Política de Segurança da Informação

InterOp

Sumário

1. Introdução

O primeiro passo para a implementação do Sistema de Gestão de Segurança da Informação e Privacidade é a adoção de uma Política de Segurança da Informação, definida e aprovada pelo Comitê de Privacidade. Este documento depende da combinação de requisitos do negócio, de estrutura de processos, do uso de tecnologias e mecanismos de proteção e, o mais relevante, depende do comportamento de seus usuários, independentemente do nível hierárquico ou da atividade desenvolvida para a InterOp.

Para ampliar a cultura de segurança da informação e privacidade, a InterOp alinhada as boas práticas e normas internacionalmente aceitas, atualizou sua Política de Segurança da Informação (PSI), a fim de adequá-la à legislação nacional vigente e garantir a proteção de todos os seus ativos tangíveis e intangíveis.

2. Objetivo

O objetivo desta política é estabelecer as diretrizes necessárias para assegurar a confidencialidade, a integridade e a disponibilidade da informação e dados pessoais utilizadas pela InterOp.

Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da organização como resultado de falta de disponibilidade, falhas de segurança ou violação de dados pessoais.

3. Abrangência

Esta política abrange todas as informações, os sistemas e recursos de Tecnologia da Informação da InterOp, incluindo também os usuários (funcionários, diretores, colaboradores, estagiários, aprendizes, terceiros, parceiros, prestadores e fornecedores) em quaisquer das dependências da InterOp ou locais onde estes se façam presentes através da utilização, manuseio ou processamento das informações.

4. Diretrizes Gerais

A InterOp por meio dessa Política, busca:

- Assegurar o cumprimento de todas as suas obrigações legais, para atender aos requisitos regulamentares e contratuais pertinentes às suas atividades, a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD), 13.709 de agosto de 2018;
- Empregar medidas técnicas e organizacionais adequadas no tratamento de dados pessoais, e envidar esforços para proteção dos dados pessoais dos titulares de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses;

- Garantir a confidencialidade, integridade e disponibilidade das informações de seus titulares de dados pessoais e da própria organização, protegendo os sistemas de informação contra acessos indevidos e modificações não autorizadas;
- Assegurar que somente pessoas autorizadas tenham acesso às instalações da InterOp, às informações e aos sistemas de informação;
- Conscientizar as pessoas das possíveis consequências para a organização e para os seus usuários, sobre incidentes de segurança da informação ou violação as políticas de segurança e privacidade;
- Garantir a continuidade de seus negócios, protegendo os processos críticos contra falhas ou desastres significativos;
- Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos de segurança da informação e privacidade, enfatizando as obrigações das pessoas pela proteção de dados;
- Garantir que todas as responsabilidades pela segurança da informação e privacidade, estão claramente definidas e que as pessoas indicadas são competentes e capazes de cumprir com as atribuições;
- Melhorar continuamente o Programa de Segurança e Privacidade.

4.1 Conformidade

A conformidade com requisitos legais e contratuais é responsabilidade de todos os colaboradores da InterOp. Os líderes imediatos devem identificar e observar a legislação aplicável à InterOp, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

Os requisitos da Lei Geral de Proteção de Dados (LGPD) e a Política de Proteção de Dados devem ser observados por todos os colaboradores visando preservar a privacidade do Titular dos Dados pessoais. Em nenhum caso, o colaborador poderá vender ou transferir informações da InterOp ou de responsabilidade desta a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia. A confidencialidade e sigilo de dados pessoais devem ser observados, preservados e garantidos por todos os usuários da InterOp.

4.2 Uso de e-mail

O correio eletrônico é um recurso de comunicação institucional da InterOp e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta PSI, além das demais diretrizes da Política de Proteção de Dados. Portanto fica proibido o uso de compartilhamento de informações da InterOp com e-mail pessoal, e é vetado o acesso à e-mail particular de dentro da rede da InterOp.

4.3 Uso de internet

A Internet é uma ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A InterOp mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, assinaturas, notas, limites de tráfego e armazenamentos. A InterOp não autoriza a utilização dos meios de comunicação da organização para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios éticos e morais da InterOp.

4.4 Uso das redes sociais e WhatsApp

A publicação de conteúdo referente à InterOp em mídias, mensageiros instantâneos (WhatsApp, telegrama, Skype, etc.) e redes sociais, são feitas por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização.
Quando no uso de suas mídias e redes sociais particulares, empregados, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:

- Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual da InterOp sem autorização prévia e expressa;
- Não é permitida a criação, participação ou interação de/com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos da InterOp, excetuando-se os canais oficiais da empresa;
- Não é permitida a publicação de conteúdo ou comentários diretamente relacionados à InterOp, seus empregados, terceiros contratados e prestadores de serviço;
- Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da InterOp sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais.

4.5 Uso de computação em nuvem

O uso de recursos de computação em nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação.
A InterOp disponibiliza para os colaboradores um espaço em nuvem para armazenamento de arquivos relacionados às atividades realizadas dentro da InterOp. Sendo assim fica proibido o acesso a drives em nuvens particulares.

4.6 Uso de dispositivos móveis

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da InterOp devem considerar, prioritariamente, os requisitos legais e a estrutura da organização, atendendo a esta Política de Segurança da Informação e a Política de Proteção de Dados, e devem ser regidas por normas específicas, a qual contempla as recomendações sobre o uso desses dispositivos.

4.7 Uso de antivírus

Toda estação de trabalho e servidor deve possuir antivírus (software) instalado e atualizado automaticamente.
É responsabilidade da área de Tecnologia da Informação assegurar o processo de controle de malware na InterOp.
É responsabilidade do colaborador comunicar à área de Tecnologia da Informação comportamentos associados a malwares e ransomware em suas estações de trabalho. O uso de dispositivos do tipo “mídia removível” (pen drives, discos externos e smartphones) é expressamente proibido e as exceções devem ser autorizadas formalmente.

4.8 Pasta de rede

Informações relacionadas ao negócio da InterOp não devem estar armazenadas em estações de trabalho e equipamentos móveis, tais como laptops, pendrives, hd externo, celulares e tablets, devem ser armazenadas em diretórios de rede para que o processo de cópia de segurança seja assegurado. É responsabilidade dos colaboradores garantir que estas informações estejam em diretórios de rede.

4.9 Monitoramento

A InterOp reserva o direito para si de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Incluindo-se o uso particular (pessoal) através destes recursos, quando da existência de informações e/ou evidências de atos ilícitos ou conduta inadequada. Estes registros também podem ser utilizados para análises estatísticas visando a boa prestação de serviços e para verificação em casos relacionados a incidentes de segurança.

5. RISCOS

A não observância dos princípios e diretrizes constantes nesta Política e seus documentos complementares, pode impactar seriamente a InterOp, possibilitar a violação de leis e regulamentos, e afetar negativamente a reputação e a estabilidade financeira da InterOp.

Desvios e exceções devem ser tratados pelo Comitê de Privacidade.
Suspeitas de violação de dados pessoais devem ser comunicadas ao superior imediato, Encarregado de Dados e/ou através de abertura de chamados.

6. RESPONSABILIDADES

6.1 Colaboradores

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT, estagiário, menor ou jovem aprendiz, terceirizado, prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da InterOp.
É dever dos colaboradores:

- Respeitar e cumprir esta Política de Segurança da Informação e seus documentos complementares;
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição durante seu horário de trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
- Relatar prontamente à área responsável, qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, violação de dados pessoais, fragilidade, mau funcionamento, presença de vírus etc.;
- Assegurar que as informações e dados de propriedade da InterOp não sejam disponibilizados a terceiros, ou sem a devida autorização por escrito do responsável hierárquico;
- Comprometer-se em não auxiliar terceiro e ou provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.

6.2 Recursos Humanos

- Ter postura exemplar em relação à segurança da informação e privacidade, servindo como modelo de conduta para os colaboradores e prestadores de serviço sob a sua gestão;
- Assegurar que todos os candidatos a emprego sejam adequadamente analisados, especialmente em cargos ou serviços com acesso a informações, dados pessoais e dados pessoais sensíveis. São obrigatórias as verificações de referência profissional;

- Garantir que todos os novos colaboradores recebam instruções sobre sua responsabilidade pela segurança da informação e privacidade, com os aspectos culturais, missão, visão, valores, normas, regulamentações, políticas, direitos e deveres que são esperados dele na InterOp, assinando o Termo de Compromisso do Colaborador;
- Garantir a solicitação de criação de perfis de acesso ao ambiente de tecnologia da informação e as dependências da InterOp para as áreas responsáveis;
- No caso de terceiros que necessitem ter acesso a informações e dados pessoais da organização, deverá ser assinado o Termo de Compromisso com Terceiros ou mediante pedido judicial e/ou Administração Pública;
- Estabelecer Plano de Treinamento e Conscientização em segurança da informação e privacidade, garantindo a ciência e aderência dos colaboradores e terceiros aos princípios e diretrizes da segurança da informação e proteção de dados;
- Garantir a devolução dos ativos de TI da InterOp e a solicitação de retirada de acesso de todos os colaboradores e terceiros no encerramento de suas atividades, contratos ou acordos;
- Aplicar as medidas disciplinares formais vigentes para os colaboradores e terceiros que tenham cometido incidente de segurança ou violação de dados pessoais, garantindo inclusive, dissuasão para que novas violações não ocorram.

6.3 Tecnologia de informação

- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes e violação de dados pessoais;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI;
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente;
- Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao

menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

- Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
- Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a organização;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;
- Proteger continuamente todos os ativos de informação da organização contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

6.4 Jurídico

Atuar previamente nos processos, validando as minutas que devem estar alinhadas aos controles de segurança da informação e privacidade aplicáveis, especialmente os Termos de Confidencialidade e as cláusulas de proteção de dados.
Fornecer ao Comitê orientações a respeito da conformidade legal nos seguintes temas:

- Direitos de propriedade intelectual;
- Proteção de registros organizacionais;
- Proteção de dados e privacidade de informações pessoais;
- Prevenção de mau uso de recursos de processamento de informação;
- Segurança da Informação e Comunicação;
- Guarda de registros de conexão e dados cadastrais; e
- Combate a corrupção.

6.5 Alta direção

- Aprovar esta Política;
- Atualizar esta política em decorrência de alterações legais, normativas ou estatutárias, tendo-se por derrogada qualquer disposição nela

descrita que resultar incompatível com alterações futuras do Estatuto Social da organização ou de norma legal, sendo no mínimo obrigatório a revisão anual ou a cada mudança que possa afetar o SGI;

- Zelar pela aplicação efetiva das melhores práticas em Segurança da Informação e Privacidade;
- Garantir que medidas corretivas sejam tomadas quando desconformidades forem identificadas.

6.6 Políticas e normas complementares

Serão criadas, aprovadas e implementadas as seguintes políticas complementares, para apoiar no Programa de Privacidade da InterOp:

1. Política de Segurança da Informação;
2. Norma de uso dos ativos TI;
3. Norma de Acesso Remoto;
4. Norma de Controle de Acesso;
5. Norma de uso de dispositivos móveis;
6. Norma de Gestão de Vulnerabilidades;
7. Norma de Respostas a Incidentes;
8. Política de Proteção de Dados;
9. Política de Backup e restauração
10. Política de Classificação da Informação;
11. Norma de Monitoramento.

7. DOCUMENTOS DE REFERÊNCIA

- **LEI Nº 13.709/18:** Lei Geral de Proteção de Dados Pessoais (LGPD);
- **ABNT NBR ISO/IEC 27001:2013:** Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos;
- **ABNT NBR ISO/IEC 27002:2013:** Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação;
- **ABNT NBR ISO/IEC 27032:2015:** Tecnologia da Informação — Técnicas de Segurança — Diretrizes para Segurança Cibernética;
- **ABNT NBR ISO/IEC 27701:2019:** Tecnologia da Informação — Técnicas de Segurança — Extensão à ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes;

8. SIGLAS E DEFINIÇÕES

- **Comitê de Privacidade:** Comitê estabelecido pela InterOp e tem como principal função ajudar na elaboração e na revisão contínua da Política de Segurança da

Informação, assim como na avaliação dos controles utilizados e na resposta pelos incidentes gerados a partir dos eventos de segurança da informação e privacidade.

- **Confidencialidade:** Garantia que a informação, quando necessária, esteja acessível apenas aos colaboradores e/ou processos autorizados, e seja devidamente protegida do conhecimento ou acesso alheio.
- **Integridade:** Garantia que uma informação esteja correta, verdadeira e não seja corrompida ou perda suas características originais.
- **Disponibilidade:** Garantia que a informação e seus ativos de tecnologia da informação sejam preservados e estejam disponíveis sempre que necessário, mediante a devida autorização para seu acesso e/ou uso.
- **Informação:** É o resultado do processamento, manipulação e organização de dados;
- **Usuários:** Todos os indivíduos que acessam as informações da organização são usuários, sejam cooperados, conselheiros, membros dos comitês, diretores, colaboradores, estagiários, jovens aprendizes, terceiros, parceiros, prestadores e fornecedores.
- **Vírus:** Um vírus de computador é um programa que, quando executado, se autorreplica inserindo cópias de si mesmo em outros programas, arquivos de dados ou no setor de boot do disco rígido. Quando a replicação é bem sucedida diz-se que estas áreas estão infectadas. Estas viroses frequentemente trazem algum tipo de dano para as atividades dos sistemas infectados tais como: diminuição do espaço de armazenamento dos discos rígidos, aumento da carga de processamento dos processadores, acesso à informação privada, corrupção de dados, exibição de mensagens políticas ou humorísticas na tela do usuário, roubo dos contatos do usuário ou captura do conteúdo digitado.