Política		Código	Versão
Política de Segurança da Informação		**PL-001-ICF**	**1.0**
Norma/Processo/procedimento/documento **Política de Segurança da Informação**	Dono do Processo/Informação **TI**	Data de Início da Vigência **24/09/2020**	
Classificação			
☐ **Público**	☒ **Corporativo**	☐ **Restrito**	☐ **Confidencial**
			N/A

Sumário

1. Introdução

A informação utilizada pela ICF Comércio é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua confidencialidade, integridade, disponibilidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.
Esta política visa ser base para as demais Normas e Serviços garantindo a segurança das informações, atuando de forma ética para assegurar a aplicação das legislações vigentes e das boas práticas reduzindo os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos da ICF Comércio.

2. Declaração de Comprometimento da Alta Direção

A Alta Direção declara seu comprometimento e apoio a aplicação desta Política de Segurança da Informação, reconhecendo o valor de seus princípios, metas e objetivos condizentes com os negócios e Código de Conduta Ética da ICF Comércio.

3. Objetivo

Esta política define o tratamento que deve ser dado as informações armazenadas, processadas ou transmitidas independente do dispositivo utilizado ou localidade, sendo uma declaração da ICF COMÉRCIO de seu compromisso com a proteção das informações de sua propriedade e sob sua guarda. Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos de controle relacionados à segurança da informação.
Em bases gerais, podemos tratar a informação de acordo com os 05 (cinco) itens que se seguem abaixo, os quais são entendidos também como objetivos desta política:

- ✓ **Confidencialidade:** Deve-se manter o sigilo das informações não podendo ser divulgadas sem autorização prévia do responsável pela informação ou da alta direção, assegurando assim que a informação é disponibilizada apenas àqueles possuem autorização.
- ✓ **Integridade:** Entende-se por manter a informação correta, isenta de modificações, alterações ou destruições não autorizadas, garantindo assim que a informação permaneça legítima/confiável e consistente;
- ✓ **Disponibilidade**: Assegurar que a informação está disponível aos utilizadores autorizados sempre que necessário;
- ✓ **Legalidade:** Garantir que o uso e manuseio das informações seguem as leis vigentes no país (Lei de crimes cibernéticos – Lei 12.737/2012, Marco Cívil da Internet – Lei 12.965/2014 e LGPD LEI Nº 13.709/2018);
- ✓ **Auditabilidade:** As informações devem ser registradas e processadas de modo a permitir que seja possível realizar auditorias que garantam e atestem sua veracidade.

4. Abrangência

Esta política apresenta um conjunto de diretrizes, requisitos e boas práticas, que devem ser cumpridas por todos os funcionários efetivos ou temporários, estagiários, aprendizes, prestadores de serviço e parceiros comerciais.

5. Atribuições e Responsabilidades

- ✓ Conhecer suas responsabilidades a respeito da segurança da informação e atuar de forma responsável, profissional, ética e legal com os recursos e informações do ICF Comércio.
- ✓ Conhecer e seguir as diretrizes das Políticas, Normas e Serviços de Segurança (incluindo seus anexos) estabelecidos pela ICF Comércio;
- ✓ Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo ICF Comércio, sendo que não se deve divulgar ou compartilhar qualquer informação confidencial ou interna sem autorização formal da companhia;
- ✓ Assegurar que os recursos disponibilizados sejam exclusivamente utilizados para execução das atribuições profissionais aprovadas pela ICF Comércio;
- ✓ Comunicar imediatamente qualquer suspeita de tentativa ou efetiva violação desta ou demais políticas e normas, bem como qualquer incidente relacionados à segurança da informação através de um chamado para de TI.

6. Comportamento Seguro

Independente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais da ICF COMÉRCIO. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações, onde o colaborador é responsável direto por todos os recursos acessados com seu usuário e senha.

6.1. Senhas Seguras

- ✓ A senha de acesso deve ser alterada no primeiro acesso, garantindo assim seu conhecimento exclusivo ao portador das credenciais;
- ✓ As senhas de acesso são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas, anotadas em papel ou em sistema visível. Deve manter todas as senhas seguras contra qualquer tipo de visualização e cópia;

- ✓ É proibida a prática de compartilhamento de contas e senhas de acesso e o titular que fornecer suas credenciais a outrem responderá pelas infrações por estes cometidas, estando passível das penalidades previstas;
- ✓ O usuário está proibido de utilizar contas e senhas de acesso pertencentes a outros usuários;
- ✓ Caso o usuário desconfie que sua senha não é mais segura, ou de seu domínio exclusivo, deverá alterá-la imediatamente;
- ✓ Deverá ser evitada a composição de senhas com sequências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome do usuário, data de nascimento, nome de entes queridos...);
- ✓ O usuário não deve incluir suas senhas em nenhum processo automático de autenticação, como por exemplo: macro, códigos fontes ou funções-chave;
- ✓ O usuário não deve utilizar as mesmas senhas com finalidades profissionais para fins pessoais, evitando assim uma disseminação de acesso inapropriado em caso de vazamentos ou acessos não autorizados.

6.2. Uso Geral

- ✓ O uso de pen drive e ou mídias de qualquer tipo para armazenamento de dados é restrito as funções autorizadas, novas solicitações devem ser encaminhadas para TI pelo gestor;
- ✓ Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais) que facilitem a divulgação mesmo dentro da empresa;
- ✓ Somente softwares homologados pela ICF Comércio podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pelo departamento de TI da ICF Comércio;
- ✓ Documentos impressos e arquivos contendo informações confidenciais devem ser protegidos de acesso não autorizado, mantido sob sua guarda ou armazenado em local de acesso restrito.
- ✓ Ao se ausentar de sua mesa faça o bloqueio de seu computador/ notebook, protegendo assim suas informações;
- ✓ Sempre armazenar informações que estão relacionadas às suas atividades profissionais em sua pasta de rede que é um ambiente seguro e passível de recuperação posterior.

7. Monitoramento Interno

Todos os colaboradores devem ter ciência de que o uso das informações, sistemas de informação e comunicação é monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

- ✓ Abaixo constam a lista de ações que são monitoradas e poderão ser utilizadas como objeto de auditoria;
- ✓ Acesso à Internet;
- ✓ E-mails enviados e recebidos, incluindo análise do conteúdo;
- ✓ Ligações telefônicas realizadas do telefone da empresa;
- ✓ Documentos impressos;
- ✓ Comunicações realizadas por chat ou conferência (mensagem, áudio ou vídeo);
- ✓ Acesso e modificações às pastas de rede;
- ✓ Acessos Físicos e Lógicos.

8. Comitê de Segurança da Informação

- ✓ O comitê de segurança da informação foi criado com a missão de condensar os princípios de segurança que a alta direção considera importante e fundamental para as atividades da ICF Comércio.
- ✓ As atividades do comitê, além de demonstrar o comprometimento da ICF Comércio com a segurança da informação, também desempenham os seguintes papéis:
- ✓ Estabelecer diretrizes e suporte perante toda a organização das iniciativas de Segurança da Informação;
- ✓ Propor políticas, regras de negócio e serviços gerais relacionados à segurança da informação;
- ✓ Apoiar as atividades de gestão de riscos (avaliação, aceitação e tratamento de riscos);
- ✓ Alinhar os objetivos de negócios e de tecnologia com a segurança da informação;
- ✓ Acompanhar e propor planos de ação para a aplicação da política de segurança da informação.

9. Penalidades e Sanções

A não observância das obrigações previstas na respectiva política ensejará à aplicação de penalidades que poderão variar de advertência, suspensão ou até a rescisão do contrato por justa causa, dependendo da gravidade da ocorrência, além da reparação de eventual dano causado, independentemente de sua responsabilidade civil ou criminal.

10. Histórico da última atualização

Resumo - atualizações efetuadas	Data	Atualizado por
Criação do Documento.	**24/09/2020**	**Marcelo Vicenzo**