Política de Uso Aceitável

Define as regras obrigatórias para o uso seguro e adequado dos ativos de informação da PX.Center (sistemas corporativos, e-mail, internet, dispositivos e redes sociais), em conformidade com a ISO/IEC 27001:2022 e a LGPD.

Código:	*POL-SEG-013*
Área responsável:	*Segurança da Informação*
Data de emissão:	*24/06/2026*
Responsável pela aprovação:	*CISO / CTO*

1. FINALIDADE/OBJETIVO

Esta política estabelece as regras obrigatórias para o uso seguro e adequado dos ativos de informação da PX.Center, prevenindo riscos à confidencialidade, à integridade e à disponibilidade das informações, em integração com a POL-SEG-001 (Política de Segurança da Informação), da qual deriva, e em conformidade com a ISO/IEC 27001:2022. A norma define o uso aceitável de sistemas corporativos, e-mail e mensageria, internet, dispositivos e computação móvel, trabalho remoto e redes sociais, bem como as responsabilidades de cada parte e as consequências do descumprimento.

Todo usuário com acesso, direto ou indireto, aos ativos de informação da PX.Center é obrigado a operar em conformidade com os controles aqui definidos.

2. ESCOPO/APLICABILIDADE

Esta política se aplica a todos os colaboradores, estagiários, fornecedores, prestadores de serviço, parceiros e terceiros que tenham acesso, direto ou indireto, aos ativos de informação da PX.Center, independentemente do local físico em que estejam ou da modalidade de trabalho adotada. A norma abrange:

a) os ativos de informação físicos, lógicos e humanos que suportem o processamento, o armazenamento ou a transmissão de informações corporativas; b) os sistemas corporativos, o e-mail e os demais canais de mensageria, a internet corporativa, as redes e os dispositivos fixos e móveis; c) o trabalho presencial e remoto, em qualquer unidade ou ambiente tecnológico da Organização. Aplica-se em conjunto com a POL-SEG-001 (Política de Segurança da Informação), à qual esta política se subordina.

3. USUÁRIOS/PÚBLICO-ALVO

Todos os colaboradores, estagiários, fornecedores, prestadores de serviço, parceiros e terceiros com acesso aos ativos de informação da PX.Center; os proprietários de ativos; os gestores de área; o Time de IAM (Identity & Access Management); a área de TI; o CISO / CTO e a equipe de Segurança da Informação responsável pela governança desta norma.

4. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001:2022 (Sistema de Gestão de Segurança da Informação)
- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- POL-SEG-001: Política de Segurança da Informação (PSI)
- POL-SEG-029: Política de Privacidade e Proteção de Dados Pessoais
- POL-SGI-001: Política de Ciclo de Vida da Informação
- POL-SEG-008: Política de Dispositivo Móvel e Trabalho Remoto
- POL-SEG-012: Política Traga Seu Próprio Dispositivo (BYOD)

- POL-SEG-010: Política de Mesa Limpa e Tela Limpa
- POL-SEG-003: Política de Cópias de Segurança
- POL-SEG-002: Política de Gestão de Incidentes
- POL-SGI-002: Política de Controle de Registros
- POL-SEG-016: Política de Controle de Acessos
- POL-SEG-022: Política de Proteção contra Malware

5. DIRETRIZES / REGRAS / CONTROLES

5.1 USO ACEITÁVEL DOS ATIVOS

Os ativos de informação devem ser utilizados exclusivamente para fins relacionados às atividades corporativas aprovadas. O acesso deve estar sempre vinculado ao perfil da função e ser aprovado pelo gestor responsável e pela área de TI. O uso deve observar a legislação brasileira, as normas internas e as obrigações contratuais. Constituem evidência para auditoria os logs de acesso, os relatórios de firewall e os registros de autorização. É estritamente proibido:

utilizar ativos para atividades ilegais, ofensivas ou discriminatórias; instalar ou executar software não autorizado; compartilhar credenciais ou acessar contas de terceiros; copiar, transferir ou divulgar informações sem autorização; e executar mineração de criptomoedas, jogos não relacionados ao trabalho ou uso excessivo de recursos para fins pessoais.

5.2 RESPONSABILIDADE PELOS ATIVOS

Os proprietários de ativos devem garantir a implementação dos controles de segurança adequados. Os usuários devem proteger os ativos contra acesso não autorizado, perda, roubo ou dano. A área de TI deve manter o inventário de ativos atualizado e protegido. A retirada de ativos das dependências da Organização exige autorização formal da gestão; equipamentos móveis com dados sensíveis devem ter criptografia de disco habilitada e o transporte deve seguir o procedimento de transporte seguro de ativos.

No encerramento do contrato, todos os ativos devem ser devolvidos em até 48 horas após o desligamento, salvo nos casos de colaborador em trabalho remoto distante da unidade matriz; a área de TI deve executar a limpeza segura de dados (wipe) e o responsável pela área deve confirmar a devolução e registrá-la no inventário.

5.3 PROTEÇÃO POR ANTIVÍRUS

O antivírus e o EDR corporativos são mantidos ativos em todos os equipamentos. É vedado ao usuário desativar, remover, contornar ou alterar as configurações dos agentes de segurança (EDR, DLP, MDM). A gestão, a atualização e o monitoramento da proteção contra malware seguem a POL-SEG-022 (Política de Proteção contra Malware).

5.4 AUTORIZAÇÃO E RESPONSABILIDADES DA CONTA

A conta é pessoal, individual e intransferível: é vedado compartilhar usuário, senha, tokens, códigos de verificação ou dispositivos de MFA com qualquer pessoa, inclusive gestores,

colegas, terceiros ou fornecedores. O usuário responde por todas as ações realizadas com sua conta até o reporte formal de suspeita de comprometimento, usa MFA nos sistemas que o exigirem e aprova solicitações de push apenas quando ele próprio inicia o acesso.

Perda, roubo ou suspeita de comprometimento de credenciais ou do dispositivo de MFA deve ser reportada imediatamente ao canal security@px.center. A concessão, a revisão e o desprovisionamento de acessos, os requisitos de senha e a gestão de segredos seguem a POL-SEG-016 (Política de Controle de Acessos).

5.5 MESA LIMPA E TELA LIMPA

O usuário mantém a mesa livre de informações sensíveis ao se ausentar e ao final do expediente e bloqueia a tela sempre que deixa a estação de trabalho. As diretrizes de mesa limpa e tela limpa estão definidas na POL-SEG-010 (Política de Mesa Limpa e Tela Limpa).

5.6 USO DA INTERNET

O uso da internet corporativa é permitido exclusivamente para fins profissionais. É proibido acessar sites com conteúdo ilícito, pornográfico, discriminatório, violento, de jogos de azar ou que incentivem conduta inadequada ou ilegal. É proibido realizar downloads de softwares, executáveis ou qualquer conteúdo sem autorização prévia da área de TI. É proibido utilizar proxy, VPN não corporativa ou qualquer outro método para contornar as restrições de acesso impostas pela Organização.

É proibido utilizar a internet corporativa para fins pessoais, atividades comerciais externas, envio de SPAM, participação em fóruns com posicionamentos pessoais polêmicos ou qualquer atividade que comprometa a imagem, os recursos ou a segurança da PX.Center. Os aplicativos de comunicação externa (ex.: aplicativos de comunicação externa não homologados) devem seguir as diretrizes da Organização e não podem ser usados para transferência de arquivos corporativos sem aprovação.

O tráfego de internet é monitorado e auditado pela área responsável; o uso inadequado sujeita o infrator às medidas previstas na seção 5.11.

5.7 E-MAIL E MENSAGERIA

O uso do e-mail corporativo e dos demais canais digitais da PX.Center (mensageria instantânea, chats corporativos, plataformas de colaboração e videoconferência) é permitido exclusivamente para fins profissionais. Apenas contas e canais corporativos autorizados pela área de TI podem ser utilizados para atividades de trabalho; é proibido o uso de e-mail pessoal, aplicativos de mensagens não autorizados ou redes sociais para tratar assuntos corporativos.

As informações classificadas como Confidenciais ou Sensíveis devem ser transmitidas apenas por canais corporativos protegidos, com criptografia ou anexos protegidos por senha; o envio de dados pessoais observa a LGPD e a Política de Classificação da Informação. É proibido o encaminhamento automático de e-mails corporativos para contas pessoais ou de terceiros e a abertura de anexos ou links de remetentes suspeitos. As mensagens suspeitas (phishing, malware, engenharia social) devem ser reportadas imediatamente ao canal security@px.center.

É proibido tentar desativar ou contornar os filtros de antispam e antivírus. É vedado o envio de conteúdo ofensivo, discriminatório, ilegal ou que comprometa a reputação da PX.Center; as comunicações devem manter padrão profissional, claro e objetivo. As comunicações corporativas podem ser monitoradas, registradas e auditadas.

5.8 DIREITOS AUTORAIS E PROPRIEDADE INTELECTUAL

É proibida a reprodução, a cópia, a modificação, a distribuição ou a utilização de materiais, softwares, documentos e conteúdos sem a devida autorização formal. Todo material desenvolvido no âmbito das atividades corporativas, incluindo código-fonte, documentação técnica, apresentações e bancos de dados, constitui propriedade intelectual da PX.Center, salvo disposição contratual em contrário.

Somente softwares licenciados e autorizados pela área de TI podem ser instalados e utilizados nos equipamentos corporativos; é vedado o uso de software pirata, versões não autorizadas ou aplicativos que violem direitos de propriedade intelectual. A cessão de direitos para uso externo exige aprovação formal da gestão. O uso da marca, do logotipo e da identidade visual da PX.Center é permitido apenas em materiais e publicações autorizados pela gestão, sendo vedado o uso em contextos que prejudiquem a reputação da Organização.

5.9 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

O uso de dispositivos móveis e o trabalho remoto para acessar recursos e informações da PX.Center observam as diretrizes da POL-SEG-008 (Política de Dispositivo Móvel e Trabalho Remoto); o uso de dispositivos pessoais segue a POL-SEG-012 (Política de BYOD). É vedado armazenar informações corporativas em dispositivos, mídias ou serviços de nuvem pessoais não autorizados.

5.10 REDES SOCIAIS

O uso de redes sociais e de aplicativos de mensageria nos equipamentos e dispositivos da PX.Center é autorizado exclusivamente às funções de negócio responsáveis por essa atividade, em especial Marketing e Comercial, mediante contas corporativas e para fins de promoção e divulgação institucional. Esse uso observa restrições de conteúdo: é vedada a publicação ou o compartilhamento de dados confidenciais, restritos ou de dados pessoais. Para as demais funções, o uso pessoal de redes sociais e de aplicativos de mensagens nos equipamentos e dispositivos da Organização é vedado.

Nenhum colaborador está autorizado a falar em nome da PX.Center ou sobre assunto interno, restrito ou confidencial em mídia social, salvo quando expressamente autorizado pela Direção.

5.11 MONITORAMENTO, INCIDENTES E CONSEQUÊNCIAS

Todas as atividades realizadas nos sistemas, redes e canais de comunicação da PX.Center podem ser registradas, monitoradas e auditadas em caráter contínuo e proporcional, em conformidade com a LGPD. É proibido ao usuário tentar desativar, contornar ou interferir nos mecanismos de monitoramento. Todo usuário é informado, no momento da contratação ou da adesão a esta política, sobre a existência e a finalidade do monitoramento.

Todo incidente de segurança, como acesso não autorizado, vazamento de dados, indisponibilidade de sistemas, infecção por malware, perda ou roubo de dispositivos, e-mails maliciosos ou falhas de configuração, deve ser reportado imediatamente ao canal security@px.center, e tratado conforme a Política de Gestão de Incidentes. Incidentes que envolvam dados pessoais são adicionalmente comunicados ao canal dpo@px.center, conforme a POL-SEG-029. O não reporte tempestivo constitui violação desta política.

O usuário reconhece e concorda com o monitoramento e a auditoria de acessos no momento do onboarding e a cada atualização relevante desta norma.

6. RESPONSABILIDADES

O CISO e o CTO aprovam esta política, definem os requisitos de segurança, proveem os recursos necessários e supervisionam a conformidade do uso aceitável na PX.Center. A equipe de Segurança da Informação implementa, gerencia e revisa os mecanismos de monitoramento, opera o canal security@px.center, conduz a investigação e o tratamento de incidentes e supervisiona a conformidade dos registros com a ISO/IEC 27001.

A área de TI mantém o inventário de ativos, as ferramentas de monitoramento, os filtros de rede e o antivírus, fornece e mantém os recursos de acesso remoto seguros e garante a proteção, o backup e a disponibilidade dos registros eletrônicos. O Time de IAM cria, altera e desprovisiona contas e credenciais, autoriza contas funcionais e conduz as revisões semestrais de acesso. Os proprietários de ativos garantem a implementação dos controles de segurança adequados aos ativos sob sua responsabilidade.

Os gestores de área aprovam acessos e o trabalho remoto de suas equipes, confirmam a devolução de ativos no desligamento e apoiam a aplicação das medidas de monitoramento. O Encarregado de Dados (DPO) atua no tratamento dos incidentes que envolvam dados pessoais, pelo canal dpo@px.center, conforme a POL-SEG-029. Os usuários e terceiros utilizam os ativos exclusivamente para fins corporativos autorizados, protegem suas credenciais e os ativos sob sua guarda e reportam imediatamente qualquer incidente ou suspeita ao canal security@px.center.

7. GESTÃO DE REGISTROS

Todos os registros gerados pela aplicação desta política são documentados, mantidos e controlados conforme a Política de Controle de Registros da PX.Center. Os registros incluem logs de acesso, evidências de autorização de uso, relatórios de incidentes, revisões semestrais de acesso e evidências de treinamento, e são armazenados em arquivos eletrônicos (PDF, DOCX, XLSX), em sistemas corporativos ou em cópia física, quando aplicável. O controle é realizado por meio da Planilha de Gerenciamento de Registros, com os campos obrigatórios:

tipo de registro, data de criação, responsável, prazo de retenção, local de armazenamento e status. O proprietário do registro garante sua criação, atualização e manutenção; a equipe de

Segurança da Informação supervisiona a conformidade; e a área de TI assegura a proteção, o backup e a disponibilidade dos registros eletrônicos. Os registros são mantidos pelo período mínimo definido na Política de Controle de Registros, ou por prazo superior quando exigido por lei, contrato ou regulamentação, e seu descarte ocorre com exclusão completa e irrecuperável das informações.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor em 23/06/2026 no Portal do SGI, com validade por prazo indeterminado, e é revisada anualmente ou sempre que houver alteração nos requisitos legais e normativos, incidentes de segurança relevantes, atualizações tecnológicas ou mudanças de processo. O descumprimento desta política sujeita o infrator às medidas disciplinares cabíveis, como advertência, suspensão, bloqueio ou revogação de acessos e rescisão contratual, conforme a gravidade da infração, a CLT e o contrato aplicável, sem prejuízo das responsabilidades civis e penais previstas na legislação.

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	09/06/2025	Setor de TI e Cybersegurança - SI	Criação e Revisão
01	24/06/2026	SGI	Recodificação para sigla