Pharmanexo
O Maior Portal de Oportunidades de Produtos Farmacêuticos do Brasil

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Diretrizes de Governança, Proteção de Ativos e Segurança em Nuvem

Última revisão: janeiro de 2026

Objetivo

A presente Política de Segurança da Informação (PSI) tem como objetivo estabelecer as diretrizes fundamentais para a proteção dos ativos de informação da Pharmanexo. Esta norma visa assegurar a Confidencialidade (garantia de que o acesso seja restrito a quem de direito), a Integridade (manutenção da exatidão e completude dos dados) e a Disponibilidade (garantia de que os sistemas estejam acessíveis quando necessário) de todas as informações processadas, com foco especial em dados sensíveis do setor de saúde.

Abrangência

Esta política aplica-se a todos os colaboradores, diretores, estagiários, prestadores de serviço e parceiros de negócio que utilizem os recursos tecnológicos da Pharmanexo. O escopo abrange a infraestrutura local, dispositivos móveis corporativos, ambientes de terceiros e, primordialmente, a infraestrutura de nuvem Oracle Cloud Infrastructure (OCI).

Estrutura de SOC — Security Operations Center (GS 14)

A Pharmanexo mantém uma estrutura de monitoramento contínuo para detecção e resposta a ameaças cibernéticas. Conforme os requisitos do item GS 14, a organização adota o seguinte modelo operacional:

- Modelo de Operação: A estrutura é composta por um modelo híbrido, utilizando ferramentas internas de monitoramento integradas a serviços especializados de resposta a incidentes.
- Tecnologias e Controles: São aplicados controles de monitoramento de logs, análise de tráfego de rede e detecção de anomalias em tempo real. A estrutura utiliza sistemas de Security Information and Event Management (SIEM) para centralizar a visibilidade de eventos de segurança em toda a infraestrutura.
- Monitoramento 24/7: O SOC opera em regime de prontidão para garantir que tentativas de intrusão ou comportamentos suspeitos sejam mitigados antes de causarem impacto operacional.

Segurança de Rede

A gestão da rede na Pharmanexo é realizada de forma compartilhada e coordenada com a empresa Globalsys. As diretrizes incluem:

- Segmentação de Rede: Utilização de redes virtuais isoladas para separar ambientes de produção, homologação e desenvolvimento.

- Perímetro e Acesso Remoto: Implementação de firewalls de próxima geração (NGFW) e túneis de comunicação criptografados (VPN) para acessos remotos, garantindo que o tráfego de dados entre a unidade local e a Global seja protegido.
- Alinhamento com gestor: Todas as alterações estruturais na topologia de rede devem ser validadas pela equipe da Globalsys para garantir a conformidade com os padrões internacionais do grupo.

Segurança na Nuvem (SN-04)

Em conformidade com o item SN-04, o ambiente de nuvem da Pharmanexo está hospedado na Oracle Cloud Infrastructure (OCI), seguindo rigorosos protocolos de segurança:

- Controles Atuais: A infraestrutura utiliza Identity and Access Management (IAM) para controle granular, restrição de acesso baseada em IP e monitoramento de auditoria nativo.
- Evolução Tecnológica: A organização está em fase de planejamento da implantação do Oracle Cloud Guard, ferramenta avançada que permite a detecção automática de configurações inseguras e atividades de risco, elevando o nível de postura de segurança (Cloud Security Posture Management - CSPM).
- Criptografia: Todos os dados em repouso e em trânsito dentro da OCI são protegidos por algoritmos de criptografia de alto nível.

Gestão de Identidade e Acesso (IAM)

O acesso aos sistemas da Pharmanexo é regido pelo princípio do privilégio mínimo. Nenhum usuário terá permissões além das estritamente necessárias para a execução de suas funções laborais.

Controle	Descrição Técnica	Frequência
Autenticação Multifator (MFA)	Obrigatório para todos os acessos à nuvem e sistemas críticos.	Sempre
Revisão de Acessos	Auditoria das permissões concedidas a cada colaborador.	Trimestral
Provisionamento	Criação de contas baseada em perfis (Roles) pré-aprovados.	Na contratação

Desprovisionamento	Revogação imediata de acessos em caso de desligamento.	Imediato

Gestão de Incidentes e Vulnerabilidades

A Pharmanexo mantém um processo formal para identificar, classificar e remediar falhas de segurança:

- Resposta a Incidentes: Em caso de violação confirmada, o Plano de Resposta a Incidentes é ativado, priorizando o isolamento da ameaça e a preservação de evidências para análise forense.
- Gestão de Vulnerabilidades: São realizados escaneamentos periódicos de vulnerabilidades nos servidores e aplicações. As correções (patches) de segurança devem ser aplicadas seguindo a criticidade: Crítica (24h), Alta (7 dias), Média (30 dias).

Auditoria e Conformidade

A organização compromete-se com a melhoria contínua e a conformidade legal, especialmente em relação à LGPD e normas internacionais de segurança:

- Logs de Auditoria: Todos os acessos são registrados e armazenados, garantindo a rastreabilidade total das operações.
- Sanções: O descumprimento das diretrizes desta política sujeitará o infrator a medidas disciplinares, que podem incluir advertência, suspensão ou rescisão do contrato de trabalho por justa causa, sem prejuízo de sanções cíveis e penais cabíveis.

Nota: Esta política deve ser revisada anualmente ou sempre que houver mudanças significativas na infraestrutura tecnológica ou no cenário regulatório.

DIRETORA ADMINISTRATIVA
PHARMANEXO