



34 ANOS

TECNOLOGIA
EM SEGURANÇA



Programa de Integridade

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

1ª edição
Janeiro de 2026

A REDEPRIME é uma empresa de tecnologia que há mais de 34 anos atende grandes projetos personalizados de infraestrutura crítica. Nosso diferencial reside na oferta de soluções integradas de videomonitoramento inteligente, monitoramento móvel e telecomunicações, todos suportados por tecnologia de ponta e acompanhamento em tempo real pela nossa Central de Operações Integradas (COI).

A informação é um dos ativos mais valiosos da nossa organização e de nossos clientes. Por isso, a presente Política de Segurança da Informação (PSI) reflete o nosso compromisso inegociável com a proteção de dados, garantindo que todas as nossas operações sigam os mais rigorosos padrões de Confidencialidade, Integridade e Disponibilidade.

Muito além da tecnologia, acreditamos que a segurança se constrói com cultura e responsabilidade. Este documento traz as diretrizes que devem nortear o comportamento de todos os nossos colaboradores e parceiros, assegurando que a confiança depositada na Redeprime ao longo de três décadas continue sendo o nosso maior pilar de crescimento.



Solange Monteiro
Compliance

SUMÁRIO

01	FINALIDADE E COMPROMISSO ESTRATÉGICO	01
02	ABRANGÊNCIA E VINCULAÇÃO	01
03	DEFINIÇÕES TÉCNICO-JURÍDICAS	01
04	GESTÃO DE ACESSOS E IDENTIDADE	02
05	SEGURANÇA NO VIDEOMONITORAMENTO	02
06	CLASSIFICAÇÃO DA INFORMAÇÃO	02
07	SEGURANÇA FÍSICA E MOBILIDADE	03
08	PLANO DE CONTINUIDADE E BACKUP	03
09	GESTÃO DE INCIDENTES E RELATO	03
10	PENALIDADES E SANÇÕES	03
11	VIGÊNCIA E TREINAMENTO	04

1. FINALIDADE E COMPROMISSO ESTRATÉGICO

1.1. A REDEPRIME, com mais de 34 anos de expertise em videomonitoramento inteligente e soluções integradas, estabelece esta Política para garantir a proteção de seus ativos de informação e dos dados de seus clientes.

1.2. Esta PSI fundamenta-se na preservação da tríade CID:

Confidencialidade: Garantia de que as informações e imagens sejam acessadas apenas por pessoas autorizadas.

Integridade: Salvaguarda da exatidão dos dados e imagens, impedindo alterações não rastreáveis.

Disponibilidade: Garantia de que os sistemas de monitoramento e a rede de telecomunicações estejam operacionais quando solicitados.

2. ABRANGÊNCIA E VINCULAÇÃO

2.1. Esta Política é de cumprimento obrigatório por todos os sócios, diretores, conselheiros, colaboradores (incluindo estagiários e aprendizes) e Terceiros (fornecedores, consultores e prestadores de serviço), independentemente da atividade exercida ou forma de contratação.

2.2. A adesão a esta Política é condição essencial para a manutenção do vínculo empregatício ou contratual com a REDEPRIME.

3. DEFINIÇÕES TÉCNICO-JURÍDICAS

Ativos de Informação: Qualquer dado, sistema, software, hardware ou infraestrutura de rede (incluindo câmeras, rádios e servidores) de propriedade ou sob gestão da REDEPRIME.

Incidente de Segurança: Qualquer evento que comprometa a CID dos dados, como invasões, vazamentos de imagens ou perda de dispositivos.

Log de Auditoria: Registro imutável de eventos ocorridos num sistema (quem acedeu, quando e o que foi visualizado).

4. GESTÃO DE ACESSOS E IDENTIDADE

4.1. Princípio do Menor Privilégio: O acesso aos sistemas de monitoramento e bases de dados será concedido apenas ao nível estritamente necessário para o desempenho da função.

4.2. Credenciais: É expressamente proibido o uso de contas genéricas ou a partilha de palavras-passe. O uso de Autenticação Multifator (MFA) é obrigatório para acessos remotos e centrais de operações integradas (COI).

4.3. Senhas: Devem seguir os critérios de complexidade da REDEPRIME e nunca serem anotadas em locais físicos ou digitais inseguros.

5. SEGURANÇA NO VIDEOMONITORAMENTO (ESPECÍFICO)

5.1. Cadeia de Custódia: As imagens captadas pela REDEPRIME devem ser tratadas como evidências potenciais. Qualquer exportação de vídeo deve seguir um protocolo de segurança para garantir a sua integridade jurídica.

5.2. Proibição de Captura Externa: É terminantemente proibido fotografar, filmar ou gravar ecrãs de monitoramento utilizando dispositivos pessoais (telemóveis).

5.3. Transmissão Segura: Todos os fluxos de vídeo entre câmeras, gravadores e nuvem devem utilizar protocolos de criptografia de ponta a ponta.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

Os dados na REDEPRIME são classificados em quatro níveis de sensibilidade:

Pública: Informações institucionais para divulgação externa.

Uso Interno: Informações operacionais não sensíveis.

Confidencial: Dados comerciais, orçamentos e contratos.

Restrita: Imagens de monitoramento, chaves de criptografia e dados biométricos (Nível Máximo de Proteção).

7. SEGURANÇA FÍSICA E MOBILIDADE

7.1. Estações de Trabalho: O colaborador deve bloquear o computador ao ausentar-se (Win + L) e manter a mesa livre de documentos sensíveis ("Mesa Limpa").

7.2. Dispositivos Móveis: Telemóveis ou portáteis da empresa devem possuir ferramentas de gestão remota (MDM) para permitir a limpeza de dados em caso de roubo ou perda.

8. PLANO DE CONTINUIDADE E BACKUP

8.1. A REDEPRIME manterá rotinas de cópias de segurança (backups) automáticas e geodistribuídas.

8.2. Testes de restauração devem ser executados e documentados periodicamente para garantir a recuperação célere em caso de ataques de Ransomware.

9. GESTÃO DE INCIDENTES E RELATO

9.1. Dever de Reportar: Qualquer suspeita de violação desta PSI deve ser reportada imediatamente através do e-mail: compliance@redeprime.com.

9.2. Investigação: A REDEPRIME conduzirá investigações imparciais para apurar falhas de segurança, garantindo o sigilo dos envolvidos conforme o Código de Conduta.

10. PENALIDADES E SANÇÕES

10.1. O descumprimento desta Política sujeita o infrator às sanções disciplinares previstas no Capítulo 03 do Código de Conduta da REDEPRIME, que incluem:

Advertência e Suspensão;

Rescisão contratual ou Demissão por justa causa;

Adoção de medidas judiciais cíveis e criminais cabíveis.

11. VIGÊNCIA E TREINAMENTO

11.1. Esta Política entra em vigor na data de sua aprovação e será revista anualmente.

11.2. A REDEPRIME promoverá treinamentos obrigatórios de conscientização em segurança da informação para todos os colaboradores.