Política de Segurança da Informação

VACCINAR

VACCINAR
nutrição e saúde animal

ÍNDICE

1. Objetivo

A política visa atingir um alto padrão de Segurança da Informação e deve guiar a conduta das pessoas no uso adequado e seguro de recursos de informação determinando algumas diretrizes. A preocupação com a Segurança da Informação é comum aos diversos níveis de gestão e um compromisso individual de todos.

2. Campo de aplicação

Esta política se aplica a todos os colaboradores e prestadores de serviços da Vaccinar.

2.1 Definições

Confidencialidade: É o aspecto relacionado a divulgação não autorizada, acesso e uso indevido da informação corporativa.
Integridade: A propriedade de que a informação não foi modificada ou corrompida, ou seja, preserva sua exatidão.
Disponibilidade: A propriedade de que a informação esteja sempre pronta para o uso devido e autorizado.

3. Diretrizes

3.1 Organização da Segurança da Informação

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação e auxilia a VACCINAR a cumprir com os objetivos e resguardar aqueles que são considerados os principais pilares: confidencialidade, integridade e disponibilidade.
A violação desta política e dos relevantes requisitos de segurança constitui na quebra de confiança entre o usuário e a VACCINAR e são passíveis de sanções disciplinares e contratuais.

3.2 Responsabilidades

As políticas, processos corporativos de Segurança da Informação e estratégias são acompanhados pelo Comitê Corporativo de Segurança da Informação, que será formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo de comitê em periodicidades pré-definidos.
O responsável pela Segurança da Informação deverá convocar formalmente as partes envolvidas para reuniões periódicas e em situações pré-definidas e/ou sempre que se fizer necessário para os negócios da VACCINAR.

3.3 Classificação da Informação

Toda informação deve ser classificada com base na confidencialidade e níveis que a informação exige, que são eles:

Informação Confidencial: informações destinadas a pessoas específicas (nível mais alto de confidencialidade);
Informação Restrita: informações destinadas a(s) área(s) específica(s) (nível médio de confidencialidade);
Informação Interna: somente membros da organização podem ter acesso (nível mais baixo de confidencialidade);
Informação Pública: todos podem ter acesso à informação (público interno e/ou externo).
Toda informação deve possuir um proprietário. O proprietário é responsável por classificar a informação e garantir que esta receba a proteção adequada em todo o seu ciclo de vida. Toda informação classificada deve ser rotulada de modo que evidencie a sua sensibilidade. Na ausência da classificação da informação, o nível de informação interna deverá ser considerado.

3.4 Controle de Acesso

Necessidades dos negócios

Deve haver diretrizes por escrito para o controle de acesso e senhas, baseadas nos requisitos de negócios e de segurança. As diretrizes devem ser reavaliadas regularmente e conter as devidas parametrizações e complexidades conforme a P-DTI 4.1 0 06.

Autorização para acesso

O acesso aos sistemas de informação deve ser autorizado pelos gestores imediatos conforme descrito na P-DTI 4.1 0 07.

3.5 Segurança Física e do Ambiente

Equipamentos de informática e informações que requeiram proteção devem estar situados em áreas fisicamente seguras e ter o controle de acesso adequado para garantir que somente as pessoas autorizadas tenham acesso.

Os data centers sobre o controle da organização devem ter os seguintes requisitos:

- Listagem de usuários que precisam do acesso permanente ao ambiente;
- Listagem de visitantes ao ambiente contendo data, hora, nome do visitante, empresa de atuação ou área e a aprovação do responsável pelo ambiente;
- Revisões periódicas dos acessos ao ambiente

3.6 Mesa limpa e tela protegida

É necessário que os colaboradores de todos os departamentos da Vaccinar tenham a consciência em manter a mesa limpa e tela protegida, de modo que papéis e mídias removíveis não fiquem expostos a acessos não autorizados quando o usuário não estiver utilizando à informação, reduzindo o risco de perda e danos à informação.

- Papéis, mídias de computadores, agendas, livros ou qualquer material quando não estiverem sendo utilizados, devem ser guardados de maneira adequada, preferencialmente em gavetas ou armários com chave, uma vez que estes podem conter informações confidenciais da empresa e particulares;

- Informações de usuário e senha de sistemas e/ou rede não devem ser anotadas em papel, ou registradas em meios de fácil acesso;

- Documentos que contenham informações relevantes sobre cargos e salários não podem ficar expostos e devem estar devidamente guardados em armários ou gavetas com chave;

- Para evitar danos indevidos aos ativos de informática evitar líquidos próximos aos teclados e computadores. (Utilizar áreas apropriadas para isto).

3.7 Dispositivos Móveis e Trabalho Remoto

As diretivas de uso dos disponíveis moveis estão descritas na P-DTI 4.1 0 01. Todo acesso remoto deve ser minunciosamente analisado e a sua concessão ocorrerá mediante solicitação formal e aprovação. É necessário que o requisitante assine o termo de responsabilidade de acesso e seja passível de sanções disciplinares por parte da VACCINAR.

3.8 Transferência da Informação

Devem ser estabelecidos procedimentos e controles para proteção adequada na geração, manuseio, armazenamento, transporte e descarte de informações. A troca de informações com terceiros, quer sejam clientes ou fornecedores requer o cumprimento de procedimentos acordados com a VACCINAR. O acesso a rede de dados e sistemas de informação envio e recebimento de e-mails e navegação na internet e telefonia, são regidos por procedimento e política de TI no documento: Manual do Funcionário – Capítulo 8.

3.9 Segurança nas Comunicações

A área de TI deve assegurar que a documentação dos sistemas de TI esteja de acordo com os procedimentos da VACCINAR. Antes de um novo sistema ser colocado em produção, planos e gerenciamento de mudanças e avaliações de risco devem ser realizados para evitar erros. Adicionalmente, procedimentos para monitoração e gestão de problemas não previstos devem ser utilizados. Os ambientes para desenvolvimento, teste e homologação, devem ser separados do ambiente de produção, a fim de reduzir o risco de acesso não autorizado ou mudanças e mitigar as condições de risco que propiciem erros.

3.10 Controles Criptográficos

Deve ser utilizado o uso de criptografia e controles de chaves para garantir a confidencialidade, autenticidade e integridade dos arquivos armazenados e transferidos, quando aplicável. Diretrizes para a administração e uso de criptografia para proteger as informações devem estar disponíveis.

3.11 Gestão de Ativos

Convém que todos os ativos da informação sejam claramente identificados de forma individual, inventariados, protegidos de acessos indevidos, com a documentação e planos de manutenção atualizados sempre que houver mudanças.

3.12 Tratamento de Incidentes

Os incidentes de segurança devem ser comunicados à gerência ou área de Segurança da Informação e todos colaboradores são responsáveis por relatar violações e possíveis quebras de segurança.

3.13 Proteção Contra Malware

Os recursos de processamento de dados devem ser protegidos contra vírus e outros códigos maliciosos de forma contínua.

3.14 Gestão de Riscos e Vulnerabilidades

A segurança da informação irá fornecer relatórios de vulnerabilidades dos sistemas da Vaccinar frequentemente. Os proprietários do sistema serão responsáveis por assegurar que as vulnerabilidades sejam tratadas reduzindo assim os riscos para um nível aceitável.

3.15 Backup

É necessário realizar regularmente backups e restauração desses backups. Os mesmos devem ser armazenados externamente ou em uma área separada do arquivo original e apropriadamente protegida, sendo somente acessível por pessoas autorizadas. Maiores informações na P_DTI_4.1_0_08.

3.16 Restrições Sobre Uso e Instalação de Software

A aquisição, contratação e/ou instalação de software devem ser solicitadas para área de TI através de chamado.

3.17 Segurança em Recursos Humanos

A área de Recursos Humanos da VACCINAR é a responsável em emitir e controlar os documentos físicos dos colaboradores, incluindo, mas não se limitando ao termo de confidencialidade assinado e o conhecimento sobre a disponibilidade das políticas e procedimentos relacionados à Segurança da Informação.

3.18 Conscientização em Segurança da Informação

A VACCINAR deve promover a conscientização dos colaboradores em relação aos princípios e diretrizes de Segurança da Informação através de campanhas, palestras, treinamentos e outros meios.

3.19 Proteção e Privacidade da Informação de Identificação Pessoal - LGPD

A VACCINAR respeita a privacidade quanto a coleta e registro de informações de seus colaboradores, prestadores de serviços, clientes e visitantes e tem o comprometimento de não divulgar sem a sua expressa permissão, a menos que seja formalmente autorizada ou obrigada por meio de decisão judicial, para fins de prevenção a fraudes ou outro crime. Tal ação é necessária para a proteção e defesa dos direitos das pessoas e segurança. Os funcionários e outros usuários externos devem ser avisados de que as evidências dos incidentes de segurança são armazenadas e a VACCINAR pode ser requisitada a entregá-las por decisão da justiça a fim de cumprir com a legislação existente e regras contratuais.

3.20 Relacionamento na Cadeia de Suprimentos

A VACCINAR deve assegurar a proteção dos ativos da organização e que são acessados pelos fornecedores. Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.
A gestão da cadeia de suprimentos não se restringe à movimentação de materiais, mas também presume em uma troca eficiente de informações, permitindo ações coordenadas.

3.21 Conformidade

A VACCINAR é comprometida com a utilização das melhores práticas e melhoria contínua de seus processos buscando sempre a conformidade tanto com requisitos legais sejam eles compulsórios ou não como também aos requisitos de clientes e com as normas institucionais.

3.22 Continuidade

Quando necessário, devem existir planos de continuidade e contingências que abranjam os sistemas de informação, de infraestrutura críticos e outros essenciais.
Os planos de continuidade do negócio devem ser focados nos riscos operacionais, estar alinhados com todos os planos de contingências e planos gerais da VACCINAR, serem testados regularmente para assegurar a adequação e que a gestão e os funcionários compreendem a sua execução. Os sistemas de produção e outros sistemas classificados como risco "alto" devem ter soluções de backup.

3.23 Uso Aceitável dos Ativos

Os colaboradores e prestadores de serviços são responsáveis pelo uso adequado das informações, dispositivos eletrônicos e recursos de rede utilizados ou que interajam com redes internas e devem estar com sua configuração em conformidade. Maiores informações na P-DTI 4.1 0 02.

4. Histórico de Revisões

Revisão	Data	Modificação
00	06/01/2020	Emissão inicial.
01	13/02/2020	Ajustes efetuados após reunião com gestores das áreas interessadas