Política de Ciclo de Vida da Informação

Classificação, rotulagem, transferência, retenção e descarte seguro da informação na PX.Center

Código:	*POL-SGI-001*
Área responsável:	*Segurança da Informação*
Data de emissão:	*24/06/2026*
Responsável pela aprovação:	*CISO / CTO*

1. FINALIDADE/OBJETIVO

Esta política estabelece as diretrizes obrigatórias de classificação, rotulagem, transferência, retenção e descarte seguro da informação ao longo de todo o seu ciclo de vida na PX.Center, em conformidade com os controles A.5.9 a A.5.14, A.5.33, A.7.10, A.7.14, A.8.10 e A.8.12 da ISO/IEC 27001:2022 e em integração com a POL-SEG-001 (Política de Segurança da Informação).

O documento define como a Organização classifica, rotula, compartilha, retém e elimina a informação para preservar sua confidencialidade, integridade e disponibilidade em qualquer formato ou meio.

2. ESCOPO/APLICABILIDADE

Esta política aplica-se à informação tratada pela PX.Center em qualquer formato ou meio, seja físico, digital ou oral, e a toda pessoa que a acesse ou utilize: colaboradores, estagiários, prestadores de serviço, consultores e parceiros.

A definição da PX.Center como entidade de referência abrange os demais CNPJs do grupo, dispensando documento específico por entidade. As disposições aqui estabelecidas observam-se em conjunto com a POL-SEG-001 e com os demais normativos de segurança, privacidade e controle de acessos.

3. USUÁRIOS/PÚBLICO-ALVO

Direção, CISO, CTO, Líder de Segurança da Informação, gestores de área na condição de donos da informação, áreas Jurídica e de Privacidade, e todos os colaboradores, prestadores de serviço e terceiros que tratem informação da Organização.

4. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001:2022 (controles A.5.9 a A.5.14, A.5.33, A.7.10, A.7.14, A.8.10, A.8.12)
- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- Lei 12.965/2014 (Marco Civil da Internet)
- POL-SEG-001: Política de Segurança da Informação
- POL-SEG-006: Política de Uso e Controles Criptográficos
- POL-SEG-016: Política de Controle de Acessos
- POL-SGI-002: Política de Controle de Registros
- POL-SEG-005: Política de Descarte e Destruição
- POL-SEG-003: Política de Cópias de Segurança
- POL-SEG-002: Política de Gestão de Incidentes
- POL-SEG-029: Política de Privacidade e Proteção de Dados Pessoais
- INT-SEG-001: Classificação da Informação

- POL-SEG-011: Política de Segurança de Fornecedores

5. DIRETRIZES / REGRAS / CONTROLES

5.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação da PX.Center é classificada conforme sua sensibilidade e criticidade. Constitui dever do gestor que origina ou utiliza a informação atribuir a classificação, com apoio da Segurança da Informação. São obrigatórios quatro níveis. Público: informação cuja divulgação externa não causa prejuízo, como material institucional já publicado. Interno: informação de uso restrito ao quadro da Organização, como comunicados e instruções de trabalho. Restrito: informação cujo acesso se limita a áreas ou funções específicas, como relatórios financeiros e dados de projetos. Confidencial:

informação de alta criticidade, como dados pessoais sensíveis, segredos de negócio, código-fonte proprietário e credenciais, cuja divulgação acarreta dano legal, financeiro ou reputacional relevante.

5.2 ROTULAGEM DA INFORMAÇÃO

É obrigatório rotular a informação classificada como Interno, Restrito ou Confidencial. Em meio físico, a indicação consta em carimbo, etiqueta, cabeçalho ou rodapé. Em meio digital, aplicam-se os rótulos de sensibilidade corporativos, conforme a INT-SEG-001. Em comunicações orais que tratem assunto Restrito ou Confidencial, o responsável sinaliza o caráter sensível no início e limita a participação às pessoas envolvidas.

5.3 TRANSFERÊNCIA E COMPARTILHAMENTO

A transferência de informação ocorre apenas por canais corporativos homologados: e-mail corporativo, ferramentas corporativas de colaboração e repositórios corporativos. É vedado compartilhar informação sem finalidade legítima e sem necessidade de conhecimento do destinatário. Informação Restrita ou Confidencial trafega com controle de acesso ao destinatário e criptografia, conforme a POL-SEG-006. O aplicativo de mensageria corporativo integrado restringe-se ao atendimento ao cliente e é vedado para dados Restritos ou Confidenciais.

5.4 RELAÇÃO COM TERCEIROS E ACORDOS DE CONFIDENCIALIDADE

O compartilhamento de informação classificada com terceiros é condicionado à assinatura de acordo de confidencialidade (NDA) e a cláusulas contratuais de sigilo, controles mínimos de segurança, notificação de incidentes e devolução ou descarte seguro ao término da relação. Os requisitos de segurança aplicáveis a fornecedores e terceiros seguem a POL-SEG-011 (Política de Segurança de Fornecedores); quando houver tratamento de dados pessoais, observam-se a LGPD e a POL-SEG-029.

5.5 RETENÇÃO DA INFORMAÇÃO

A retenção observa os prazos exigidos por lei, regulamento ou contrato e a necessidade operacional da Organização. É vedado reter informação por prazo superior ao necessário. As cópias de segurança seguem a POL-SEG-003 e os registros seguem a POL-SGI-002. Encerrado o prazo, a informação é eliminada, anonimizada ou mantida apenas mediante justificativa documentada.

5.6 DESCARTE E DESTRUIÇÃO SEGURA

Ao término do prazo de retenção, a informação e as mídias que a armazenam são descartadas de modo irreversível e proporcional à classificação. Os procedimentos de descarte e destruição segura, como fragmentação, sobrescrita, destruição física e registro do descarte, seguem a POL-SEG-005 (Política de Descarte e Destruição).

5.7 EXCEÇÕES

Toda exceção a esta política é prévia, fundamentada, de prazo limitado e acompanhada de medidas compensatórias. A Segurança da Informação avalia e aprova a exceção e registra justificativa, escopo, prazo e controles adicionais, com revisão periódica até o retorno à diretriz padrão.

6. RESPONSABILIDADES

A Direção aprova esta política e provê os recursos necessários à sua execução. O CISO e o CTO definem os controles de ciclo de vida da informação e respondem por sua manutenção. O Líder de Segurança da Informação coordena a aplicação da política, avalia exceções e conduz o tratamento de incidentes conforme a POL-SEG-002. Os gestores de área, na condição de donos da informação, classificam a informação sob sua responsabilidade e asseguram o cumprimento desta política por suas equipes. A área Jurídica analisa NDAs e cláusulas contratuais de sigilo.

Os usuários protegem a informação sob sua guarda, observam a classificação e a rotulagem e reportam incidentes pelo canal security@px.center; questões de privacidade e LGPD seguem ao canal dpo@px.center.

7. GESTÃO DE REGISTROS

Os registros desta política compreendem os registros de classificação, as exceções aprovadas e os comprovantes de descarte de informação sensível. Os rótulos de sensibilidade residem na solução corporativa de classificação. As versões desta política residem no repositório documental do SGI. É obrigatório preservar a integridade dos registros, com acesso restrito por necessidade de conhecimento, e mantê-los disponíveis para auditorias internas e externas do SGI. Incidentes que envolvam informação seguem o tratamento da POL-SEG-002.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor em 24/06/2026, com validade por prazo indeterminado. A Segurança da Informação revisa o documento anualmente ou diante de mudança legal ou regulatória, incidente relevante ou adoção de nova tecnologia que afete os controles aqui definidos. O descumprimento desta política sujeita o infrator às medidas disciplinares previstas nas normas internas da PX.Center.

9. ANEXOS

Não há anexos. Os registros operacionais residem nos sistemas indicados na seção Gestão de Registros.

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Criador	Descrição de Alterações
00	09/02/2026	Setor de Cybersegurança	Criação e Revisão
01	24/06/2026	SGI	Recodificação para sigla