POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A Política de Segurança da Informação (PSI) é uma declaração formal acerca do comprometimento com a proteção dos ativos de informações de propriedade e/ou sob a guarda do HORTOPREV, devendo ser cumprida e respeitada por todos os servidores e colaboradores. O HORTOPREV, que lida com dados sensíveis de segurados, fornecedores e colaboradores, tem como objetivo a implantação da PSI para garantir a segurança dos dados das quais são de sua responsabilidade, que as informações provenientes de fontes externas (fornecedores e segurados) que trafegam pelo sistema desenvolvido e fornecido pelo HORTOPREV, estejam protegidas, evitando qualquer intercepção, fraude ou perda. Além de prover a conscientização interna, para que as normas sejam seguidas por todos seus servidores e colaboradores, garantindo a confidencialidade, integridade e disponibilidade das informações, não somente de segurados e fornecedores, porém dos próprios servidores do instituto.

2. DEFINIÇÕES

2.1. Ativos de Informação

Conforme definição da norma ABNT NBR ISO/IEC 27002:2013,

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. […] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Assim, para efeitos desta Política de Segurança da Informação, são considerados os seguintes Ativos de Informação:

- Recursos de Tecnologia da Informação;
- Informações pertencentes, concedidas ou relacionadas aos segurados;
- Informações relacionadas aos servidores e colaboradores do HORTOPREV;
- Informações pertencentes ou relacionadas aos fornecedores;
- Estratégias e decisões da alta administração;
- Informações contábeis do HORTOPREV;
- Processos internos do HORTOPREV;

2.2. Princípios da Segurança da Informação

Princípios Básicos

Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
Confidencialidade: garantia de que o acesso à informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos sem autorização.

Disponibilidade: garantia de que os usuários autorizados tenham acesso à informação quando necessário.

Resiliência: garantia de que o sistema estará disponível para acesso das informações pelo tempo necessário, utilizando de redundância e escalabilidade sempre que possível.

Princípios Complementares

Autenticidade: Garantia da identidade do remetente da informação. Pela autenticidade garante-se que a informação é proveniente da fonte anunciada, sem sofrer alteração durante o envio.

Legalidade: Garantir que o uso e manuseio das informações seguem as leis vigentes no país (Lei de crimes cibernéticos – Lei 12.737/2012, Marco Civil da Internet – Lei 12.965/2014 e LGPD LEI Nº 13.709/2018).

Não repúdio: Garantia de que o autor não negue ter criado e assinado determinado arquivo ou documento.

2.3. Incidentes de Segurança da Informação

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos Recursos de Tecnologia da Informação (RTIs) levando a perda de um dos princípios da Segurança da Informação, mencionados anteriormente. São exemplos de incidentes de segurança:

- Tentativas de ganhar acesso não autorizado a sistemas ou dados lógicos ou físicos;
- Indisponibilidade de informações e dados para a execução de rotinas e processos;
- Ataques de negação de serviço;
- Exploração de vulnerabilidades de protocolos;
- Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio de um gestor;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

a. Comunicação de Incidentes:
O HORTOPREV deve divulgar e incentivar seus colaboradores a reportarem imediatamente os casos de incidentes de segurança da informação, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

b. Tentativa de Burla:
Qualquer tentativa de burla às diretrizes e controles estabelecidos pelo HORTOPREV, quando constatada, deve ser tratada como uma violação.

2.4. Sistema de Gestão da Segurança da Informação

O Sistema de Gestão da Segurança da Informação (SGSI) deverá fazer parte do sistema de gestão global do HORTOPREV, baseada em uma aproximação de risco empresarial, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a Segurança da Informação.

a. Estrutura:
A estrutura apresentada pela ISO 27.001 para um sistema de gestão da segurança da informação, leva em consideração o contexto em que a organização está situada, bem como as expectativas e requisitos passados pela Liderança e pela equipe de apoio que irá participar da execução do sistema. O ciclo da segurança da informação inicia em seu planejamento, passa por sua operação, avaliação do desempenho do sistema e por fim sua melhoria contínua. Desta forma, liderança e apoio retornam à segurança da informação gerenciada.

Este ciclo de planejamento, operação, avaliação de desempenho e melhoria, que se repete ao longo do tempo, junto com a liderança e o apoio é a garantia da efetividade para a segurança da informação da HORTOPREV. O Sistema de Gestão para a Segurança da Informação abrange as esferas da Tecnologia (controles de segurança em ativos tecnológicos e o uso seguro da tecnologia), Processos, Ambientes (acessos físicos e proteção ao ambiente de trabalho) e Pessoas (conscientização de pessoas no tratamento e uso seguro das informações).

b. Detalhamento
A Norma ABNT NBR ISO/IEC 27.002 Código de Práticas para Controles de Segurança da Informação fornece diretrizes de práticas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes e os riscos da segurança da informação da organização.

2.5. Classificação da informação

O HORTOPREV deve assegurar que seus servidores e colaboradores respeitem os controles conforme a classificação da informação, através da implementação de ferramentas e formalização de processos conforme a classificação estabelecida. Por fim, o HORTOPREV deve orientar seus servidores e colaboradores quanto à inserção, classificação, rotulação, publicação, compartilhamento e manuseio de ativos, conforme consta na ISO 27.001 A.8.1 e A.8.2.

2.6. Controle de Acessos

O HORTOPREV deve controlar o acesso físico e lógico, às suas dependências e aos seus RTIs. Para isso, ela deve garantir que cada colaborador possua uma credencial de uso pessoal, intransferível e de conhecimento exclusivo. Os acessos físicos aos ambientes controlados e lógicos às informações e recursos computacionais devem ser autorizados pelos gestores ou diretoria.

2.7. Análise dos Recursos de Tecnologia da Informação (RTIs)

O HORTOPREV deve analisar, periodicamente, seus processos e RTIs, assegurando que estes estejam documentados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

a. Ambientes Lógicos:
Deve ser assegurado que os ambientes de sistemas e processos que suportam os RTIs sejam confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.

b. Ambientes Físicos:
O HORTOPREV deve possuir o controle de acesso nos perímetros de segurança delimitados para garantir a proteção das áreas, bem como controles e registros apropriados para assegurar o acesso somente aos colaboradores autorizados e aos RTIs homologados.

2.8. Monitoramento

O HORTOPREV deve comunicar os seus colaboradores sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, seus RTIs, além de seus ambientes, físicos e lógicos, para verificação dos controles implantados, proteção de seu patrimônio e reputação, rastreando eventos críticos e evidenciando possíveis incidentes.

O Correio Eletrônico e o acesso à Internet são recursos corporativos, instalados e mantidos para o atendimento dos objetivos de negócios do HORTOPREV. Os acessos e históricos são gravados, podendo ser monitorados, portanto, não há expectativas de privacidade em sua utilização.

2.9. Tratamento de Incidentes de Segurança da Informação

Deve ser feito um acompanhamento e a análise da vulnerabilidade dos incidentes de Segurança da Informação mencionados nesta política.

2.10. Continuidade do Negócio e Contingência dos RTIs

Para mitigar os riscos de interrupção causados por incidentes de segurança e manter os níveis de serviços de TI adequados no HORTOPREV, são elaboradas ações de prevenção e recuperação, sempre alinhando a Política de Segurança da Informação.

2.11. Conformidade

Este documento deve passar por um programa de revisão e atualização periódico, para garantir que todos os pontos aqui mencionados estejam implementados e sendo cumpridos dentro da empresa. Auditoria Interna incluirá em seu planejamento de trabalho anual as revisões dos controles internos descritos na Política de Segurança da Informação.

3. DIRETRIZES

3.1. Divulgação da Política

O HORTOPREV deve garantir que esta política e suas normas complementares sejam divulgadas aos membros da empresa, além de mantê-la num local de fácil acesso a todos que se relacionam com a empresa.

Deve ser esclarecido que é responsabilidade de cada colaborador a consulta esporádica e voluntária para identificar possíveis atualizações dos documentos.

3.2. Autorização de uso

Esta política e suas normas complementares devem ser interpretadas de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, no qual os usuários têm acesso somente aos recursos de informação necessários para o pleno desempenho de suas atividades.

Tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade da solicitação.

3.3. Manuseio das informações

As informações do HORTOPREV, dos segurados, dos fornecedores e do público em geral, geradas, acessadas, manuseadas, armazenadas ou descartadas por um colaborador, bem como os Recursos de Tecnologia da Informação (RTI) disponibilizados, são de propriedade e direito de uso exclusivo do HORTOPREV. Estas devem ser empregadas unicamente para fins profissionais – limitado às atribuições de cargo e/ou função desempenhadas pelo servidor e/ou colaborador – que deve cumpri-las dentro do padrão de conduta ética estabelecida e alinhado à sua obrigação legal de sigilo profissional.

3.4. Gestão da informação

A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada. A gestão da informação deve ser assegurada por meio de medidas que proporcionem acesso e divulgação devidamente autorizados e de acordo com a legislação vigente.

3.5. Controle de Acesso

O HORTOPREV deve controlar o acesso físico e lógico às suas dependências e aos seus RTI. Desse modo, a empresa deve garantir que cada colaborador possua uma credencial de uso individual, intransferível, de conhecimento exclusivo e qualificando-o como responsável pelas ações realizadas. O HORTOPREV deve ainda orientar seus colaboradores sobre a responsabilidade quanto ao uso e sigilo além de coibir o compartilhamento de credenciais (Crachás, Login e Senha), sob qualquer hipótese.

3.6. Monitoramento

Os RTIs fornecidos pelo HORTOPREV podem ser utilizados para atualização de seus colaboradores, bem como estimular a cooperação entre eles. Desse modo, qualquer uso de RTI que permita maior mobilidade, bem como a participação em ambientes de relacionamento, como Redes Sociais, devem estar diretamente relacionados a uma

justificativa do negócio, com motivo estritamente de trabalho, dentro das atribuições do colaborador. Qualquer dano causado, por ação ou omissão, resultante de sua postura e/ou comportamento, pode resultar em processo administrativo disciplinar mediante apuração de responsabilidade.

3.7. Termos/Contratos

O contrato com os colaboradores, funcionários, estagiários e prestadores de serviços deve respeitar os termos e condições desta Política de Segurança da Informação. Junto ao contrato, um Termo de Confidencialidade, Responsabilidade e Sigilo deverá ser acordado, relacionado com o escopo de sua contratação e também sanções administrativas ou pecuniárias em caso de sua violação. O HORTOPREV deve prover auditorias periódicas que visam certificar o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

3.8. Violação

As ocorrências que podem ser consideradas violações desta Política de Segurança da Informação devem ser avaliadas pela área de Segurança da Informação do HORTOPREV. Se caso constatado como um incidente, deve ser encaminhado para um Comitê de decisão para avaliar as medidas a serem tomadas.

3.9. Fale Conosco

Se após a leitura desta Política de Privacidade, ainda houver qualquer dúvida, ou por qualquer razão for necessário se comunicar com o instituto, para assuntos envolvendo os seus dados pessoais, pode-se entrar em contato pelo e-mail abaixo:

Encarregado (DPO): E-mail: **controladoria@hortoprev.hortolandia.sp.gov.br**.

O HORTOPREV está sempre à disposição para esclarecer dúvidas e colocar o segurado no controle dos seus dados pessoais.