Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Segurança da Informação.

Objetivo

Esta Política busca estabelecer os conceitos e diretrizes de Segurança da Informação, visando proteger as informações da Instituição e de seus clientes. Posiciona-se como um documento estratégico, com vistas a promover o uso seguro dos ativos de informação da Instituição e asseverar o seu compromisso com a proteção das informações sob a sua custódia, devendo ser cumprida por todos os integrantes da Instituição.

Visão Geral

Esta Política aplica-se a todas as áreas da Instituição, sendo de observância obrigatória a todos os integrantes, tendo em vista que a Instituição busca resguardar a segurança das suas informações de acordo com as melhores práticas de mercado.

A implementação contínua e eficaz desta política depende do compromisso de todos os integrantes da Instituição, e qualquer violação desta política será investigada e poderá resultar em uma ação disciplinar, bem como eventual responsabilização cível ou criminal do integrante da Instituição.

EMBRASI

Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

1. Pilares da Segurança da Informação

Os pilares abaixo elencados devem ser observados pela Instituição para atender aos padrões de Segurança da Informação no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis.

a) Confidencialidade

A Instituição visa garantir que o acesso as suas informações internas, relativas à própria Instituição, seus parceiros ou seus clientes, seja obtido somente por pessoas autorizadas e nas ocasiões em que este acesso for de fato necessário.

Procedimentos e medidas da Instituição que visam garantir a confidencialidade das informações podem ser consultados na Política de Privacidade e Proteção de Dados Pessoais, na Política de Cookies, na Política de Senhas, na Política de Anonimização e Pseudonimização e na Política de Mesa Limpa.

b) Integridade

A Instituição visa garantir a exatidão e a completude das informações através de seus métodos de processamento, bem como a integridade dos Dados Pessoais de titulares que estejam sob sua responsabilidade.

Procedimentos e medidas da Instituição que visam garantir a integridade das informações podem ser consultadas na Política de Criptografia, na Política de

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Antivírus e *Malware*, na Política e Plano de Respostas a Incidentes, e demais políticas, quando necessário.

c) Disponibilidade

A Instituição visa garantir que a informação esteja sempre disponível aos integrantes que de fato possuam as permissões de acesso necessárias, assegurando-se de que os dados estejam sempre disponíveis quando for preciso.

Procedimentos e medidas da Instituição que visam garantir a confidencialidade das informações podem ser consultadas na Política de Backup, na Política de Gestão de Ativos, Política de Acesso às Instalações Físicas, Política de Acesso Remoto e Acesso à Rede e na Política de Retenção de Dados.

d) Rastreabilidade

A Instituição visa garantir a disponibilidade de trilhas de auditoria de informações e meios de processamento, através de registros das transações e alterações realizadas em seus sistemas e aplicações.

Procedimentos e medidas da Instituição que visam garantir a rastreabilidade das informações podem ser consultadas na Política de Registro de LOGs, na Política de Bring Your Own Device, na Política de Acesso Remoto e à Rede, na Política de Acesso a Instalações Físicas e na Política de Comunicação de Dados Pessoais.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

2. Diretrizes de Segurança da Informação

As informações de titulares de Dados Pessoais devem ser tratadas de forma ética e sigilosa, de acordo com as diretrizes estabelecidas pela Política de Privacidade e Proteção de Dados Pessoais da Instituição e pelas demais políticas, legislações e regulamentações aplicáveis.

Todos os integrantes da Instituição devem ter ciência de que o acesso e uso aos sistemas de informação fornecidos pela Instituição são monitorados, e que os registros assim obtidos podem servir de evidência para a investigação de ocorrências e aplicação de medidas disciplinares, observando-se o disposto na Política de Acesso Remoto e Acesso à Rede.

Os integrantes da Instituição devem possuir uma identificação única, pessoal e intransferível, que seja capaz de o qualificar como responsável por suas ações, observando-se o disposto na Política de Senhas.

Informações confidenciais como senhas ou qualquer outra informação a qual o profissional possua em seu poder durante exercício do seu cargo devem sempre ser mantidas de forma secreta, sendo terminantemente proibido o seu compartilhamento, observando-se o disposto na Política de Senhas.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Os acessos devem sempre obedecer ao critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades.

Todo procedimento relacionado à segurança da informação deve garantir, durante toda a sua execução, a segregação de funções e atribuições, por meio da participação de mais de uma pessoa ou equipe.

As diretrizes e procedimentos contidos nesta Política de Segurança da Informação devem ser amplamente divulgadas entre as empresas pertencentes à Instituição e às empresas parceiras.

3. Gestão de Níveis de Acesso

Para assegurar a proteção adequada às informações da Instituição, somente profissionais autorizados devem possuir acesso às informações armazenadas pela Instituição, através da caracterização de documentos por nível de acesso e pela utilização de credenciais de acesso devidamente conferidas pelo Responsável pela Segurança da Informação. Estes níveis de acesso à informação são classificados da seguinte maneira:

- Informações Públicas: são informações de domínio público, que não contém quaisquer informações confidenciais ou sensíveis e podem ser acessados por qualquer pessoa, dentro ou fora da Instituição;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Informações Internas: são informações internas da Instituição, que contém informações relevantes e potencialmente confidenciais à Instituição, podendo ser acessados apenas pelos integrantes da Instituição, sob dever de confidencialidade;
- Informações Confidenciais: são documentos sigilosos da Instituição, que contém informações sensíveis e restritas da Instituição ou de seus clientes, podendo ser acessados apenas pelos integrantes da Instituição instituídos com as devidas credenciais de acesso.

Os acessos lógicos dos integrantes da Instituição devem ser controlados de forma que somente as informações necessárias ao desempenho de suas atividades estejam disponíveis, de acordo com as suas credenciais de acesso, conforme disposto na Política de Senhas.

O acesso físico dos integrantes da Instituição e visitantes aos locais que possuírem recursos tecnológicos da Instituição deve ser controlado mediante utilização de credenciais de acesso, conforme disposto na Política de Acesso a Instalações Físicas e Política de Acesso Remoto e Acesso à Rede.

As informações devem ser utilizadas pelos integrantes de forma transparente e apenas para as finalidades para as quais foram coletadas, sem expor os indivíduos a que dizem respeito.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

4. Gestão de Riscos, Objetivos e Incidentes de Segurança da Informação

Os riscos devem ser identificados por meio de um procedimento estabelecido para a avaliação dos riscos e ameaças à segurança da informação que possam afetar o negócio ou suas estratégias, alinhados com o contexto do negócio de forma a preservar e proteger adequadamente os ativos da Instituição, conforme previsto na Política e Plano de Respostas a Incidentes e na Política de Antivírus e *Malware*.

Os incidentes e eventos de segurança da informação devem ser analisados, tratados, registrados, monitorados e reportados ao Responsável pela Segurança da Informação, conforme previsto na Política e Plano de Respostas a Incidentes.

5. Treinamentos de Conscientização

A Instituição deve realizar treinamentos de forma regular e periódica, conforme estabelecido pelo Responsável pela Segurança da Informação, a fim de conscientizar todos os seus integrantes acerca do tema da Segurança da Informação. As ações de conscientização devem ser realizadas em diferentes formatos e abranger diferentes públicos, envolvendo treinamentos de modo presencial, treinamentos através de educação à distância (EAD) e campanhas informativas.