Política de Segurança da Informação

Diretrizes corporativas de proteção dos ativos de informação da PX.Center e instituição do SGSI

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

1. FINALIDADE/OBJETIVO

A PX.CENTER LTDA. (doravante denominada "PX.Center" ou "Organização") institui a presente Política de Segurança da Informação (PSI) como o pilar estratégico e normativo destinado à proteção dos ativos de informação de sua propriedade, bem como daqueles sob custódia de todas as suas empresas controladas e subordinadas, no âmbito de todas as unidades de negócio e sociedades sob sua gestão.

A segurança da informação é compreendida pela Organização não apenas como um controle operacional, mas como um ativo de viabilização de negócios e um requisito mandatório de resiliência, visando assegurar a estrita observância aos princípios da confidencialidade, integridade e disponibilidade dos dados.

O objetivo desta política é estabelecer diretrizes de governança que orientam o Sistema de Gestão de Segurança da Informação (SGSI), de modo a mitigar riscos tecnológicos e humanos e assegurar que o tratamento de dados pessoais e corporativos esteja em conformidade com a Lei 13.709/2018 (Lei Geral de Proteção de Dados, LGPD) e com padrões internacionais de segurança.

O compromisso da Alta Direção da PX.Center com este corpo normativo reflete a busca incessante pela integridade reputacional e pelo cumprimento das obrigações contratuais e regulatórias vigentes, sendo a adesão a estas normas um dever inerente a todos os seus stakeholders.

2. ESCOPO/APLICABILIDADE

Esta política possui abrangência corporativa e sua aplicação é de caráter mandatório e irrestrito a todas as unidades de negócio, departamentos e sociedades sob gestão da PX.Center. O escopo estende-se, sem exceções, a todos os stakeholders, incluindo colaboradores de qualquer nível hierárquico, estagiários, diretores, conselheiros, prestadores de serviço, consultores e parceiros comerciais que, em virtude de suas atribuições, utilizem a infraestrutura tecnológica ou processem informações de propriedade da Organização.

A observância destas diretrizes abrange todos os ativos de informação, incluindo sistemas de software, bases de dados, redes de comunicação, dispositivos físicos, ambientes de computação em nuvem e documentos. Seu cumprimento é condição essencial para a manutenção do vínculo empregatício ou contratual com a PX.Center, e o acesso aos recursos informacionais da Organização pressupõe a aceitação formal dos termos e obrigações aqui estabelecidos.

Todos os colaboradores, estagiários e terceiros com acesso a informações da PX.Center devem assinar Acordo de Confidencialidade e Não Divulgação (NDA) ou documento equivalente antes do início de suas atividades, com vigência que se estende após o encerramento do vínculo pelo período definido em norma técnica complementar, não inferior a dois anos para informações classificadas como Restritas.

A PX.Center deve assegurar que prestadores de serviço, consultores, parceiros comerciais e demais terceiros com acesso a ativos de informação estejam vinculados a cláusulas contratuais específicas de segurança da informação e proteção de dados, compatíveis com os riscos das atividades desempenhadas, podendo ser submetidos a avaliações de risco, auditorias e exigências adicionais de controles.

Os fornecedores e parceiros devem ser classificados por nível de risco, em Alto, Médio ou Baixo, com base no tipo de acesso a ativos de informação, no volume de dados pessoais tratados e na criticidade dos serviços prestados. Os Fornecedores de Alto Risco devem ser submetidos a avaliação de segurança e due diligence antes da contratação e anualmente durante a vigência do contrato.

Esses terceiros devem comunicar à PX.Center, no prazo máximo definido contratualmente, não podendo exceder 30 (trinta) dias corridos, qualquer incidente de segurança ou violação de dados que possa afetar a Organização ou titulares de dados pessoais.

3. USUÁRIOS/PÚBLICO-ALVO

Alta Direção, Comitê de Segurança da Informação e Privacidade (CSIP), Gestor de Segurança da Informação (CISO), Encarregado de Proteção de Dados (DPO), gestores de área, proprietários de ativos de informação e todos os colaboradores, estagiários, prestadores de serviço, consultores e parceiros comerciais que utilizem recursos tecnológicos ou processem informações em nome da PX.Center.

4. DOCUMENTOS DE REFERÊNCIA

- Lei 13.709/2018 (Lei Geral de Proteção de Dados, LGPD)
- Lei 12.965/2014 (Marco Civil da Internet)
- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- Código de Ética e Conduta da PX.Center
- MAN-SGI-001 (Manual do SGI)
- PLC-17-002 (Declaração de Aplicabilidade do SGSI)
- POL-SEG-016 (Norma Técnica de Controle de Acessos)
- POL-SEG-029 (Política de Privacidade e Proteção de Dados Pessoais)
- POL-SEG-027 (Política de Governança em Privacidade)
- POL-SEG-002 (Política de Gestão de Incidentes)
- POL-SEG-017 (Política de Treinamento e Conscientização)
- POL-SGI-001 (Política de Ciclo de Vida da Informação)
- POL-SEG-004 (Metodologia de Gestão de Riscos)
- POL-SGI-002 (Política de Controle de Registros)
- Política de Classificação da Informação
- Normas Técnicas de Gestão de Ativos, Backup e Continuidade de Negócios

A eventual ausência de detalhamento técnico sobre um controle específico nesta política não exime o indivíduo do cumprimento das obrigações contidas nas normas técnicas complementares. Em caso de conflito entre este documento e as normas específicas, prevalecem as diretrizes desta PSI, salvo disposição em contrário formalmente deliberada pelo Comitê de Segurança da Informação e Privacidade.

5. DIRETRIZES / REGRAS / CONTROLES

5.1 ESTRUTURA DE GOVERNANÇA

A governança da segurança da informação é exercida de forma centralizada pela PX.Center, que detém a autoridade para estabelecer as diretrizes e controles aplicáveis a todas as sociedades sob sua gestão. A Alta Direção assume a responsabilidade pelo provimento dos recursos necessários e pelo respaldo estratégico ao SGSI, devendo garantir o alinhamento entre a proteção dos ativos e os objetivos de negócio.

A estrutura de supervisão é composta pelo Comitê de Segurança da Informação e Privacidade (CSIP), órgão colegiado multidisciplinar responsável por deliberar sobre investimentos, aprovar revisões normativas e monitorar a eficácia dos controles internos, com autonomia para intervir em processos que apresentem riscos críticos à continuidade das operações ou à conformidade legal; pelo Gestor de Segurança da Informação (CISO), responsável pela implementação técnica do SGSI, pela coordenação das respostas a incidentes e pela auditoria dos controles lógicos e físicos de todas as unidades de negócio; e pelo Encarregado de Proteção de Dados (DPO), responsável pela comunicação oficial junto à Autoridade Nacional de Proteção de Dados (ANPD) e pelo zelo aos direitos dos titulares, atuando de forma transversal para garantir o cumprimento da LGPD.

É dever de todo colaborador e terceiro observar as normas de conduta estabelecidas, zelar pelo sigilo das informações e reportar, de forma imediata e obrigatória, qualquer evento suspeito através dos canais oficiais da Organização.

A PX.Center deve manter e atualizar uma Declaração de Aplicabilidade (SoA), formalizada na PLC-17-002, que documenta quais controles do Anexo A da ISO/IEC 27001:2022 são aplicáveis à Organização, com as respectivas justificativas de inclusão ou exclusão e o estado de implementação, conforme o requisito §6.1.3 da norma, constituindo a base de auditabilidade e certificabilidade do SGSI.

A Alta Direção da PX.Center deve realizar análise crítica do SGSI ao menos anualmente, com pauta mínima definida em norma técnica complementar, abrangendo o desempenho dos indicadores, os resultados de auditorias, o status do tratamento de riscos e as decisões de melhoria, devendo os resultados ser registrados formalmente, conforme §9.3 da ISO/IEC 27001:2022.

A PX.Center deve definir, documentar e monitorar objetivos de segurança da informação mensuráveis, incluindo indicadores de desempenho (KPIs) alinhados ao contexto de risco do negócio, os quais devem ser revisados na análise crítica conduzida pela Alta Direção ao menos anualmente, conforme §6.2 da ISO/IEC 27001:2022.

A PX.Center compromete-se com a melhoria contínua de seu SGSI, devendo promover revisões periódicas de seus objetivos, indicadores e controles, de forma a adequá-los às mudanças tecnológicas, regulatórias e de contexto de risco do negócio. A Alta Direção deve assegurar que os resultados das avaliações, auditorias e incidentes sejam considerados na atualização desta política e dos demais normativos correlatos.

5.2 GESTÃO DE RISCOS E CLASSIFICAÇÃO DA INFORMAÇÃO

A PX.Center adota metodologia de gestão baseada em riscos para priorizar a proteção de seus ativos de informação, por meio de avaliações periódicas que identificam, analisam e tratam ameaças que possam comprometer a continuidade das operações ou a privacidade dos dados sob sua custódia. A metodologia de gestão de riscos, a escala de probabilidade e impacto, o limiar de aceitação e o apetite a risco da Organização devem ser estabelecidos em documento complementar formalmente aprovado pelo CSIP, com revisão mínima anual, conforme §6.1.2 da ISO/IEC 27001:2022.

Todo novo projeto, sistema ou contratação de fornecedor crítico deve ser precedido de análise de impacto à segurança e à privacidade, garantindo que os controles preventivos sejam integrados desde a fase de concepção (Privacy by Design). Mudanças relevantes em processos de negócio, criação de novos produtos ou serviços digitais e integrações significativas com sistemas de terceiros também devem ser precedidas dessa avaliação, cujos resultados orientarão a definição e a implementação dos controles adicionais necessários à mitigação dos riscos identificados.

Para assegurar o tratamento adequado e o controle de acesso, a informação na Organização deve ser categorizada conforme seu nível de criticidade e sensibilidade. Informação Pública é aquela cujo acesso externo não gera impacto negativo à PX.Center ou a terceiros. Informação Interna corresponde a dados de uso operacional cotidiano que, se expostos indevidamente, podem causar prejuízos operacionais leves ou administrativos.

Informação Confidencial abrange dados estratégicos, segredos de negócio ou dados pessoais, cujo acesso é restrito exclusivamente a indivíduos com necessidade funcional de conhecê-los. Informação Restrita compreende dados críticos de alta sensibilidade, cujo vazamento ou perda pode resultar em sanções legais graves, danos irreparáveis à reputação ou prejuízos financeiros severos.

A proteção das informações abrange também documentos físicos e mídias de armazenamento não digitais. Registros que contenham informações Internas, Confidenciais ou Restritas devem ser armazenados em locais adequadamente protegidos, com acesso físico controlado e compatível com seu nível de criticidade. O descarte de documentos e mídias que contenham informações sensíveis deve observar procedimentos de destruição segura, como trituração, descarte por empresa especializada ou destruição física de mídias, de modo a impedir a recuperação não autorizada de seu conteúdo.

A atribuição do nível de classificação e a definição dos direitos de acesso são de responsabilidade do proprietário da informação, e o manuseio, armazenamento e descarte de ativos devem seguir rigorosamente os procedimentos estabelecidos nas normas complementares da PX.Center.

Os registros de acesso, uso de sistemas e tráfego de rede poderão ser coletados e analisados pela PX.Center para fins de segurança da informação, cumprimento de obrigações legais e proteção de seus ativos, em conformidade com a legislação aplicável. Os usuários ficam cientificados de que não devem ter expectativa de privacidade quanto ao uso de recursos tecnológicos corporativos e devem utilizá-los em observância aos normativos internos vigentes.

5.3 PROGRAMA DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

A PX.Center deve manter Programa Corporativo de Conscientização em Segurança da Informação de participação obrigatória para todos os colaboradores e terceiros com acesso a ativos de informação, com frequência mínima anual e conteúdo atualizado conforme o cenário de ameaças vigente, incluindo engenharia social, phishing e uso seguro de Inteligência Artificial.

O registro de conclusão deve ser mantido como evidência para auditorias, e simulações de phishing e avaliações de conhecimento poderão ser aplicadas periodicamente para aferir a eficácia do programa, em conformidade com o Controle A.6.3 da ISO/IEC 27001:2022.

5.4 GESTÃO DE ATIVOS E ACESSO FÍSICO

O acesso às dependências físicas da PX.Center é controlado por mecanismos formais de identificação, sendo obrigatório o uso de crachá por todos os colaboradores, estagiários, prestadores de serviço e visitantes durante sua permanência nas instalações. A entrada em áreas internas, especialmente as classificadas como críticas, depende de autenticação em sistemas de controle de acesso, que podem incluir validação por crachá e reconhecimento facial, garantindo a rastreabilidade de todas as entradas e saídas.

É vedado o compartilhamento de crachás ou a permissão de ingresso de pessoas não autorizadas, devendo qualquer perda, extravio ou suspeita de uso indevido ser comunicada imediatamente pelos canais oficiais. Todo terceiro ou visitante deve possuir cadastro prévio e estar vinculado a um responsável interno, com acesso condicionado à validação de identidade e ao registro de horários de entrada e saída. A Organização poderá estabelecer zonas de acesso com diferentes níveis de restrição física, de forma alinhada à criticidade dos ativos e informações ali presentes.

Todos os equipamentos, dispositivos móveis, mídias de armazenamento e demais recursos tecnológicos fornecidos pela PX.Center são de propriedade exclusiva da Organização e devem ser utilizados estritamente para finalidades profissionais, cabendo ao usuário o zelo pela integridade física e pela segurança lógica dos ativos sob sua guarda.

A Organização deve manter inventário atualizado de ativos, com registro de responsável, localização e status, sendo proibida a instalação de softwares não autorizados, o uso de equipamentos pessoais em desacordo com as normas internas e a alteração de configurações de segurança sem anuência prévia do departamento de tecnologia. Em caso de desligamento, mudança de função ou término de contrato, todos os ativos e informações de propriedade da PX.Center devem ser restituídos de imediato, em conformidade com os procedimentos internos de devolução e revogação de acessos.

O uso de dispositivos pessoais para acesso a recursos corporativos (BYOD) somente é permitido quando expressamente autorizado e condicionado ao atendimento dos requisitos de segurança definidos em normas técnicas específicas, incluindo mecanismos de proteção contra malware, criptografia e capacidade de gestão remota. A utilização de mídias removíveis, como pen drives e discos externos, deve ser restrita, sujeita a controles técnicos de proteção e, sempre que possível, substituída por soluções corporativas seguras de compartilhamento e armazenamento de arquivos.

5.5 CONTROLE DE ACESSO E GESTÃO DE IDENTIDADES

O acesso aos recursos informacionais da PX.Center deve ser concedido de forma restritiva e controlada, fundamentado nos princípios do privilégio mínimo (PoLP) e da necessidade de conhecer (Need to Know). A Organização deve assegurar que cada usuário possua acesso estritamente limitado às informações e sistemas indispensáveis ao desempenho de suas atribuições funcionais.

A concessão, alteração ou revogação desses acessos deve seguir processos formais de autorização, sendo obrigatória a revisão periódica das permissões para garantir que permaneçam alinhadas às atividades vigentes do colaborador ou terceiro.

A autenticação nos sistemas e redes da PX.Center deve ser realizada por meio de credenciais individuais e intransferíveis, sendo vedado o compartilhamento de senhas ou a utilização de contas genéricas para atividades rotineiras. A Organização deve implementar mecanismos de autenticação multifator (MFA) e monitorar os logs de acesso para fins de auditoria e investigação de incidentes, garantindo a rastreabilidade de todas as ações executadas em sua infraestrutura tecnológica.

Todas as credenciais de acesso, incluindo senhas, tokens, chaves de API e demais meios de autenticação, devem ser armazenadas e transmitidas de forma segura, observando padrões de criptografia e o uso de cofres de senhas ou soluções corporativas equivalentes, sendo vedada sua anotação em locais inseguros, o armazenamento em texto aberto ou o envio por canais não autorizados, como e-mail pessoal ou aplicativos de mensagens.

A definição, renovação e recuperação de senhas devem seguir os procedimentos internos estabelecidos, assegurando combinações fortes, a troca periódica quando aplicável e a imediata alteração em caso de suspeita de comprometimento.

As contas com privilégios administrativos devem ser gerenciadas por solução de Gestão de Acessos Privilegiados (PAM), com autenticação multifator obrigatória, gravação de sessões auditável, rotação periódica de credenciais e uso exclusivo para tarefas que requeiram tais privilégios. As contas de administrador local em estações de trabalho devem ser desabilitadas ou gerenciadas pela solução de PAM corporativa, em conformidade com o Controle A.8.2 da ISO/IEC 27001:2022.

Os processos de criação, alteração e revogação de contas de usuário devem seguir fluxos formais de gestão de identidades, garantindo que novos acessos sejam devidamente autorizados, que mudanças de função resultem na imediata adequação de perfis e que os acessos de colaboradores desligados ou terceiros desvinculados sejam revogados no prazo máximo de 15 (quinze) dias úteis. A manutenção de contas órfãs ou desnecessárias é vedada,

devendo ser periodicamente verificada pelas áreas responsáveis em conjunto com o setor de tecnologia.

5.6 USO DA INTERNET, REDES SOCIAIS E INTELIGÊNCIA ARTIFICIAL

O acesso à internet fornecido pela Organização destina-se exclusivamente ao suporte das atividades profissionais. A PX.Center poderá implementar filtros de conteúdo, monitorar o tráfego de dados e bloquear o acesso a sítios eletrônicos que apresentem riscos de segurança ou sejam incompatíveis com suas diretrizes éticas.

O uso de redes sociais a partir de recursos corporativos é permitido aos colaboradores cujas funções de negócio o exijam, em especial nas áreas de Marketing e Comercial, restrito às finalidades institucionais e vedada a divulgação de informações confidenciais ou de dados pessoais por esses canais. Para as demais funções, o uso pessoal de redes sociais a partir dos recursos corporativos é proibido.

Quanto ao uso de ferramentas de Inteligência Artificial, é terminantemente proibida a inserção de dados pessoais, segredos de negócio, códigos-fonte proprietários ou informações confidenciais da Organização em ferramentas de IA generativa públicas sem avaliação prévia de segurança e aprovação do CISO. Todo resultado gerado por IA deve ser revisado por profissional qualificado antes de sua aplicação, sendo a responsabilidade final pelo conteúdo ou código integralmente do usuário humano.

O uso de IA para geração de ativos deve respeitar os direitos de propriedade intelectual, sendo vedada a violação de direitos autorais de terceiros que possam comprometer a PX.Center.

5.7 DESENVOLVIMENTO SEGURO DE SOFTWARE

Sendo a tecnologia a atividade fim da PX.Center, o ciclo de desenvolvimento de sistemas deve integrar controles de segurança em todas as suas fases (Security by Design), sendo a segurança um requisito mandatório desde a concepção do produto. É obrigatória a segregação lógica e física entre os ambientes de desenvolvimento, homologação e produção; em nenhuma hipótese dados reais de clientes ou dados pessoais protegidos pela LGPD podem ser utilizados nos ambientes de desenvolvimento ou teste.

Quando necessário o uso de dados com estrutura similar à de produção para fins de teste, devem ser empregadas técnicas de mascaramento, pseudonimização ou geração sintética de dados, de forma a preservar o formato sem expor informações pessoais reais, conforme o Controle A.8.11 da ISO/IEC 27001:2022 e o Art. 13 da LGPD. Todo código-fonte deve ser submetido a análises de segurança (SAST/DAST) antes de sua promoção para produção, visando identificar e corrigir falhas antes que sejam exploradas.

O uso de bibliotecas de terceiros ou componentes open-source deve ser monitorado para garantir a utilização de versões estáveis e livres de vulnerabilidades conhecidas. O acesso aos repositórios de código da PX.Center é restrito e auditável, e qualquer alteração em sistemas críticos deve passar por processo de revisão por pares (code review).

5.8 SEGURANÇA EM OPERAÇÕES E REDES

A PX.Center deve manter controles técnicos e administrativos para garantir a integridade dos sistemas e a segurança das comunicações trafegadas em sua infraestrutura. As operações de rede devem ser protegidas por mecanismos de defesa perimetral, criptografia de dados em trânsito e ferramentas de monitoramento contínuo contra intrusões e códigos maliciosos. A gestão das configurações de rede e de servidores é restrita a profissionais autorizados e deve ser documentada para assegurar a rastreabilidade e a conformidade com as normas de segurança da Organização.

Qualquer alteração relevante no ambiente tecnológico deve seguir processo formal de gestão de mudanças, visando mitigar impactos negativos à estabilidade dos sistemas e à segurança das informações.

A PX.Center deve implementar controles de Prevenção de Perda de Dados (DLP) para monitorar e bloquear a transmissão não autorizada de informações classificadas como Confidenciais ou Restritas por canais como e-mail, armazenamento em nuvem não corporativo, dispositivos removíveis e aplicações de comunicação, com regras definidas pelo CISO e revisadas semestralmente, conforme o Controle A.8.12 da ISO/IEC 27001:2022.

A PX.Center deve realizar testes de intrusão (pentest) ao menos anualmente em seus sistemas e infraestrutura críticos, conduzidos por equipe interna qualificada ou por terceiro especializado independente, com resultados reportados ao CISO e ao CSIP. Exercícios de simulação de resposta a incidentes (tabletop exercises) devem ser realizados ao menos semestralmente para validar a eficácia dos planos de resposta e a capacidade das equipes, conforme §5.29 da ISO/IEC 27001:2022.

A continuidade das operações deve ser assegurada por processos rigorosos de cópias de segurança (backup) e planos de recuperação de desastres, cabendo à Organização garantir que os dados críticos sejam armazenados de forma segura e testados periodicamente para validar sua disponibilidade em caso de falhas ou incidentes. As cópias de segurança estão sujeitas a políticas de retenção e descarte alinhadas às exigências legais, contratuais e regulatórias aplicáveis, bem como aos princípios de necessidade e minimização de dados.

Os backups que contenham informações Confidenciais ou Restritas devem receber o mesmo nível de proteção das bases de produção, inclusive quanto a controle de acesso, criptografia e descarte seguro ao final de seu ciclo de vida.

A PX.Center deve estabelecer diretrizes para a gestão de vulnerabilidades, realizando varreduras e atualizações de segurança de forma sistêmica. É responsabilidade de cada usuário zelar pelo uso seguro do e-mail corporativo, proteger o conteúdo de suas caixas de entrada e saída, evitar o armazenamento de informações sensíveis em pastas ou serviços não autorizados e observar rigorosamente as orientações de prevenção a golpes de phishing e a outras formas de engenharia social.

É vedado o uso do endereço de e-mail corporativo para cadastros ou finalidades alheias às atividades profissionais, bem como o encaminhamento de informações corporativas para contas de e-mail pessoais ou não autorizadas, devendo qualquer mensagem suspeita, link ou anexo potencialmente malicioso ser imediatamente reportado aos canais oficiais de segurança.

O acesso remoto aos sistemas e informações da PX.Center deve ser realizado exclusivamente por meio de canais corporativos autorizados, como redes privadas virtuais (VPN/ZTNA) e mecanismos de autenticação forte, observando-se o uso de dispositivos devidamente gerenciados e protegidos. É vedado o acesso a informações Confidenciais ou Restritas utilizando redes públicas ou dispositivos não autorizados sem a devida proteção criptográfica e os controles adicionais definidos nas normas técnicas complementares.

5.9 GESTÃO DE INCIDENTES E CONTINUIDADE DE NEGÓCIOS

A PX.Center deve manter estrutura dedicada à detecção, resposta e remediação de incidentes de segurança da informação e de eventos que possam comprometer a privacidade de dados pessoais. Todo evento identificado como ameaça real ou potencial à confidencialidade, integridade ou disponibilidade dos ativos da Organização deve ser reportado de imediato pelos canais oficiais de comunicação, sendo o canal oficial de segurança da informação o endereço security@px.center e o canal oficial para violações que envolvam privacidade e proteção de dados pessoais o endereço dpo@px.center.

A gestão de incidentes é coordenada pelo Gestor de Segurança da Informação (CISO), que possui autoridade para acionar o Plano de Resposta a Incidentes e mobilizar as áreas necessárias à contenção de danos e à investigação das causas. Em caso de incidentes que envolvam dados pessoais, a Organização deve proceder à análise de risco e impacto para cumprimento das obrigações de notificação perante a ANPD e os titulares afetados, conforme os prazos e requisitos estabelecidos pela legislação vigente e pela Política de Gestão de Incidentes (POL-SEG-002).

A PX.Center deve conduzir investigações pós-incidente para identificar falhas nos controles e implementar melhorias preventivas, mantendo todos os registros de incidentes e ações tomadas de forma segura para fins de auditoria e prova legal. Para garantir a resiliência institucional, a Organização deve estabelecer diretrizes e planos formais de Continuidade de Negócios destinados a manter as atividades críticas em funcionamento diante de falhas graves ou desastres, os quais devem ser revisados e testados periodicamente.

A observância e a colaboração com os protocolos de recuperação são obrigatórias para todos os departamentos, assegurando que a retomada das operações ocorra de forma ordenada e segura.

5.10 CONFORMIDADE, AUDITORIA E SANÇÕES

A observância das diretrizes estabelecidas nesta política é obrigatória para todos os indivíduos vinculados à PX.Center, que deve conduzir um Programa de Auditoria Interna do SGSI, executado ao menos anualmente por auditores independentes da área auditada, conforme §9.2 da ISO/IEC 27001:2022, com resultados documentados e reportados ao CSIP e à Alta Direção, além de monitoramentos e demais verificações técnicas e administrativas destinados a assegurar o cumprimento dos controles de segurança e da legislação aplicável.

O descumprimento das normas desta PSI ou de seus normativos complementares poderá acarretar medidas disciplinares e legais proporcionais à gravidade da infração. Para colaboradores, as penalidades podem incluir advertência verbal ou escrita, suspensão ou rescisão do contrato de trabalho por justa causa, sem prejuízo das responsabilidades civis e

criminais cabíveis. No caso de prestadores de serviço e parceiros comerciais, a violação poderá resultar na suspensão imediata de acessos, na aplicação de multas contratuais ou na rescisão motivada do vínculo comercial com a PX.Center.

6. RESPONSABILIDADES

A Alta Direção aprova esta política, provê os recursos necessários ao SGSI, realiza a análise crítica periódica do sistema e responde pelo compromisso estratégico da Organização com a segurança da informação e a conformidade legal.

O Comitê de Segurança da Informação e Privacidade (CSIP) delibera sobre investimentos, aprova revisões normativas, aprova a metodologia e os critérios de risco da Organização, arbitra conflitos de interpretação, decide sobre casos omissos e monitora a eficácia dos controles internos, devendo intervir em processos que apresentem riscos críticos.

O Gestor de Segurança da Informação (CISO) responde pela implementação técnica do SGSI, pela coordenação das respostas a incidentes, pela gestão de vulnerabilidades, pela definição das regras de DLP e pela auditoria dos controles lógicos e físicos.

O Encarregado de Proteção de Dados (DPO) conduz a interlocução oficial com a ANPD, zela pelos direitos dos titulares e atua de forma transversal para assegurar o cumprimento da LGPD nos tratamentos de dados pessoais.

Os gestores de área respondem pela aplicação desta política em seus processos, asseguram a adequação dos acessos de suas equipes e comunicam ao CISO e ao DPO eventos e mudanças relevantes.

Os proprietários da informação atribuem o nível de classificação dos ativos sob sua responsabilidade e definem os respectivos direitos de acesso.

Os colaboradores, estagiários, prestadores de serviço, consultores e parceiros comerciais devem observar as normas de conduta estabelecidas, zelar pelo sigilo das informações, proteger as credenciais e os ativos sob sua guarda e reportar de imediato qualquer evento suspeito pelos canais oficiais.

A inobservância das responsabilidades descritas sujeita o infrator às medidas disciplinares e legais cabíveis, conforme a legislação vigente e os contratos de trabalho ou de prestação de serviços da PX.Center.

7. GESTÃO DE REGISTROS

Os registros gerados pela aplicação desta política residem nos repositórios oficiais de governança da PX.Center. As versões desta política, as atas do CSIP, a Declaração de Aplicabilidade (PLC-17-002), os registros da análise crítica do SGSI, as avaliações de impacto e os relatórios de auditoria devem ser mantidos no repositório documental do SGI. Os registros

de incidentes de segurança e as respectivas ações de tratamento devem ser preservados conforme a Política de Gestão de Incidentes (POL-SEG-002).

Os logs de acesso, uso de sistemas e tráfego de rede devem ser retidos pelos prazos definidos nas normas técnicas complementares do SGI, com no mínimo revisão anual e na legislação aplicável. O inventário de ativos deve ser mantido atualizado pelo departamento de tecnologia. 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.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor em 24/06/2026 e possui validade por prazo indeterminado, revogando integralmente quaisquer disposições, comunicados ou práticas anteriores que tratem da mesma matéria no âmbito da PX.Center. O CSIP deve promover revisões ordinárias anuais, ou extraordinárias a qualquer tempo, para garantir a atualização do documento frente a mudanças tecnológicas, novas legislações ou alterações nos riscos de negócio. A aprovação desta política e de suas revisões compete ao CISO / CTO, sob deliberação do CSIP.

Os casos omissos, situações excepcionais ou interpretações dúbias não previstos nesta política devem ser submetidos à análise e deliberação do CSIP, e nenhuma exceção às regras aqui estabelecidas é permitida sem a devida formalização e aprovação por escrito da Alta Direção, após avaliação técnica de impacto e risco. É responsabilidade de todos os integrantes da PX.Center manterem-se atualizados quanto à versão vigente desta política, permanentemente disponível para consulta nos repositórios oficiais de governança.

A nulidade ou invalidade de qualquer item isolado deste documento não prejudica a vigência e a eficácia das demais disposições.

A aplicação deste documento não exclui as demais obrigações previstas em contratos de trabalho, contratos de prestação de serviços ou em códigos de conduta específicos adotados pela Organização. A nulidade ou invalidade de qualquer item isolado desta política, declarada por autoridade competente, não prejudica a vigência e a eficácia das demais disposições, que permanecem em pleno vigor para todos os efeitos de direito.

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	14/01/2026	Setor de Cybersegurança	Criação e Revisão
01	26/01/2026	Jurídico	Revisão
02	24/06/2026	SGI	Recodificação para sigla