Política de Segurança Cibernética – (Colaborador, Prestadores de Serviço e Parceiros)

OBJETIVO

Esta política tem como objetivo proteger as informações e os sistemas da **Interlog** contra riscos cibernéticos, como vazamentos, ataques ou acessos indevidos. Também garante que todos sigam boas práticas de segurança digital, conforme as exigências da LGPD (Lei Geral de Proteção de Dados).

APLICAÇÃO

Este documento política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam ou acessam sistemas, redes, documentos ou dados da Interlog, seja de forma física ou digital.

Princípios Básicos de Segurança

- **Confidencialidade**: Somente os colaboradores autorizados podem acessar determinadas informações.
- **Integridade**: Os dados devem ser mantidos protegidos contra alterações indevidas.
- **Disponibilidade**: os sistemas e informações precisam estar acessíveis quando necessário.

Ações realizadas pela Interlog

- **Controle de Acessos**: Cada colaborador tem acesso apenas ao que é necessário para sua função.
- **Auditorias e Revisões:** Revisões e registros de acessos são feitos periodicamente.
- **Testes de Segurança**: A empresa realiza testes para identificar falhas e vulnerabilidades.
- **Bloqueio de Dispositivos:** o uso de pen drives, HDs externos e outros dispositivos não sao permitidos, o uso do celular corporativo deverá ser autorizados pela alta gestão da Interlog.
- **Proteção contra vazamentos**: medidas são aplicadas para evitar que dados sejam enviados por e-mail ou aplicativos sem autorização.
- **Plano de Resposta a Incidentes:** caso aconteça algum incidente (como um ataque), a empresa tem planos para agir rapidamente e evitar prejuízos maiores.
- **Backup e Recuperação:** Cópias de Segurança são feitas regularmente para garantir que dados importantes não sejam perdidos.

Principais riscos que todos os colaboradores devem conhecer.

- Virus e malware
- E-mails falsos (phishing)
- Ransomware (sequestro de dados)
- Engenharia social (golpes que usam confiança e distração)
- Acesso indevido por terceiros

Responsabilidade de cada um.

Política de Segurança Cibernética – (Colaborador, Prestadores de Serviço e Parceiros)

1. Colaboradores e terceiros

- Usar senhas seguras e não compartilhá-las.
- Evitar clicar em links ou abrir anexos suspeitos.
- Informar ao Gestor ou TI imediatamente sobre qualquer atividade estranha ou possível risco.
- Participar de treinamentos de Segurança da Informação.
- Utilizar apenas equipamentos e redes autorizadas pela empresa.

2. Gestores

- Garantir que suas equipes cumpram as diretrizes de segurança.
- Apoiar e divulgar treinamentos juntamente com o RH.
- Controlar acessos às informações do seu departamento.

3. Tecnologia da Informação (TI)

- Monitorar os sistemas e manter a proteção ativa.
- Aplicar correções e atualizações de segurança.
- Conduzir ações de resposta a incidentes.

Importante:

Esta política é revisada periodicamente para garantir que esteja sempre atualizada frente às novas ameaças. Todos os colaboradores devem seguir suas diretrizes.

Canal de dúvidas e comunicação:

Se você tiver dúvidas, sugestões ou quiser relatar algo relacionado à segurança da informação, entre em contato com o Departamento de Tecnologia

Versão	Data de Emissão	Depto Responsável	Próxima Revisão
0	04/12/2024	Tecnologia da Informação	05/12/2025

Política de Segurança Cibernética – (Colaborador, Prestadores de Serviço e Parceiros)