POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INFORMACTION
MAIO/2024

Elaboração		
Responsável – Cargo/Setor	**Versão**	**Data**
Daniel Heller – Encarregado	1.0	08/05/2024
Aprovação		
Comitê do Projeto	1.0	24/05/2024

A Política de Segurança da Informação é uma declaração formal acerca do compromisso da InformAction para com a proteção das informações de sua propriedade e/ou sob sua guarda.

Este documento define a Política de Segurança da Informação, e se aplica a todos os diretores, funcionários, prestadores, fornecedores, visitantes e demais pessoas que venham a ter acesso às informações de propriedade da InformAction e/ou sob sua guarda.

A InformAction manterá um Comitê de Privacidade, responsável pela atualização contínua desta política, com base em processo de avaliação sistemática de impactos e riscos à privacidade.

É obrigação, de todas as pessoas e empresas submetidas à esta política, reportar ao Comitê de Privacidade, qualquer violação que tenham conhecimento.

Esta Política de Segurança da Informação é aderente aos princípios instituídos pela Lei Geral de Proteção de Dados Pessoais – Lei n. 13.709/2018.

1 Objetivo

O objetivo desta Política é orientar as ações e estabelecer as diretrizes corporativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Ela deve ser cumprida e aplicada em todas as áreas da InformAction.

Objetivos Principais:

I – Manter e aperfeiçoar as práticas de Segurança da Informação em todos os níveis da instituição;

II – Conscientizar os colaboradores, fornecedores e prestadores em relação às práticas de Segurança da Informação;

III – Reforçar o compromisso estratégico acerca da Privacidade; e

IV – Garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais.

Em complemento à Política de Segurança, serão elaborados outros documentos:

- Política de Gestão de Riscos;
- Política de Acesso à Internet; e
- Política de Uso de Dispositivos de Tecnologia.

2 Conceitos

Termo de Confidencialidade. É a cláusula ou instrumento contratual que contém responsabilidades, direitos e deveres dos empregados, prestadores e fornecedores de serviços, que tem como objetivo assegurar que determinadas informações sejam mantidas em sigilo.

Análise de Risco. É o processo que envolve a consideração das vulnerabilidades, causas e consequências, a fim de se determinar as probabilidades dos riscos se tornarem reais e os impactos decorrentes.

Logging. É o registro de todas as transações efetuadas durante a utilização de um sistema e necessário ao rastreamento do seu uso.

Ativo Tecnológico. São os Equipamentos e Sistemas de Tecnologia da instituição.

Risco. É qualquer coisa, desconhecida ou incerta, que possa impedir os objetivos da instituição, é qualificado pela probabilidade da ocorrência e pelo impacto que pode causar no projeto, caso ocorra.

Dado Pessoal Sensível. É um dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Tratamento. É toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Backup. É a cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes.

Incidente de Segurança da Informação. É a ocorrência de uma possível violação de segurança da informação com potencial de causar dano.

Dispositivos Móveis. É qualquer equipamento ou acessório portátil, capaz de se conectar à internet e/ou armazenar dados, tais como: celular, smartphone, tablet, notebook, mp4, pendrive, CD/DVD e outros semelhantes.

Usuário. É uma pessoa que utiliza um equipamento ou sistema de informática da instituição.

3 Classificação das Informações

O primeiro passo para dar início às práticas de segurança é a classificação das informações. Dessa forma é possível compreender quais medidas serão aplicáveis e os esforços necessários para garantir a privacidade dos dados e informações sob custódia.

Nível	Descrição	Exemplos
Público	É a informação que pode ser divulgada a qualquer pessoa, independentemente da sua relação com a instituição.	As informações divulgadas no website e redes sociais são bons exemplos de dados públicos.
Interno	É a informação que a instituição não tem interesse em divulgar e o acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso a informação seja disponibilizada por alguma razão, não causará danos sérios à instituição.	Os memorandos, correspondências e atas de reuniões que contêm informações que não estão disponíveis publicamente.

Confidencial	É a informação cuja divulgação pode causar danos financeiros ou à imagem da instituição.	Os dados pessoais sob a guarda da InformAction.

4 Política de Segurança

Os quatro fundamentos da Segurança da Informação são:

- **Confidencialidade**: limita o acesso à informação tão somente às pessoas e/ou entidades autorizadas pelo proprietário da informação ou quem tenha a reserva legal de preservá-la;
- **Integridade**: garante que a informação, mesmo que alterada, mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção, alteração e destruição);
- **Disponibilidade**: garante que a informação esteja sempre disponível para uso dos usuários autorizados pelo proprietário da informação; e
- **Irretratabilidade**: garante a impossibilidade de negar a autoria em relação a uma transação anteriormente realizada, permitindo a rastreabilidade no manejo da informação com os registros que demonstrem a fidedignidade do processo de guarda e autoria.

Os recursos de informática da InformAction devem ser utilizados pelos colaboradores e prestadores apenas para a execução das suas atividades profissionais.

Os usuários devem conhecer, entender e cumprir a política de segurança da informação e os procedimentos aplicáveis às suas funções, zelando pela correta aplicação das medidas de proteção. São responsáveis pelo uso adequado das informações e dos recursos de informática, além de registrar os incidentes de Segurança da Informação para o Comitê de Privacidade.

4.1. Incidente

Para a Lei Geral de Proteção de Dados, incluindo, mas não limitado a, pode ser considerado um incidente de segurança:

➢ Qualquer acesso não autorizado a dados que contenham informações pessoais que possam identificar o indivíduo;

➢ Vazamento de informações de um único registro ou base de dados contendo informações pessoais; e

➢ Perda das informações pessoais.

4.2. Regras

➢ As senhas de acesso (credenciais) aos computadores e aos sistemas da InformAction são pessoais, não deverão ser emprestadas ou compartilhadas, e não deverão ficar anotadas em blocos de notas ou estações de trabalho;

➢ É proibido salvar documentos com Dados Pessoais Sensíveis em computadores ou outros dispositivos pessoais, excetuadas as situações que tenha consentimento do superior hierárquico;

➢ É proibido compartilhar informações da instituição por e-mail particular e redes sociais;

➢ É proibido conversar em locais públicos mencionando Dados Pessoais e Dados Pessoais Sensíveis;

➢ É proibida a instalação de softwares ou sistemas nas estações de trabalho sem autorização da equipe de Tecnologia da Informação, excetuadas as situações que tenha consentimento do superior hierárquico;

➢ O e-mail corporativo deve ser utilizado exclusivamente no interesse da InformAction. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório;

➢ Desconfie de todos os e-mails com assuntos estranhos, e não abra anexos se não tiver certeza de que o solicitou;

➢ Os usuários não podem criar ou repassar mensagens de conteúdo abusivo, obsceno, pornográfico, racista, constrangedor ou difamatório, em qualquer formato;

➢ O celular corporativo deve ser utilizado exclusivamente no interesse da InformAction. É proibido o empréstimo para pessoas não autorizadas;

➢ Os documentos físicos que envolvam dados pessoais não devem ficar expostos sobre a mesa ou em gavetas que não estejam fechadas, e devem ser guardadas em local seguro para proteção integral da informação;

➢ Os computadores deverão ser programados para bloquear automaticamente a tela quando ficarem por quinze minutos sem movimentação;

➢ O uso da internet e do e-mail podem ser auditados, e o usuário é responsável pelo seu uso, que deve ser condizente com a função exercida;

➢ Em caso de uso de equipamento próprio, o colaborador se compromete a seguir todas as práticas de segurança em respeito à Lei Geral de Proteção de Dados; e

➢ Todos os funcionários e prestadores da InformAction devem assinar o Termo de Confidencialidade.

5 Terceiros

Os fornecedores e prestadores deverão estar cientes e comprometidos com esta Política, através de cláusulas relacionadas às diretrizes de Segurança da Informação.

Justifica-se a rescisão contratual com fornecedores e prestadores que não estejam se adequando à Lei Geral de Proteção de Dados ou que não queiram subscrever os termos de ciência e compromisso com esta política.

6 Sanções

O descumprimento comprovado de qualquer disposição desta política poderá acarretar a imposição de sanções à pessoa ou empresa que incorrer no desvio.

Os funcionários, fornecedores e prestadores, em razão das infrações cometidas às normas previstas nesta Política, ficam sujeitos às seguintes sanções:

I – Advertência;

II – Suspensão;

III – Demissão por justa causa; e

IV – Rompimento e/ou Multa de contrato.

O procedimento de apuração será conduzido pelo Comitê de Privacidade, e as sanções poderão ser advertência verbal, advertência por escrito, rescisão de contrato.

As sanções serão aplicadas em conformidade com a CLT e o Código de Processo Civil.

7 Considerações Finais

A InformAction se reserva o direito de modificar, a qualquer momento, as presentes normas, especialmente para adaptá-las aos requisitos de segurança, aos padrões de boas práticas e de governança.

Qualquer alteração e/ou atualização da Política de Segurança passará a vigorar a partir da data de sua publicação e deverá ser integralmente observada pelos Usuários.