POLÍTICA DE CIBERSEGURANÇA

Versão001

SUMÁRIO

1. OBJETIVOS

Esta política se aplica a todos os colaboradores, prestadores de serviços, estagiários e terceiros que utilizam recursos de tecnologia, sistemas, redes e dados do Grupo Serval, incluindo ambientes locais, remotos e em nuvem.

2. ÂMBITO

Esta política se aplica a todos os colaboradores ou prestadores de serviço em regime de trabalho CLT / PJ com o Grupo Serval.

3. PRINCÍPIOS

Confidencialidade: acesso às informações apenas por pessoas autorizadas.

- Integridade: proteção contra alterações não autorizadas de dados e sistemas.
- Disponibilidade: garantir que sistemas e dados estejam acessíveis quando necessários.
- Autenticidade: assegurar que usuários, dispositivos e comunicações sejam legítimos.
- Responsabilidade: cada usuário é responsável por suas ações no ambiente digital.

4. DIRETRIZES

4.1. Segurança de Acesso

- Uso obrigatório de senhas fortes (mín. 8 caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais).
- Troca periódica de senhas e proibição de reutilização em diferentes sistemas.
- Utilização de Autenticação multifator (MFA) em sistema que possibilitem, mas obrigatória para sistemas críticos.
- Cada usuário deve ter credenciais pessoais e intransferíveis.

4.2. Proteção contra Ameaças

- Uso de antivírus, firewall e sistemas de detecção de intrusão atualizados.
- Bloqueio de sites e aplicativos maliciosos conforme lista de restrições da empresa.
- Proibição de downloads de fontes não confiáveis.
- Monitoramento contínuo de tráfego e atividades suspeitas.

4.3. Segurança de Dispositivos

- Proibição de uso de dispositivos de armazenamento externo sem autorização formal.
- Bloqueio automático da estação de trabalho ao se ausentar.
- Atualização obrigatória de sistemas operacionais e softwares.

4.4. Tratamento da Informação

- Aplicar os princípios de segurança em todo o ciclo de vida dos dados: geração, armazenamento, transmissão e descarte seguro.
- Dados pessoais sensíveis devem ter proteção adicional e exclusão segura quando não mais necessários, salvo obrigações legais.

4.5. Navegação e Comunicação

- Uso da internet prioritariamente para fins profissionais.
- Proibição de acesso a conteúdo ilegal, discriminatório ou ofensivo.
- Proibição de compartilhamento de informações confidenciais sem autorização.

5. RESPOSTA A INCIDENTES

Qualquer tentativa ou suspeita de ataque cibernético deve ser reportada imediatamente Canal de Ética no endereço gruposerval.com.br/canal-de-ética/ com os possíveis **Tipo de Incidente** (**Privacidade e Segurança de Dados**, **Violação de Políticas Internas**)

- O TIC realizará análise, conterá o incidente e adotará medidas corretivas.
- Registros e evidências serão preservados para investigação.

6. RESPONSABILIDADES

Colaboradores: seguir esta política, manter sigilo, armazenar arquivos em locais autorizados e relatar incidentes.

- **Gestores:** promover a conscientização, validar solicitações de acesso e supervisionar o uso adequado dos recursos.
- **Departamento TIC:** implementar controles, monitorar ambientes, manter backups, executar testes de segurança e atualizar esta política.

7. CONSCIENTIZAÇÃO E TREINAMENTO

Treinamentos periódicos serão realizados sobre boas práticas de cibersegurança, prevenção a fraudes digitais e proteção de dados.

8. PENALIDADES

O descumprimento desta política poderá resultar em advertência, suspensão, desligamento e/ou medidas legais cabíveis.

9. REVISÃO

Esta política será revisada anualmente ou sempre que houver mudanças significativas nas ameaças cibernéticas, nos ativos da empresa ou na legislação vigente.