1. Introdução

A segurança da informação é uma prioridade fundamental para a Quanta Previdência Cooperativa. Este documento estabelece diretrizes e responsabilidades para garantir a confidencialidade, integridade e disponibilidade dos ativos de informação da organização. Essa diretriz tem a mesma função do documento conhecido como PSI (Política da Segurança da Informação), foi denominada Diretriz na Quanta devido a tipificação de documentos adota pela Quanta Previdência Cooperativa. Todos os colaboradores, contratados e terceiros devem aderir a esta diretriz.

2. Objetivo

Os principais objetivos dessa diretriz são:

- Proteger informações confidenciais e sensíveis.
- Prevenir acessos não autorizados.
- Garantir a integridade dos dados e sistemas.
- Assegurar a continuidade dos negócios.
- Cumprir com regulamentos de segurança e privacidade.

O cumprimento desses objetivos visa preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações sob a gestão da Entidade nos aspectos físicos, lógicos e comportamentais.

3. Termos e Definições

- **Usuários:** Incluem todos os funcionários, estagiários, aprendizes, conselheiros, terceiros e visitantes com acesso a informações ou recursos da Quanta.
- **Recursos de Tecnologia da Informação (TI):** Englobam hardware e software, como computadores, servidores, notebooks, smartphones, telefones, arquivos digitais, dispositivos de rede, internet, impressoras e e-mail.
- **Software:** Refere-se a todos os programas instalados nos computadores fornecidos pela equipe de TI para fins operacionais.
- **Ambiente Lógico:** Define o ambiente eletrônico e controlado onde informações públicas ou confidenciais, softwares e sistemas são armazenados e circulam.
- **Ambiente físico:** Refere-se às instalações físicas que compõem a estrutura da Entidade.
- **Entidade:** QUANTA PREVIDÊNCIA COOPERATIVA

4. Âmbito da Aplicação

Esta Diretriz de Segurança da Informação aplica-se a toda estrutura organizacional da Entidade, incluindo seus prestadores de serviço, clientes, fornecedores e parceiros.

5. Base legal e regulamentar

A Entidade compromete-se a cumprir todas as regulamentações relevantes de segurança e privacidade de dados.

Esta diretriz de segurança é uma parte essencial da cultura da Entidade e deve ser seguida por todos os colaboradores. O não cumprimento desta diretriz pode resultar em medidas disciplinares, incluindo ações legais, dependendo da gravidade da violação.

Para a elaboração dessa diretriz tomou-se como base, referências normativas como as abaixo:

- NBR ISO/IEC 27001:2022 – Sistemas de Gestão da Segurança da Informação – Requisitos;
- NBR ISO/IEC 27002:2022 – Técnicas de segurança - Código de Prática para controles de Segurança da Informação;
- NBR ISO/IEC 27005:2022 – Técnicas de segurança - Gestão de Riscos de Segurança da Informação;
- Lei Geral de Proteção de Dados Pessoais (LGPD).

6. Princípios Fundamentais

1. Todos os dados e informações produzidas para a Entidade, total ou parcialmente, tanto físicas quanto lógicas, são de propriedade da Entidade, assim como os recursos de TI fornecidos para o armazenamento, acesso e o controle destas.

2. Todos os recursos baseados em Tecnologia da Informação ou produzidos por estes, estão sujeitos ao monitoramento e rastreabilidade, possibilitando a pronta resposta à incidentes de segurança.

3. A Entidade, como custodiante de dados e informações de Participantes, Assistidos, Beneficiários, Ex-participantes, Instituidores e Parceiros, os declara sigilosos, logo devem ser tratados assim pelos seus Funcionários, Terceiros e Visitantes.

4. Os recursos de TI devem ser usados apenas para fins comerciais autorizados.

5. Senhas e credenciais não devem ser compartilhadas.

6. O acesso de funcionários, Terceiros e Visitantes aos ambientes lógicos e físicos é restrito e controlado. O acesso inicial considerará o princípio do menor privilégio, que estabelece os recursos mínimos de trabalho e uso, podendo ser alterado conforme as atividades definidas pelo processo, alçada, cargo ou função. O preenchimento e assinatura do Termo de Responsabilidade e Confidencialidade é condição inegociável para a concessão de chaves de acesso e senhas aos ambientes lógicos e físicos.

7. O acesso deve ser encerrado quando não for mais necessário. Encerrar não significa necessariamente excluir, pois existem acessos que são mantidos devido validade de dados ou necessidades processuais

8. Todos os usuários de dados e informações devem estar atentos e comprometidos com a Gestão dos Riscos, auxiliando na identificação dos tipos de exposição, avaliação das probabilidades de incidência e impactos, baseados nos processos operacionais da Entidade.

9. Os dados e informações, independente do seu formato, devem ser classificados quanto a sua confidencialidade, conforme sua importância estratégica para a Entidade. A classificação definirá a forma como serão armazenadas, copiadas, transmitidas, manuseadas, descartadas ou destruídas. As informações não classificadas são declaradas sigilosas.

10. É dever de todos proteger informações sensíveis contra acesso não autorizado.

11. Esta Diretriz e todos os seus complementos devem integrar os contratos e acordos comerciais, definindo claramente os papéis, responsabilidades e os acordos de confidencialidade das partes envolvidas, quanto aos níveis de processamento de dados e informações, segurança, monitoramento e requisitos de contingência.

12. Todos os usuários serão treinados e conscientizados quanto ao uso correto dos recursos que produzem ou manuseiam dados e informações.

13. Todos os usuários devem receber treinamento em segurança da informação e LGPD.

14. Todos os usuários devem relatar incidentes de segurança ao time de infraestrutura imediatamente.

15. Todos os usuários devem colaborar na investigação e mitigação de incidentes.

16. Os Funcionários, Terceiros e Parceiros devem utilizar os recursos e informações, seguindo os princípios do Código de Ética e da Segurança da Informação, sem afetar ou causar prejuízo a outrem. Todas as espécies de pressões e chantagens devem ser denunciadas.

17. No que se refere às informações em custódia da Entidade, considera-se proibido tudo aquilo que não esteja previamente autorizado por esta diretriz e demais documentos normativos.

7. Responsabilidades

7.1 Diretoria Executiva

- Estabelecer uma cultura de segurança.
- Alocar recursos para implementação de medidas de segurança.
- Revisar e aprovar a diretriz de segurança.
- Definir e aplicar sanções, conforme Código de Ética, normativos internos e legislação vigente.

7.2 Gerência de Infraestrutura e Gerência de Sistemas e Canais

- Implementar e manter controles de segurança.
- Monitorar ameaças e vulnerabilidades.
- Responder a incidentes de segurança.
- Manter a diretriz de segurança atualizada.
- Disponibilizar recursos e garantir o cumprimento desta diretriz.

- Manter o Comitê de Segurança da Informação e LGPD, que analisa os riscos da Entidade sobre o aspecto da segurança das informações.
- Propor normas específicas para regular comportamentos, dados e informações.

7.3 Gerência de Riscos e Compliance (GRC)

- Zelar, em nível físico e lógico, pelos ativos de informações e de processamento.
- Monitorar e reportar qualquer uso inadequado de dados, informações ou condutas que possam ferir esta diretriz.
- Implementar normas específicas para regular recursos baseados em tecnologia.
- Monitorar o setor de atuação da Entidade e encaminhar para as gerências conforme necessário, normativas, novidades e informações relacionadas ao tema de segurança.

7.4 Dos Funcionários, terceiros e usuários

- Preservar a integridade e guardar sigilo das informações que fazem uso, bem como zelar e proteger os respectivos recursos usados para produzir, acessar ou armazenar os dados e informações, protegendo informações confidenciais.
- Usar senhas fortes e proteger suas credenciais.
- Cumprir e disseminar os princípios desta diretriz, sob pena de incorrer em sanções disciplinares e legais cabíveis.
- Reportar incidentes de segurança imediatamente.
- Utilizar recursos, dados e informações da Entidade somente para os fins a que se destinam.
- Responder pelo uso de recursos e informações, bem como seus efeitos.

8. Revisão e Atualização

A equipe de segurança revisará e atualizará essa diretriz anualmente ou conforme necessidade, baseado em mudanças nas ameaças cibernéticas ou nas regulamentações.

9. Documentos integrantes

- POL05 - Estatuto Quanta Previdência Cooperativa;
- POL07 - Política de Ética e Conduta;
- POL13 - Política de Gestão de Riscos;
- DR70 - Diretrizes do GT de segurança da informação e LGPD.