Política de Dispositivo Móvel e Trabalho Remoto

Uso seguro de dispositivos móveis e acesso remoto na PX.Center

Código:	*POL-SEG-008*
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 para o uso seguro de dispositivos móveis e a prática de trabalho remoto na PX.Center, em conformidade com o controle 6.7 da ISO/IEC 27001:2022 (trabalho remoto), com os controles 7.9 (segurança de ativos fora das instalações) e 8.1 (dispositivos de endpoint do usuário), e em integração com a POL-SEG-001 (Política de Segurança da Informação).

O documento define as regras de proteção aplicáveis a notebooks, smartphones, tablets e demais ativos que acessem informações da Organização fora de suas dependências físicas, para preservar a confidencialidade, a integridade e a disponibilidade das informações mesmo em ambientes remotos e conexões fora do perímetro corporativo.

2. ESCOPO/APLICABILIDADE

Esta política aplica-se a todos os colaboradores, prestadores de serviço e terceiros que acessem ativos de informação da PX.Center fora das dependências físicas da Organização, em qualquer dispositivo corporativo ou pessoal autorizado. A definição pela PX.Center como entidade de referência abrange os demais CNPJs do grupo, dispensando documento específico por entidade.

Estão incluídos os dispositivos de computação móvel, como notebooks, smartphones, tablets, mídias USB corporativas e dispositivos IoT com conectividade externa, e todo acesso remoto a sistemas, serviços em nuvem e dados internos da Organização. O uso de dispositivos pessoais (BYOD) observa as regras específicas da POL-SEG-012. As disposições aplicam-se em conjunto com a POL-SEG-001 (Política de Segurança da Informação), à qual esta política se subordina.

3. USUÁRIOS/PÚBLICO-ALVO

Direção, CISO, CTO, Líder de Segurança da Informação, equipe de Infraestrutura de TI, gestores de área e todos os colaboradores, prestadores de serviço e terceiros autorizados a utilizar dispositivos móveis ou a acessar remotamente os ativos de informação da PX.Center.

4. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001:2022 (controles 6.7, 7.9 e 8.1)
- POL-SEG-001: Política de Segurança da Informação
- POL-SEG-012: Política de BYOD (uso de dispositivos pessoais)
- POL-SEG-002: Política de Gestão de Incidentes
- POL-SEG-016: Política de Controle de Acessos
- POL-SGI-001: Política de Ciclo de Vida da Informação
- POL-SEG-013: Política de Uso Aceitável

5. DIRETRIZES / REGRAS / CONTROLES

5.1 PROVISIONAMENTO E GESTÃO DE DISPOSITIVOS MÓVEIS

São considerados dispositivos de computação móvel os notebooks, smartphones, tablets, mídias USB corporativas, dispositivos IoT com conectividade externa e qualquer outro ativo capaz de acessar sistemas ou informações da PX.Center fora das dependências da Organização. A concessão de dispositivos corporativos é atribuição da área de Tecnologia da Informação, mediante anuência do gestor imediato do colaborador.

O inventário, o gerenciamento e o monitoramento dos dispositivos fornecidos são conduzidos pela equipe de Infraestrutura de TI por meio da solução corporativa de gestão de endpoints (UEM), e a proteção de endpoint é assegurada pela solução corporativa de EDR. É vedado acessar informações da Organização em dispositivo não inventariado pela TI.

5.2 CONFIGURAÇÃO SEGURA DO DISPOSITIVO

Todo dispositivo móvel corporativo deve manter proteção de endpoint (EDR) ativa e atualizada, criptografia de disco habilitada, autenticação forte e bloqueio automático de tela. O bloqueio automático de tela é obrigatório e deve ocorrer após, no máximo, 5 minutos de inatividade, com desbloqueio protegido por senha, PIN ou biometria. Os sistemas operacionais e aplicativos devem ser mantidos atualizados conforme a política de patches da TI. A instalação de softwares não autorizados ou não avaliados previamente pela TI é proibida.

5.3 USO EM DESLOCAMENTO E PROTEÇÃO DE ATIVOS FORA DAS INSTALAÇÕES

Em conformidade com o controle 7.9 da ISO/IEC 27001:2022, a retirada e o transporte de dispositivos corporativos exigem autorização e registro no inventário da TI. O equipamento é mantido em local físico seguro, não é deixado desacompanhado em locais públicos e não é utilizado por terceiros. O colaborador deve impedir a visualização de informações por pessoas não autorizadas em ambientes públicos e é vedado compartilhar o dispositivo com pessoas não autorizadas.

A manutenção do dispositivo fora da Organização é autorizada e controlada pela TI, e a devolução do ativo é registrada com a respectiva baixa no inventário.

5.4 ACESSO REMOTO E TRABALHO REMOTO

Em conformidade com o controle 6.7 da ISO/IEC 27001:2022, o acesso remoto a sistemas internos da PX.Center deve ocorrer exclusivamente por canais seguros, sendo obrigatório o uso de VPN corporativa combinada com autenticação multifator (MFA). É vedado acessar sistemas internos por conexões diretas que não trafeguem pela VPN corporativa. A autorização para trabalho remoto é atribuição da liderança direta do colaborador, e a habilitação técnica do acesso é conduzida pela equipe de TI.

O colaborador deve garantir ambiente físico privado e seguro, com conectividade adequada, e é vedado o uso de dispositivos de terceiros para acessar dados da Organização.

5.5 PROTEÇÃO E ARMAZENAMENTO DE DADOS

Dados sensíveis ou confidenciais não devem ser armazenados localmente no dispositivo sem criptografia e sem aprovação da área responsável. É proibido armazenar documentos da Organização em dispositivos não autorizados ou em mídias externas não corporativas. Na substituição ou no descarte do dispositivo, o equipamento deve ser devolvido à TI para formatação segura e baixa no inventário.

5.6 REPORTE DE PERDA, FURTO OU INCIDENTE

A perda ou o furto de dispositivo móvel deve ser comunicada imediatamente ao canal security@px.center. A Segurança da Informação aciona o bloqueio ou o apagamento remoto do dispositivo por meio das soluções corporativas de gestão de endpoints e de EDR. Incidentes envolvendo dispositivos móveis ou acesso remoto seguem o tratamento definido na POL-SEG-002; quando houver envolvimento de dados pessoais, aciona-se também o canal dpo@px.center para avaliação das obrigações da LGPD.

5.7 USO DE DISPOSITIVOS PESSOAIS (BYOD)

O uso de dispositivos pessoais para acessar ativos de informação da PX.Center observa as regras específicas da POL-SEG-012. Na ausência de autorização e de enquadramento nos controles dessa norma, é vedado o acesso a sistemas e dados da Organização por meio de dispositivos pessoais.

6. RESPONSABILIDADES

A Tecnologia da Informação (TI) é a área responsável por garantir o cumprimento desta política e responde pela apuração de violações às suas disposições, com canal de contato security@px.center para questões de segurança da informação e dpo@px.center para questões de privacidade e LGPD. A Direção aprova esta política e provê os recursos necessários à sua execução. O CISO e o CTO aprovam esta política, definem os controles aplicáveis a dispositivos móveis e acesso remoto e respondem pela sua manutenção.

A equipe de Infraestrutura de TI provisiona os dispositivos corporativos, mantém o inventário, o gerenciamento e o monitoramento por meio da solução corporativa de gestão de endpoints (UEM), e habilita os acessos remotos via VPN com MFA. O Líder de Segurança da Informação recebe os reportes de perda, furto e incidente, aciona o bloqueio ou apagamento remoto e conduz o tratamento de incidentes conforme a POL-SEG-002.

Os gestores de área autorizam o trabalho remoto de suas equipes, validam a necessidade de concessão de dispositivos e asseguram a conformidade dos colaboradores sob sua gestão com esta política. Os colaboradores, prestadores de serviço e terceiros cumprem as regras desta política, protegem fisicamente os dispositivos sob sua guarda e reportam imediatamente qualquer perda, furto ou incidente.

7. GESTÃO DE REGISTROS

Os registros mantidos de acordo com este documento residem nos seguintes repositórios: - Inventário de dispositivos móveis corporativos, com histórico de concessão, revogação, manutenção e descarte: solução corporativa de gestão de endpoints (UEM). - Registro de acessos remotos autorizados: sob custódia da equipe de Infraestrutura de TI. - Eventos de proteção de endpoint e bloqueio/apagamento remoto: solução corporativa de EDR e a de gestão de endpoints. - Incidentes envolvendo dispositivos móveis ou acesso remoto: conforme a POL-SEG-002. - Versões desta política: 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.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor em 23/06/2026, com validade por prazo indeterminado. O documento é revisado anualmente ou diante de incidente relevante envolvendo dispositivos móveis ou trabalho remoto, mudança regulatória ou de compliance, ou adoção de nova tecnologia que impacte 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	23/06/2025	Setor de TI e Cybersegurança - SI	Criação e Revisão
01	24/06/2026	SGI	Recodificação para sigla