POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

1. OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da Fundação Itaú Unibanco de Previdência Complementar ("Fundação"), dos participantes e assistidos e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

2. PÚBLICO ALVO

Colaboradores da Fundação, diretores, conselheiros ou prestadores de serviço que tenham acesso às informações.

3. INTRODUÇÃO

A informação é um dos principais bens de uma organização. Assim, a Fundação define a estratégia de segurança da Informação e Cyber Security para proteger a integridade, disponibilidade e confidencialidade da informação.
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.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações da Fundação, participantes e 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.

5. DIRETRIZES

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 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 e grupos de interesse e com a legislação vigente.
As diretrizes e eventuais exceções serão levadas para avaliação dos órgãos estatutários da Fundação.

6. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

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

a) Gestão de Ativos

Entende-se por ativo toda informação que a Fundação considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos (p.ex. informações em suporte físico, pessoas, processos e dependências físicas) relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário e serem protegidos 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).

Os ativos da Fundação, dos participantes e assistidos e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas

internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade:

- Acesso amplo, quando se tratar de informações públicas ou tornados manifestamente públicas pelo titular da informação, que não estão sujeitos a restrição de acesso e compartilhamento, resguardados os diretos 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 ao negócio, 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 compartilhados 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 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, vulnerabilidades, 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 modo a garantir interoperabilidade e integridade das informações.

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.

Dependendo da 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 e Cyber Security

A monitoração de segurança do ambiente tecnológico da Fundação é feita utilizando-se da estrutura e suporte da Patrocinadora, através da sua área de Cyber, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto 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 pessoas sensíveis que possa 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 detalhamentos pertinentes aos incidentes como causa, impacto, classificação, etc..

A gerência de Controle Interno e Compliance da Fundação elaborará um Relatório Anual contendo os incidentes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes.

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

g) Conscientização em Segurança da Informação e Cyber Security

A Fundação participa dos programas da Patrocinadora relacionados a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas

são veiculadas através de e-mails, portal corporativo, e-learning, telemídias, redes sociais aos colaboradores e clientes.

h) Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas 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, participantes e assistidos, em local de acesso restrito, preservado de fácil visualização, acesso ou cópia.

j) Segurança nos Sistemas

Os sistemas utilizados 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 em Lei.

Em caso de aquisição de novos sistemas, os mesmos deverão ser homologados seguindo o padrão de segurança estabelecido pela Patrocinadora, conforme legislações 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 Cyber Security

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 instituição

Conforme sua criticidade, o programa divide-se em:

I. **Críticas** - Consiste de 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 DDoS, Spam, Phishing, APT/Malware, invasão de dispositivos de rede e servidores, ataques a aplicação e scan externos.

Para mitigação do risco de vazamento de informações, a Fundação utiliza ferramentas preventivas da Patrocinadora, instaladas em dispositivos móveis, estações de trabalho, 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.

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 da Fundação consideram-se formalmente comprometidos a agir segundo os critérios e definições descritas e a adotar as medidas indicadas, quando aplicável.

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

7. 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 fóruns específicos de riscos das áreas e nas Comissões Executivas que tratam Risco Operacional ou Tecnologia.

7.1 Auditoria Interna

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

7.2 Controles Internos

Os papéis e responsabilidades de Controles Internos estão descritos no Manual de Governança da Fundação Itaú Unibanco.

7.3 Segurança Corporativa da estrutura compartilhada pela Patrocinadora

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 do negócio e minimizar os riscos ao negócio;
III. Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação (SGSI) da Patrocinadora.
IV. Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com o Comitê Executivo de Segurança da Informação da Patrocinadora.
V. Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pelos comitês, envolvendo as áreas responsáveis.
VI. Estabelecer e disseminar uma cultura de segurança da informação.
VII. Propor o investimento para a segurança da informação.
VIII. Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.

7.4 Comitê Executivo de Segurança da Informação da Patrocinadora

O Comitê Executivo de Segurança da Informação é composto por membros da Patrocinadora, que tem como dever aprovar a estratégia, objetivos, orçamento e ações necessárias para a mitigação dos riscos dos processos de segurança da informação.

7.5 Comitê de Auditoria da Fundação Itaú Unibanco

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

7.6 Área de Tecnologia da estrutura compartilhada pela Patrocinadora

Manter o parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos, de acordo com as definições da Patrocinadora.

7.7 Fundação Itaú Unibanco

Proteger as informações sob sua responsabilidade.

8. SANÇÕES DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas na legislação e nos procedimentos da Patrocinadora, bem como nas normas internas da Fundação do Itaú Unibanco.

9. DOCUMENTOS RELACIONADOS

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.

10. GLOSSÁRIO

APT (Advanced Persintent Threat): ataques avançados persistentes.

Colaboradores: abrange todos os empregados, menores aprendizes, estagiários e administradores da Fundação, bem como empregados cedidos da Patrocinadora em exercício de funções exclusivamente para a Fundação Itaú Unibanco.

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.

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 colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

11. CANAIS DE COMUNICAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- Suspeitas de incidentes de segurança da informação?
Encaminhe e-mail para: monitoracao_soc@itau-unibanco.com.br ou 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

- Suspeitas de incidentes de segurança da informação?
Encaminhe e-mail para: monitoracao_soc@itau-unibanco.com.br

- Está com dúvida sobre como solicitar, excluir ou alterar um acesso?
Fale com a Unidade de Relacionamento de Segurança
Telefone: 11 2733-8960
Acesse: http://pms.itau > Solicitação de Acessos > Solicitar Acessos > Descrição de Acesso > DÚVIDAS

12. APROVAÇÃO

Esta Política foi aprovada pela Diretoria da Fundação em 30.07.2020

13. RESPONSÁVEIS PELO DOCUMENTO

Etapa	**Nome da área**
Elaboração	Controles Internos e Compliance
Aprovação	Diretoria Executiva Fundação Itaú Unibanco de Previdência Complementar
Órgão Responsável	Diretoria Executiva Fundação Itaú Unibanco de Previdência Complementar