Governança

POL – 0021_Política de Segurança da Informação

@libertyhealth.io
(61) 3202-3222

R. Funchal, 203
Vila Olímpia, São Paulo

Histórico de Versões

Data	Versão	Descrição	Autor
21/02/2024	1.0	Documento Política Segurança da Informação_V1	Angélica Ferreira/Diego Pereira
11/03/2024	2.0	Documento Política Segurança da Informação_V2	Angélica Ferreira/Diego Pereira

1. Objetivo

A Política de Segurança da Informação estabelece normas e diretrizes com a finalidade de garantir a disponibilidade, integridade e confidencialidade dos dados de segurança da informação, aplicadas às necessidades da Liberty Health Tech.
Os colaboradores e terceiros devem assegurar o cumprimento de todas as políticas, regras e orientações de segurança da informação adotadas pela área de Gestão da Segurança da Informação, com o objetivo de assegurar a disponibilidade, integridade e confidencialidade de dados.
É de responsabilidade de todos, garantir que as diretrizes da Política de Segurança da Informação estabelecidas pela Gestão da Segurança da Informação sejam seguidas.

2. Abrangência

As normas e diretrizes definidas neste documento aplicam-se à toda organização, terceiros e parceiros da Liberty Health Tech.

3. Conteúdo Geral

3.1. Definições

Nome	Descrição
Informação	É um ativo da empresa e, como todo ativo, deve ser protegido. A informação pode ser escrita ou impressa em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou falada em conversas.
Política de Segurança	A Segurança da Informação é composta pela manutenção da confidencialidade, integridade e disponibilidade da informação, promovendo a conscientização interna dos profissionais que atuam na Liberty Health Tech (direta ou indiretamente). Como extensão da Segurança da Informação existe a Segurança da Informação para ataques externos, chamada de Cibernética, que se preocupa em defender dados sensíveis que possam ser acessados por hackers.
Confidencialidade	É a garantia de que a informação é acessível somente a pessoas autorizadas.
Integridade	Integridade refere-se à preservação dos dados e informações, de forma a salvaguardar a exatidão e completeza da informação e dos métodos de processamento, impedindo que sejam corrompidos, danificados e/ou comprometidos.

Disponibilidade	A disponibilidade está relacionada à acessibilidade dos dados e das informações sempre que necessário.
Virus e software malicioso	Entende-se por vírus qualquer programa que tem a capacidade de se reproduzir automaticamente, sem o conhecimento ou autorização do usuário. Entende-se por software malicioso qualquer software que realize ações nocivas aos sistemas, como vírus, Cavalo de Tróia, verme (worm) e afins.
VPN	Rede Privada Virtual
OSI	Objetivo de Segurança da Informação
OE	Objetivo Estratégico
VPC	Nuvem Privada Virtual

4.1. Diretrizes Gerais

Diversas informações da Liberty Health Tech, de seus colaboradores, clientes e parceiros estão sob responsabilidade de pessoas físicas e jurídicas, que agem em nosso nome ou benefício. Por isso, a Liberty Health Tech espera que todos que têm acesso a informações de negócio e/ou dados pessoais sejam cautelosos com exposições indevidas na vida social e digital (transporte público, festas, bares, e-mails, comentários e publicações em redes sociais etc.).
Em caso de violação das diretrizes definidas nestas Políticas e em outros Procedimentos Operacionais Padrão, as medidas cabíveis previstas no acordo contrato estabelecido serão tomadas.
A Liberty Health Tech tem compromisso com a melhoria contínua dos processos. Desta forma, eventuais dúvidas e relato de incidentes de segurança da informação e privacidade de dados, podem ser realizados por meio do registro de ocorrência com a área de Segurança da Informação.

4.1.1 Objetivos da Segurança da Informação

Para garantir o cumprimento dos objetivos da segurança da informação, há a definição dos indicadores estratégicos, e respectivo acompanhamento.
Por meio do acompanhamento dos indicadores, será possível avaliar a eficiência dos processos e identificar falhas, permitindo assim, a promoção da melhoria contínua dos processos organizacionais relacionados à Segurança da Informação.

4.2. Confidencialidade

Ao estabelecer o contrato de trabalho, o colaborador deverá assinar o Acordo de Confidencialidade, no qual se compromete a seguir todas as normas e procedimentos estabelecidos pelo Sistema de Gestão da Segurança da Informação, firmando assim seu comprometimento à disponibilidade, integridade e confidencialidade dos dados que tiver acesso.

Os prestadores de serviços, parceiros e terceiros que venham a ter acesso aos sistemas internos da Liberty Health Tech e/ou de seus clientes, deverão firmar acordo de confidencialidade de seus administradores, empregados ou subcontratados envolvidos na prestação de serviços, exigindo a manutenção de estrito sigilo e confidencialidade das informações que vierem a receber ou tomar conhecimento em decorrência do respectivo contrato, firmando assim seu comprometimento à disponibilidade, integridade e confidencialidade dos dados que tiverem acesso.

4.3. Treinamento e conscientização da Segurança da Informação

Treinamentos relativos à segurança da informação serão disponibilizados na plataforma E-learning orientados pela Liberty Health Tech.
Campanhas de conscientização são feitas periodicamente com o intuito de orientar e reforçar a importância da segurança da informação na Liberty Health Tech.
Parceiros, prestadores de serviços e terceiros que venham a ter acesso aos sistemas internos também são orientados a seguirem a Política da Segurança da Informação.

4.4. Propriedade Intelectual

Todo e qualquer trabalho desenvolvido e armazenado com a utilização de recursos e informações da Empresa, ou durante a jornada de trabalho do colaborador e/ou prestador, é de propriedade da Liberty Health Tech, sendo facultada à Empresa a reivindicação da propriedade intelectual parcial ou total sobre o trabalho produzido.
Apenas a Diretoria pode autorizar o uso ou transferência de qualquer ativo cuja propriedade intelectual seja da Liberty Health Tech.
Nenhum software de propriedade ou licenciado para a Liberty Health Tech está autorizado a ser retirado da Empresa, seja por meio de mídias, cópias ou de links de comunicação, sob qualquer pretexto. Todo software deve ser usado em conformidade com licenças, observações, contratos e acordos aplicáveis.
Todos os colaboradores e/ou prestadores de serviços devem observar o uso legal de propriedade intelectual de terceiros, incluindo livros, artigos, filmes, áudios, imagens ou qualquer outro conteúdo sujeito à legislação de propriedade intelectual.

4.5. Legislação aplicável

Correlacionam-se com a Política, as diretrizes e as normas de Segurança da Informação, as leis abaixo relacionadas, mas não se limitando a elas:

- Lei 8.159/91, (dispõe sobre a política nacional de arquivos públicos e privados);
- Lei 9.610, de 19 de fevereiro de 1998 (dispõe sobre direitos autorais);
- Lei 9.279, de 14 de maio de 1996 (dispõe sobre marcas e patentes);

- Lei 3.129, de 14 de outubro de 1882 (Regula a concessão de patentes aos autores de invenção ou descoberta industrial);
- Lei 10.406, de 10 de janeiro de 2002 (institui o Código Civil);
- Decreto-Lei 2.848, de 7 de dezembro de 1940 (institui o Código Penal);
- Lei Federal 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

4.6. Papeis e Responsabilidades

É de responsabilidade de todos os colaboradores e prestadores de serviços, o comprometimento com os requisitos da segurança da informação e divulgação da Política de Segurança da Informação.

4.7. Arquitetura de Rede

A infraestrutura de rede da Liberty Health Tech possui uma arquitetura de Rede em Nuvem. A infraestrutura de segurança de acesso da Liberty Health Tech possui capacidade de atendimento aos principais serviços de conectividade disponíveis no mercado, como por exemplo: links privados, DMZ, Rede Wireless, VPN e VPC.
A infraestrutura dos principais serviços que estão em nuvem possui redundância de hardware, garantindo, assim, o maior nível de serviço para a empresa e nossos clientes, sendo esses recursos monitorados e gerenciados em uma plataforma web que permite total controle dos requisitos de segurança de rede, adotados pela Empresa.

4.8. Backup

Os procedimentos de realização de backups estão definidos em REG-0009-RegulamentoBackupRestore.

4.9. Antivírus

- Todos os computadores da Liberty Health Tech são protegidos com antivírus, que são mantidos atualizados de forma automática. A rede corporativa é protegida por Firewall.
- É terminantemente proibido ao colaborador introduzir, de forma consciente, vírus de computador nas estações de trabalho da Liberty Health Tech. A qualquer suspeita de contaminação por vírus, o colaborador deve imediatamente desligar a máquina no botão Power off e, em seguida, acionar a equipe de Segurança da Informação.
- Será considerado ato intencional de quebra de segurança, o ato de desligamento do antivírus homologado pela Liberty Health Tech, e será tratado como um incidente de segurança.

- A instalação de antivírus nas estações de trabalho da organização é realizada de forma manual para garantir o êxito da instalação, por intermédio da Infraestrutura. A atualização das vacinas é feita automaticamente, após o término da instalação.
- A atualização de vacinas é feita a partir de uma console central, que tem como objetivo principal gerenciar, monitorar, baixar novas versões de vacinas e distribuí-las de forma automática para todos os servidores e estações de trabalho, bastando apenas que o equipamento esteja conectado à internet ou à rede da Liberty Health Tech. Por meio da console central, é possível verificar quais estações e servidores estão com a vacina de antivírus atualizada ou desatualizada. Mensalmente são verificadas quais máquinas estão com o antivírus em mau funcionamento, desatualizado ou com algum alerta para que a Infraestrutura possa atuar de forma preventiva, corretiva, presencial ou remotamente.

4.10. Monitoramento

Todas as mensagens criadas, enviadas ou recebidas usando a rede corporativa ou com a utilização do e-mail corporativo são de propriedade da Liberty Health Tech, que se reserva ao direito de acessar todo o conteúdo, caso necessário.

O Software SGHX está habilitado para gerar arquivos de logs e armazená-los em cada servidor, respectivamente, por sua unidade. Este detalhamento está descrito no REG_0008_AmbientePadraoTrabalho
Caso seja identificado algum alerta ou registro inadequado, medidas cabíveis às correções serão aplicadas.

4.11. Incidentes de Segurança

Incidentes de Segurança são eventos que podem causar danos à confidencialidade, integridade, disponibilidade ou processamento das informações. Elas se materializam como incidentes ou atos intencionais realizados por agentes externos ou como incidentes por não seguir as diretrizes desta Política.
Caso algum incidente seja constatado pelos colaboradores, este incidente de segurança deve ser registrado na ferramenta de incidentes por abertura de chamado através da Central de Atendimento 0800 591 1956 ou e-mail: atendimento@libertyti.com.br.

4.12. Mesa Limpa

A Política de Mesa Limpa/Tela Limpa busca resguardar a Liberty Health Tech, bem como o próprio colaborador e/ou prestador contra o acesso não autorizado a informações como, por exemplo, terceiros observando dados expostos em mesas ou telas.

Assim, segue algumas diretrizes que devem ser seguidas:

- Documentos com informações pessoais e de terceiros, relatórios, livros e mídias eletrônicas que contenham informações confidenciais devem ser armazenados em armários trancados adequados e/ou em outras formas de mobiliário de segurança quando não estiverem em uso;
- Computadores pessoais e terminais de computador não devem ser deixados autenticados/registrados quando não houver um operador (usuário) junto, e devem estar com tela bloqueada (CTRL+ALT+DEL) por senha, quando não estiver em uso;
- Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;
- Papéis, anotações e lembretes da sua mesa de trabalho, devem ser mantidos, sempre que possível, fora da superfície da mesa (mesa limpa);
- Ao final do dia, ou no caso de ausência prolongada, deve-se limpar a mesa de trabalho, retirando objetos como bloco de anotações feitas e documentos;
- Documentos sensíveis/confidenciais sem utilidade devem ser destruídos de forma apropriada, utilizando-se por exemplo, a desfragmentadora de papel.

4.16. Mascaramento de dados

O mascaramento de dados (termo que engloba anonimização, pseudoanonimização, redefinição, limpeza ou desidentificação de dados), é um método de proteção de dados sensíveis que substitui o valor original por um valor equivalente fictício, mas realista. O mascaramento de dados também é chamado de camuflagem de dados.
O objetivo do mascaramento de dados é manter sua confidencialidade. Um mascaramento correto pode proteger o conteúdo dos dados e preservar o valor para o negócio. A segurança dos dados, em especial, dados pessoais e sensíveis se faz ainda mais necessária para garantir a confidencialidade das informações de colaboradores e clientes, evitando possíveis violações.

4.17. Auditoria

As auditorias são planejadas e executadas conforme procedimentos definidos em POP-0013_Auditoria.

5. Anexo

Não aplicável