Encarregado: Rafael Rocha da Silva
E-mail: dpo@integratesoftware.com.br

Política de Segurança da Informação

Nº. Doc./Versão: 1
Início da Vigência: 25/08/2021

1. INTRODUÇÃO

A Política Corporativa de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2013 reconhecida mundialmente como código de práticas para controles de segurança da informação (atualização da ISO/IEC 27002:2005).

2. APLICAÇÃO

Aplica-se a toda Integrate.

3. RESPONSÁVEIS

Eduardo (Diretor);
Rafael Rocha da Silva (DPO);
E todos os demais colaboradores da Integrate.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

• **Pública**: são informações aprovadas pelo seu responsável para consulta irrestrita e cuja sua divulgação externa não compromete o negócio da organização. Ex: editais, licitações, rotinas.

• **Interna**: são informações disponíveis para a execução de suas tarefas rotineiras, não se destinando, portanto ao usuário público externo. Ex: Memorandos, portarias, padrões, políticas e procedimentos.

• **Confidencial**: são informações de acesso restrito a um colaborador ou a um grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros. Ex: exames, processos judiciais, dados cadastrais de funcionários.

• **Restrita**: são informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da organização e restrita a superintendentes, gerentes, supervisores e funcionários cujas funções queiram conhecê-las. Ex: indicadores estatísticos de processos de negócio, resultados de auditorias internas.

5. DISPOSIÇÕES

5.1. Proteção da Informação

a. Os colaboradores devem assumir uma postura proativa no que diz respeito à proteção das informações da empresa e devem estar atentos às ameaças, bem como fraudes, sabotagem,

roubo de informações e acessos indevidos ao sistema de informação;
b. Assuntos confidenciais são de uso restrito e não devem ser expostos publicamente.

5.2. Correio Eletrônico (E-mail)
a. A troca de mensagens entre usuários, via correio eletrônico deve estar relacionada a assuntos de interesse da organização;

b. É proibido enviar, transmitir, manusear ou disseminar informações sigilosas, segredos de negócio
ou qualquer outra informação confidencial da Organização;

c. É proibido acessar a caixa postal de outro usuário sem a sua autorização, exceto em casos de auditoria e investigação de procedência, pelas Assessorias e Departamentos competentes;

d. É responsabilidade do usuário o acompanhamento diário e leitura dos e-mails em sua caixa postal, bem como exclusão periódica de mensagens não utilizadas;

e. Mensagens eletrônicas suspeitas recebidas, link de acesso, anexos ou qualquer outro tipo de arquivo, devem ser excluídos.

5.3. Login e Senha
a. As senhas dos usuários são pessoais e intransferíveis, pois asseguram que apenas ele, devidamente identificado, utilize e mantenha de acordo com a necessidade, os acessos aos sistemas;

b. O usuário não deve escolher senhas óbvias, baseadas em nomes próprios, datas de aniversários, siglas conhecidas, nome da organização, data de nascimento e etc.;

e. Colaboradores devem ter seus acessos lógicos bloqueados e inativados imediatamente após saída da empresa conforme documento PSI0068 Gestão de Pessoas;

f. Cadastro de novos usuários, inativação de acessos, mudança de função devem ser registrados em chamado pelo Departamento de RH conforme fluxo descrito no documento PSI0068 Gestão de Pessoas.

6. COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS
a. Para garantir a adequada utilização dos recursos de processamento de informações, fica criado Comitê de Privacidade e Proteção de Dados, composta por membros de áreas de interesse e que serão nomeados internamente, que ficará autorizada a aplicar penalidades, previstas no PSI0068 Gestão de Pessoas, aos que violarem a legislação em vigor e as dispostas nesta política;

b. Sempre que julgar necessário para a preservação da integridade dos recursos computacionais, dos serviços aos usuários ou dos dados, a Gerência de Tecnologia poderá suspender

temporariamente qualquer conta, seja ou não o responsável pela conta suspeita de alguma violação;

c. As penalidades a serem aplicadas por infração à presente política são redução ou eliminação, temporárias ou permanentes, dos acessos aos recursos computacionais.

8. DISPOSIÇÕES FINAIS

a. Os membros do Comitê de Privacidade e Proteção de Dados podem sugerir a inclusão de novos tópicos e ou revisão dos já existentes neste documento, mas toda e qualquer alteração que for realizada será avaliada e aprovada pelos citados como responsáveis. A responsabilidade de atualizar periodicamente este documento é do DPO nomeado.