POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E USO DOS RECURSOS TECNOLÓGICOS

1. OBJETIVO

Esta Política estabelece as diretrizes para a gestão da segurança da informação e uso dos recursos tecnológicos da **SERQUIP TRATAMENTOS RESÍDUOS PR LTDA., Matriz e Filiais**. O objetivo é proteger a **integridade**, **disponibilidade** e **confidencialidade** das informações e sistemas da empresa, bem como garantir o uso responsável e ético dos recursos tecnológicos.

A **integridade** está consubstanciada na guarda e transmissão da informação, prevenindo-se alterações indevidas, intencionais ou acidentais, garantindo-se, por meio deste que a informação seja mantida em seu estado original.

A **confidencialidade** resume-se a garantir que o acesso à informação seja obtido apenas por pessoas autorizadas, e a **disponibilidade** é a garantia de acesso a quem tenha autorização, sempre que necessário.

2. ABRANGÊNCIA

O presente documento orienta colaboradores, gestores, fornecedores e visitantes sobre Política de Segurança e a utilização dos recursos computacionais, de telecomunicação e infraestrutura de Tecnologia da Informação.

3. INFORMAÇÕES E ORIENTAÇÕES GERAIS

Os recursos e serviços ofertados pela SERQUIP devem ser utilizados pelos colaboradores exclusivamente para a realização das atividades profissionais.

O uso pessoal dos recursos e/ou serviços poderão ser permitidos somente com a anuência do superior imediato e desde que não prejudique o desempenho dos sistemas e serviços institucionais.

O colaborador que estiver fazendo a utilização do recurso ou serviço é responsável por eventuais perdas e/ou problemas em dados e equipamentos nos casos em que comprovada a negligência, imprudência ou imperícia.

A SERQUIP reserva-se no direito de registrar e rastrear todo o uso dos equipamentos, sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

O Acordo de Confidencialidade assinado por todos os colaboradores é um dos documentos de referência da presente Política, devendo ser observados os seus termos e orientações, bem como a responsabilidade em relação à segurança da informação.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao superior direto, que deverá encaminhar posteriormente setor de Tecnologia da Informação – TI e ao DPO (Lei Geral de Proteção de Dados – LGPD).

A não observância aos requisitos previstos nesta política poderá implicar em sanção por meio das medidas administrativas cabíveis.

4. DAS RESPONSABILIDADES

A SERQUIP é responsável por implementar e manter um programa de segurança da informação eficaz. Os colaboradores são responsáveis por utilizar os recursos tecnológicos de acordo com esta política.

Dos Colaboradores

Será de inteira responsabilidade de cada colaborador, o prejuízo ou dano que vier a sofrer ou causar à SERQUIP e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, realizar backups periódicos dentro da infraestrutura disponível, não compartilhar senhas, não disseminar notícias ou informações inconsistentes.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos

individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação e Uso dos Recursos Tecnológicos.

Da Área de Tecnologia da Informação

Informar aos gestores os serviços específicos que serão prestados e os procedimentos de resposta aos incidentes, formulando assim um portfólio de serviços.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir e assegurar os requisitos de segurança estabelecidos por esta Política e demais documentos congêneres, integrantes do *Compliance* Trabalhista e LGPD.

Permitir, quando necessário, a execução de atividades operacionais sob sua responsabilidade como, por exemplo, manutenção de computadores, realização de cópias de segurança ou testes no ambiente.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir para cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados ou qualquer outro ativo de informação a um responsável identificável como pessoa física, de acordo com a Lei Geral de Proteção de Dados (LGPD), sendo que:

- Os usuários (logins) individuais de colaboradores serão de responsabilidade do próprio colaborador;
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante;

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado, bem como após auditados pela TI.

Realizar manutenções corretiva, evolutiva e preventiva semestral, a fim de revisar tecnicamente os dispositivos tecnológicos de trabalho e mitigar os riscos para assegurar o bom funcionamento dos recursos.

Auxiliar na instalação e configuração de assinaturas digitais e certificados digitais, por meio de ferramentas específicas. Orientar os usuários quanto aos backups de dados e auditá-lo quando necessário.

Garantir, de maneira rápida e com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de resguardar os ativos da empresa.

5. USO DOS RECURSOS TECNOLÓGICOS

Os colaboradores devem utilizar os recursos tecnológicos da SERQUIP para fins profissionais. O uso para fins pessoais é permitido apenas quando não interfere nas atividades profissionais e mediante autorização do superior hierárquico imediato.

Os colaboradores devem seguir as seguintes regras de uso dos recursos tecnológicos:

- Não instalar software sem autorização;
- Não acessar sites ou abrir arquivos de fontes desconhecidas;
- Não compartilhar senhas com terceiros;
- Reportar qualquer incidente de segurança à equipe de TI.

6. INCIDENTES DE SEGURANÇA

Qualquer incidente de segurança deve ser reportado imediatamente à equipe de TI e ao DPO (Lei Geral de Proteção de Dados – LGPD). As equipes, conjuntamente, investigarão o incidente e tomarão as medidas necessárias para mitigar os danos.

7. REVISÃO

Esta política será revisada periodicamente para garantir que esteja alinhada com as necessidades da SERQUIP.

Curitiba/PR, 15 de dezembro de 2023.