – Capacidade de um sistema de se comunicar de forma transparente com outro sistema. Para um sistema ser considerado interoperável, é muito importante que ele trabalhe com padrões abertos.

Data de publicação: 10/12/2024

**Parque tecnológico** – conjunto de ativos de infraestrutura e sistemas de tecnologia.

**Patrocinadora** – Itaú Unibanco Holding S.A.

**Segregação de funções** – consiste na separação das atividades entre áreas e pessoas potencialmente conflitantes ou que possuem informações privilegiadas, na qual, o dirigente ou colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

**Antimalware** – categoria de softwares que monitora um computador ou rede de computadores para combater ameaças.

**Patches** – programas que visam atualizar e/ou corrigir erros e/ou vulnerabilidades de um software.

**Hardening** – consiste em processo e documento contendo as melhores práticas de segurança que deve ser aplicado nos ativos de rede com revisão anual ou a cada mudança significativa nos sistemas envolvidos.

---

## ANEXOS

Não há.