MANUAL DE GOVERNANÇA DA SEGURANÇA DE INFORMAÇÃO

V1. 15/04/2025

Sumário:

Introdução.....3

Objetivo:.....3

Escopo:.....3

1. Responsabilidades de Segurança da Informação......3

1.1. Responsabilidades:.....3

1.2. Comitê de Segurança da Informação:.....3

2. Políticas de Segurança da Informação.....4

Classificação e Rotulagem de Informações:.....4

Lei Geral de Proteção de Dados.....6

- **Atendimento à Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.749, de 14/08/2018)**. .6

Uso Aceitável dos Recursos de TI:.....7

Procedimentos e Diretrizes de Segurança.....7

- **Gestão de Senhas:**.....7
- **Cópias de Segurança e Recuperação de Desastres:**.....7
- **Auditoria e Monitoramento:**.....7
- **Treinamento de Sensibilização em Segurança:**.....7
- **ISO 27001:2022:**.....8
- **Segurança de Informação e Proteção de Dados:**.....8

Termo de Ciência e Acordo para Integrantes da Staffer Talentos e Tecnologia Ltda.....9

Introdução

Objetivo:

Este Manual tem como objetivo construir diretrizes, orientações e regras para combater vazamento de dados e quaisquer riscos impelidos na manipulação dos mesmos, além de informar sobre as condutas e normas da **STAFFER** sobre LGPD e Segurança da Informação. As diretrizes deste manual devem ser aplicadas por todos os gestores, administradores, colaboradores e fornecedores independentemente de serem pessoa física ou jurídica ou de prestarem serviços em caráter eventual, que de alguma forma representem a STAFFER TALENTOS ou atuem em seu nome perante a empresas ou órgãos públicos ou privados.

Escopo:

Determinar as diretrizes que embasam a política de segurança da Informação adotada pela STAFFER. Este manual é de aplicação abrangente a todas as áreas da empresa e requer estrita conformidade em sua totalidade. A falta de observância das diretrizes estabelecidas neste documento pode acarretar investigações, advertências, suspensões do trabalho, imposição de multas e, em casos de gravidade extrema, a rescisão do vínculo profissional do indivíduo em questão.

1. Responsabilidades de Segurança da Informação.

1.1. Responsabilidades:

Cabe ao colaborador a responsabilidade pela integridade de todos os dados sob sua custódia durante a realização de suas atribuições profissionais. A preservação das informações confiadas pelos clientes assume relevância primordial, devendo ser aderido rigorosamente às diretrizes de segurança, de modo a evitar qualquer possibilidade de vazamento ou perda de informações.

1.2. Comitê de Segurança da Informação:

No evento de denúncias e incidentes de vazamento de dados, o Comitê de Denúncia procederá com investigações e conduzirá auditorias relacionadas aos casos.

2. Políticas de Segurança da Informação

Classificação e Rotulagem de Informações:

Para melhor compreensão de como serão classificados os dados e os processos que os envolvem, abaixo estão identificados as classificações dos dados, suas rotulagens, categorias de acessos e uso das informações.

Classificação de Dados Sensíveis:
Dados do cliente: Informações pessoais, como nomes, endereços, números de telefone, e-mails, devem ser rotulados como "Confidenciais".

Dados de pagamento: Informações de cartão de crédito, números de contas bancárias e informações de pagamento devem ser rotuladas como "Altamente Confidenciais".

Demais dados, utilizados em projetos específicos e que por determinação do cliente da STAFFER, devam ser considerados sensíveis, confidenciais ou altamente confidenciais, também deverão ser classificados, armazenados, ou manipulados com o mesmo critério e rigor.

Classificação por Níveis de Acesso:
- Interno: Documentos e informações de uso interno da empresa.
- Restrito: Dados que só podem ser acessados por equipes autorizadas.
- Público: Informações que podem ser compartilhadas publicamente.

Classificação de Projetos:
- Projetos em andamento: Rotulados de acordo com o status do projeto, como "Em desenvolvimento" ou "Em fase de teste".
- Projetos arquivados: Projetos encerrados e arquivados com uma identificação correspondente.

Rotulagem de Vulnerabilidades:
- Vulnerabilidades críticas: Problemas de segurança de alto risco que requerem ação imediata, que podem comprometer sigilo de informações, necessitam de senhas de acesso com confirmação em 2 ou 3 níveis
- Vulnerabilidades menores: Problemas menos críticos, mas que ainda precisam ser tratados com rigor para que não causem danos mais severos e impactem direta ou indiretamente em sistemas anexos ao principal.

Classificação de Documentação Técnica:

- Manuais de Usuário: Documento orientativo para guiar os usuários no uso adequado de software ou sistemas.
- Documentação Técnica: Todos os documentos pertinentes a um processo ou projeto que deverão estar atualizadas para informações internas das equipes de suporte.

Classificação de Incidentes de Segurança:

- Incidentes graves: Classificam-se em incidentes de segurança críticos que podem causar sérios danos a vazamento de informações, permitir acessos não autorizados a informações sensíveis, degradação da imagem e serviço prestados pela empresa.
- Incidentes menores: Problemas de segurança que não tem interferência direta em bases de dados que contenha informações sensíveis, mas que requerem atenção e rigor no tratamento e solução de forma rápida.

Classificação de Ativos de TI:

Todos os ativos de TI deverão ser identificados fisicamente através de etiqueta com código de barras e digitalmente em arquivos de base de dados cujas informações estarão disponíveis para a gestionar quanto a cadastro com suas características técnicas, tempo de uso, responsável pelo uso, por qual período, retirada e devolução na empresa, alarme para manutenção periódica, tempo em manutenção, e obsolescência.

- Hardware: Etiquetas/códigos de barras para diferentes tipos de equipamentos, como servidores, computadores, periféricos, etc.
- Software: Identificação completa a partir do momento de sua aquisição, motivo de uso, responsável pelo uso, fabricante, empresa que comercializou, notas fiscais, categorização de software, incluindo sistemas operacionais, aplicativos e ferramentas.

Classificação de Tickets de Atendimento/Suporte:

A abertura dos tickets deverão ser classificadas como atendimento de dúvidas, suporte para instalação, suporte para manutenção/uso, defeito e troca. Cada um dos chamados que gerarão os tickets, deverão ser classificados por prioridade para encaminhamento no atendimento e solução que obedecerão os SLAs correspondentes.

- Prioridade: identificadas como "Prioridade Alta", "Prioridade Média" ou "Prioridade Baixa".

Controle de Acesso:

Os acessos deverão ser solicitados de acordo com as necessidades de uso e justificadas quanto ao uso individual ou compartilhado das informações acessadas. As informações compartilhadas serão de inteira responsabilidade de quem solicitou o acesso e compartilhou tais informações. Em caso de incidente gerado, através de vazamento de informações sensíveis, o solicitante do acesso estará sujeito as penalidades previstas na política de

Compliance, que estabelece que em hipótese alguma as informações tratadas pelos funcionários STAFFER, poderão ser utilizadas para outros fins que não sejam os determinados pela atividade a que foram destinados.

- A atribuição de acesso a pastas específicas e ferramentas será realizada com base nas hierarquias organizacionais, bem como nas funções individuais dos colaboradores. Em caso de necessidade de solicitar ou revogar acessos, favor consultar o Manual de Políticas de Acesso para obter orientações pertinentes.

Gestão de Incidentes:

Para gestionar os incidentes, serão utilizados os critérios já mencionados anteriormente e serão aplicadas advertências proporcionais ao dano.

- Os incidentes devem ser comunicados através do canal de denúncia da STAFFER. Após o relato, o Comitê de Denúncia procederá à classificação do incidente, considerando sua gravidade, e, em conformidade, iniciará uma investigação visando esclarecer os eventos que deram origem ao incidente.

Lei Geral de Proteção de Dados

- **Atendimento à Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.749, de 14/08/2018)**

Para o atendimento das regras estabelecidas na LGPD à STAFFER definiu em suas práticas:

1.1. Informar, orientar e treinar os seus profissionais quanto às normas estabelecidas na Lei Geral de Proteção de Dados Pessoais – LGPD.

1.2. Que todo o profissional da STAFFER alocado em um determinado cliente, por prazo determinado ou indeterminado, em um projeto que trate de dados pessoais deverá:

1.2.1. Obedecer a todas as metodologias, normas e procedimentos das práticas de proteção de dados, segurança e sigilo das informações determinadas e adotadas pelo cliente;

1.2.2. Estará atento para que, no que tange a sua responsabilidade, proteger todos e quaisquer dados pessoais, dados sensíveis e dados de crianças que tiver acesso no desenvolvimento de seu trabalho.

1.2.3. Atuar sempre como “Operador” nos conceitos estabelecidos pela LGPD obedecendo sempre as determinações do “Controlador” de Dados que sempre deverá ser de responsabilidade de um profissional nomeado pelo cliente STAFFER.

1.3. Permitir aos seus Clientes que façam, sempre que necessário, as auditorias de seus ambientes, processos e práticas de adequação e conformidade com a LGPD.

1.4. Manter seus ambientes de Sistemas internos e de eventuais acessos aos sistemas dos clientes seguros e protegidos contra práticas de invasão de dados.

1.5. Que todos os profissionais formalizem o cumprimento das normas estabelecidas

na LGPD firmando este documento.

Uso Aceitável dos Recursos de TI:

Os profissionais que fazem uso de notebooks ou celulares corporativos assumem o compromisso de preservar a integridade desses dispositivos, bem como de utilizá-los estritamente para as atividades correlatas ao desempenho de suas funções laborais. Qualquer uso pessoal dos referidos equipamentos, assim como sua utilização para fins de entretenimento, é expressamente proibido.

Procedimentos e Diretrizes de Segurança

- **Gestão de Senhas:**

  As senhas devem conter no mínimo 8 caracteres, sendo no mínimo um deles maiúsculo e um caracter numérico.

- **Cópias de Segurança e Recuperação de Desastres:**

  A STAFFER mantém cópias de segurança em nuvem para todos os dados que são processados por ela. Em situações de recuperação de desastres, a empresa dispõe de equipamentos de reserva para minimizar os impactos e também disponibiliza acesso remoto às informações.

- **Auditoria e Monitoramento:**

  A STAFFER conduz auditorias semestrais com o propósito de identificar potenciais riscos e vulnerabilidades, de modo a estar preparada para enfrentar eventuais incidentes. Em caso de ocorrência de um incidente, a empresa iniciará auditorias específicas para apurar os eventos que lhe deram origem, além de manter um monitoramento contínuo do fluxo de informações.

- **Treinamento de Sensibilização em Segurança:**

  A STAFFER assume o compromisso de proporcionar formação contínua e manter os seus colaboradores informados a respeito de sensibilização em segurança, boas práticas e prevenção de vazamentos de dados.

  A empresa disponibilizará treinamentos durante o processo de integração, bem como treinamentos de reciclagem para profissionais envolvidos em incidentes, treinamentos semestrais para colaboradores que lidam com dados críticos e treinamentos anuais para os demais integrantes da organização.

Conformidade Regulatória

- **ISO 27001:2022:**

A STAFFER assume o compromisso de assegurar a segurança da informação e de aderir estritamente aos padrões estabelecidos pela norma ISO 27001:2022. Para cumprir esse compromisso, a empresa faz uso de suas ferramentas e processos de melhoria contínua, mantendo-se alinhada aos requisitos da ISO.

- **Segurança de Informação e Proteção de Dados:**

A STAFFER TALENTOS assume o compromisso de salvaguardar qualquer forma de informação ou dados que estejam sob sua gestão, quer sejam provenientes de clientes ou colaboradores. Dispomos de tecnologias avançadas de criptografia e rastreamento de dados, além de procedimentos estabelecidos para o controle e distribuição eficaz de informações.

Termo de Ciência e Acordo para Integrantes da STAFFER Talentos e Tecnologia Ltda.

Declaro que recebi, li e entendi o Manual de Governança da Segurança de Informação da STAFFER Talentos e estou ciente das diretrizes estabelecidas e sua relevância para mim e para a empresa.

Comprometo-me a cumpri-lo integralmente, sob pena de sujeitar-me às medidas punitivas e rescisórias previstas em contrato de trabalho e legislação vigente.

Nome Completo:

Data:__/__/___ Assinatura:

Este termo consta de duas vias, uma para o Integrante e outra para a sua pasta funcional