Política de Segurança da Informação e Uso de Tecnologia

1. Introdução, Objetivo e Abrangência

1.1. Propósito

O objetivo primário desta Política é estabelecer as diretrizes, princípios e normas de segurança que regem o uso e a proteção dos **Ativos de Informação** da Serfer (dados, sistemas, *hardware*, *software*, *know-how* e infraestrutura). A Política visa garantir a **Confidencialidade**, **Integridade** e **Disponibilidade** das informações em todas as suas formas e meios de armazenamento, protegendo o valor do negócio.

1.2. Escopo de Aplicação

Esta Política é de cumprimento **obrigatório** e abrange:

- **Pessoas:** Todos os colaboradores (efetivos ou temporários), estagiários, terceiros, parceiros de negócio e prestadores de serviço que, por qualquer motivo, tenham acesso aos ativos e informações da Serfer.
- **Ativos:** Todos os dispositivos, sistemas, redes, dados e instalações físicas e virtuais utilizados nas operações da Serfer.
- **Localização:** Aplica-se em todas as dependências da Serfer e em ambientes externos, incluindo o trabalho remoto (*home office*) e o uso de dispositivos corporativos em trânsito.

1.3. Vigência e Revisão

Esta Política entra em vigor na data de sua publicação e será revisada, no mínimo, anualmente, ou sempre que ocorrerem mudanças significativas no ambiente de negócios, nos sistemas de informação ou nas regulamentações legais (ex: LGPD).

1.4. Princípios Fundamentais e Compromisso

- A informação é um **ativo estratégico** da Serfer e deve ser protegida de forma adequada.
- **Responsabilidade Individual:** Todo usuário é responsável pela segurança dos ativos sob sua guarda.
- **Conformidade Legal:** Atendimento integral à legislação vigente, em especial à Lei Geral de Proteção de Dados (LGPD).
- O conhecimento e a aceitação desta Política são **condição obrigatória** para o vínculo com a Serfer.

2. Papéis e Responsabilidades

- **Comitê/Gestor de Segurança da Informação (ou TI):** Responsável pela elaboração, divulgação, treinamento, monitoramento e manutenção desta Política.
- **Gestores/Lideranças de Área:** Garantir que suas equipes conheçam e cumpram as diretrizes e auxiliar na classificação da criticidade das informações de sua área.

- **Colaboradores e Usuários em Geral:** Conhecer, aceitar e cumprir integralmente esta Política e seus procedimentos complementares, zelando pelos ativos e recursos da empresa.

3. Classificação e Manuseio da Informação

3.1. Níveis de Classificação

As informações na Serfer são classificadas em:

- **Pública:** Informação destinada ao uso externo.
- **Interna:** Uso exclusivo da Serfer, sem causar grande dano.
- **Confidencial:** Prejuízo financeiro ou vantagem competitiva perdida (ex: Estratégia de preços, *know-how* industrial).
- **Estritamente Confidencial/Restrita:** Dano legal e financeiro severo (ex: Dados Pessoais, segredos de patente, chaves de criptografia).

3.2. Diretrizes de Manuseio e Descarte

- **Armazenamento:** Informações Confidenciais e Estritamente Confidenciais devem ser armazenadas apenas em locais ou sistemas corporativos seguros e nunca em dispositivos ou serviços de *cloud* pessoais.
- **Transmissão:** A transmissão de dados sensíveis para fora da rede da Serfer deve ser feita, sempre que possível, por ferramentas de criptografia homologadas pela TI.
- **Descarte Seguro:** Documentos físicos contendo informações Confidenciais devem ser destruídos usando fragmentadoras. Mídias digitais devem ser entregues à TI para descaracterização profissional.

4. Controle de Acesso Lógico e Uso de Senhas

4.1. Gestão de Identidades e Privilégios

- **Acesso Pessoal e Intransferível:** O acesso é individualizado, pessoal e intransferível. O compartilhamento de senhas é **estritamente proibido** e será tratado como falta grave.
- **Princípio do Mínimo Privilégio:** O acesso será concedido apenas na medida estritamente necessária para o desempenho da função do usuário.
- **Revogação Imediata:** Todos os direitos de acesso serão revogados imediatamente em caso de desligamento.

4.2. Política de Criação e Uso de Senhas Fortes

- **Comprimento Mínimo:** 12 caracteres.
- **Complexidade:** Mínimo de 3 das 4 categorias (maiúsculas, minúsculas, números, caracteres especiais).
- **Troca Periódica:** Alteração obrigatória a cada **90 dias**.
- **Proteção da Senha:** As senhas nunca devem ser escritas ou armazenadas em arquivos não criptografados.

4.3. Bloqueio de Estações de Trabalho

- O usuário deve **bloquear (travar)** sua estação de trabalho (**tecla Windows + L** ou equivalente) sempre que se afastar dela.
- Todas as estações de trabalho devem ter bloqueio de tela automático configurado após **10 minutos** de inatividade.

5. Segurança em Equipamentos, Infraestrutura e Comunicação

5.1. Estações de Trabalho e Servidores

- **Software Licenciado e Aprovado:** Proibida a instalação de *software* não licenciado ou não autorizado pela TI.
- ***Patch Management*:** O usuário não deve interferir ou adiar as atualizações de segurança programadas pela TI.
- **Proteção Anti-malware:** O *software* de proteção deve estar instalado, ativo e atualizado em todos os dispositivos.
- **Conexão de Dispositivos:** Proibido conectar dispositivos de armazenamento removível pessoal (*pen-drives*) sem autorização prévia da TI.

5.2. Dispositivos Móveis e Uso Remoto

- Diretrizes para uso de dispositivos móveis corporativos e/ou pessoais (**BYOD** - se aplicável).
- Uso obrigatório de **VPN** ou outros mecanismos seguros para acesso remoto à rede.

5.3. Internet e Correio Eletrônico (E-mail)

- **Prioridade Profissional:** O uso da internet e e-mail deve ser **prioritariamente profissional**.
- **Conteúdo Proibido:** É **estritamente proibido** o acesso, *download* ou transmissão de conteúdo ilegal, ofensivo ou impróprio.
- **Alerta Phishing:** O colaborador deve ser **extremamente cauteloso** com e-mails suspeitos e **nunca** fornecer senhas ou dados confidenciais por e-mail. Qualquer suspeita deve ser reportada **imediatamente**.
- **Monitoramento e Privacidade:** A Serfer **reserva-se o direito** de monitorar todo o tráfego de internet e e-mail. Não há expectativa de privacidade ao utilizar recursos corporativos.

6. Segurança de Redes e Sistemas

- Uso obrigatório de **Firewall** para proteção da rede.
- Restrições rigorosas para o uso de pen-drives, HDs externos e outros dispositivos de armazenamento.
- Regras claras para o acesso à rede *wireless* corporativa e/ou convidada.

7. Resposta a Incidentes de Segurança

7.1. Comunicação Obrigatória (Reporte Imediato)

O colaborador deve notificar **imediatamente** (em até 30 minutos da descoberta) o Gestor Imediato e a equipe de **Tecnologia da Informação (TI)** sobre qualquer suspeita ou confirmação de incidente (ex: *malware*, vazamento de dados, perda de equipamento).

7.2. Fases de Resposta (Responsabilidade da TI/Comitê)

A Equipe de Resposta a Incidentes da Serfer (ERIS) seguirá as fases:

1. **Identificação:** Determinar a origem, o escopo e a criticidade do incidente.
2. **Contenção:** Impedir que o incidente se espalhe (ex: isolar a máquina).
3. **Erradicação:** Remover a causa raiz (ex: limpar o *malware*).
4. **Recuperação:** Restaurar sistemas e serviços à operação normal.
5. **Lições Aprendidas:** Documentar e revisar o processo para prevenir reincidências.

7.3. Tratamento Específico de Vazamento de Dados (LGPD)

Em casos de vazamento de Dados Pessoais, a Serfer deve notificar a **Agência Nacional de Proteção de Dados (ANPD)** e os titulares afetados, conforme a legislação.

8. Monitoramento e Auditoria

A empresa reserva-se o direito de **monitorar** o uso de todos os recursos tecnológicos (e-mails, internet, logs) para fins de segurança, auditoria e conformidade legal, notificando os colaboradores sobre isso. Auditorias periódicas serão realizadas para verificar a aderência à Política.

9. Consequências e Sanções

9.1. Disposições Gerais

O não cumprimento desta Política e seus anexos constitui falta, sujeitando o colaborador às sanções disciplinares previstas na legislação (CLT) e no Código de Conduta da Serfer.

9.2. Gradação das Sanções

As sanções serão aplicadas de forma progressiva, proporcional à gravidade e dano causado:

- **Advertência:** Violação inicial de regras não críticas (ex: esquecer de bloquear a tela).
- **Suspensão:** Reincidência de faltas leves ou compartilhamento não autorizado de acesso de *baixo risco*.
- **Dispensa por Justa Causa:** Vazamento intencional ou por negligência grave de dados Confidenciais ou Estritamente Confidenciais, ou uso da rede para atividades criminosas.

Conclusão

A segurança da informação na **Serfer Comércio e Indústria de Ferro e Aço LTDA** não é apenas uma responsabilidade da Tecnologia da Informação, mas sim um **valor fundamental** e uma **responsabilidade compartilhada** por todos que lidam com os ativos da empresa.

Em um setor estratégico como o de ferro e aço, a interrupção da produção, a perda de *know-how* industrial ou o vazamento de dados competitivos podem causar prejuízos incalculáveis e comprometer a excelência e a confiabilidade da Serfer no mercado.

Esta Política é o nosso compromisso formal em proteger as operações, a reputação e a vantagem competitiva da Serfer. O cumprimento rigoroso destas normas e o engajamento contínuo de cada indivíduo são essenciais para manter um ambiente de trabalho seguro, produtivo e em total conformidade legal.

A segurança começa com você.