POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CASA DA ESPERANÇA DE SANTOS®

CES®
CASA DA ESPERANÇA DE SANTOS

Sumário

MATRIZ DE RESPONSABILIDADE

ATIVIDADES	AGENTES DE PROCESSO		
R = RESPONSÁVEL; A= AUTORIDADE; C= CONSULTADO; I = INFORMADO			
	Direção	Analista de TI	Colaborador
Aprovar e Apoiar a Divulgação da Política de Segurança da Informação	A / R	A / C / I	I
Publicar a Política da Segurança da Informação	I	A / R	I
Seguir às diretrizes estabelecidas neste documento	R	R	R

1. OBJETIVO

Estabelecer as diretrizes para garantir a Segurança da Informação (SI) da **Casa da Esperança de Santos®**, conforme escopo definido.

A Política de Segurança da Informação (PSI) busca continuamente adoção de ações destinadas a preservar os princípios básicos da segurança aplicados à informação, sendo estes:

- **Confidencialidade:** Garantir que os dados e os sistemas somente sejam acessados por pessoas devidamente autorizadas.
- **Integridade:** Garantir a exatidão da informação e dos sistemas contra alteração, perda ou destruição, seja de forma acidental ou fraudulenta.
- **Disponibilidade:** Garantir que a informação e os sistemas possam ser utilizados na forma e tempo requeridos.

Todos os colaboradores da **Casa da Esperança de Santos®** devem zelar pela segurança das informações sejam elas internas, de clientes ou de parceiros, seguindo as boas práticas de Segurança da Informação.

2. ABRANGÊNCIA

Esta política abrange todas as informações utilizadas na **Casa da Esperança de Santos®** para realização de suas atividades, e recursos envolvidos.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1 Segurança para a Informação

A informação é um ativo valioso para empresa e salvaguarda a confidencialidade, integridade e disponibilidade da informação é essencial para preservar a continuidade dos negócios, para minimizar os danos e maximizar o retorno dos investimentos e as oportunidades de negócio.

O ciclo de vida da informação é definido pelo processo de criação, classificação, armazenamento, acesso, transmissão, transporte, reclassificação e descarte.

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *hardware* e *software*. A informação pode existir sob várias formas:

- Impressa ou escrita em papel;
- Armazenada eletronicamente (por exemplo: computadores, *tablets*, celulares, HDs, CDs, DVDs);
- Transmitida pelo correio ou por meios eletrônicos;
- Verbal (falada).

A informação deve ser adequadamente protegida, independente da forma ou meios pelas quais ela é armazenada ou compartilhada.

Tomando os devidos cuidados com a informação, podemos evitar incidentes como vazamentos de conteúdo, alterações indevidas de dados e fraudes.

A **CASA DA ESPERANÇA DE SANTOS®** pode a qualquer momento monitorar seus ativos de informação, inclusive o acesso à Internet, Correio Eletrônico, Computadores e outros equipamentos.

3.2 Por que a SI é necessária?

Confidencialidade, integridade e disponibilidade da informação são essenciais para preservar o ambiente, dentre outros benefícios, visa aumentar a competitividade, a qualidade, a lucratividade, o atendimento dos requisitos legais e a imagem da **CASA DA ESPERANÇA DE SANTOS®** perante o mercado.

3.3 Boas Práticas de SI

Segue abaixo exemplos de boas práticas que devem ser seguidos por todos os colaboradores:

- As informações confidenciais não devem ser discutidas ao telefone, em elevadores, corredores, escadas e em lugares públicos;
- Nunca divulgue informações pessoais ou profissionais de colaboradores para pessoas de fora da organização;
- Arquive documentos e informações confidenciais em local seguro e com o devido controle de acesso;
- Ao repassar informações certifique-se que a pessoa esteja autorizada a recebê-las e informe somente o necessário;
- Nunca jogue documentos com informações confidenciais no lixo sem antes destruí-los;
- Não reproduza nenhum documento ou informação confidencial sem o consentimento de seu superior;
- Verifique a autenticidade e legibilidade de todos os destinatários ao enviar uma informação, seja por correio, correio eletrônico ou qualquer outro meio.
- Armazene seus arquivos de trabalho na rede da **CASA DA ESPERANÇA DE SANTOS®**, garantindo assim a integridade dos documentos mesmo em caso de panes em seu equipamento;

3.4 Objetivo da Segurança da Informação

O objetivo da Segurança da Informação (SI) é preservar a confidencialidade, integridade e disponibilidade da informação, por meio dos controles de segurança adequados para proteção dos ativos da **CASA DA ESPERANÇA DE SANTOS®**.

A Política de Segurança da Informação (PSI) aplica-se a todas as pessoas, processos, tecnologias e ambientes físicos.

3.5 Política de Segurança da Informação

Para que os objetivos de Segurança da Informação (SI) sejam alcançados, as seguintes diretrizes devem ser seguidas e consideradas em todas as atividades realizadas:

- Todas as atividades inerentes à Segurança da Informação (SI) devem estar em conformidade com a Política de Segurança da Informação (PSI);

- Todos os recursos e informações devem ser protegidos nos quesitos: confidencialidade, integridade e disponibilidade;
- Análises de riscos devem ser realizadas sempre que necessário ou de acordo com a periodicidade estabelecida na metodologia determinada;
- Devem ser atendidos todos os requisitos legais, regulamentares e contratuais aplicáveis ao negócio;
- Todos os colaboradores e envolvidos nas atividades sob controle da empresa, de acordo com o escopo, devem estar cientes da Política de Segurança da Informação (PSI), receber treinamentos e conscientização em Segurança da Informação (SI) periodicamente, sendo no momento da contratação e/ou anualmente;
- Incidentes de Segurança da Informação (SI) devem ser reportados imediatamente ao setor de TII.

Um procedimento disciplinar formal deve ser estabelecido, em caso de violação desta Política de Segurança da Informação (PSI) e em casos de descumprimento das normativas e processos relativos à Segurança da Informação (SI). Caberá a Diretoria de Recursos Humanos em conjunto com a Gestão da **CASA DA ESPERANÇA DE SANTOS®** definir quais as sanções disciplinares deverão ser aplicadas.

3.6 Propriedade da Informação

Toda informação produzida na **CASA DA ESPERANÇA DE SANTOS®** é considerada de sua propriedade, não importando a data de sua criação ou sua forma de representação e transporte. Exceções devem ser comunicadas pelo colaborador no momento da sua contratação, estas exceções devem ser formalmente aceitas pela Alta Direção.

3.7 Responsabilidades

Todos os colaboradores envolvidos com o escopo apresentado neste documento, são responsáveis pelo cumprimento de suas responsabilidades para atendimento dos princípios de Segurança da Informação (SI). As responsabilidades quanto ao cumprimento das ações documentadas, estão declaradas da Matriz de Responsabilidades, localizada no início de todo documento.

3.8 Acordo de Confidencialidade e Aceitação da Política de Segurança da Informação

Todos os colaboradores da **CASA DA ESPERANÇA DE SANTOS®**, no início das atividades, deverão ser treinados, orientados e estar de acordo com esta Política de Segurança da Informação (PSI).

O cumprimento da Política de Segurança da Informação (PSI) e a preservação da confidencialidade das informações e de dados sensíveis da empresa é um dever de todos. É vetada a reprodução de quaisquer documentos, dados ou informações da empresa, sem o expresso consentimento desta, através de autorização de representante com poderes para tanto.

3.9 Comunicação da Política de Segurança da Informação

A comunicação e ciência dos colaboradores da CASA DA ESPERANÇA DE SANTOS® a respeito do cumprimento e disponibilidade da Política de Segurança da Informação (PSI), são realizadas também por meio dos treinamentos e atividades de conscientização.

3.10 Consequências das Violações da Política de Segurança da Informação

Em caso de não cumprimento total ou parcial desta Política de Segurança da Informação (PSI) por parte de colaborador da **CASA DA ESPERANÇA DE SANTOS®** o caso deverá ser levado pelo gestor à Diretoria.

Dentre as medidas disciplinares que poderão ser aplicadas, estão: Advertência verbal, advertência escrita, suspensão e em casos mais graves até mesmo o desligamento do colaborador. A definição da medida disciplinar será com base na gravidade do ato praticado e/ou impacto dele nas atividades da área ou organização. O objetivo do procedimento de medida disciplinar é orientar e corrigir a conduta do colaborador, justificando-se assim, a eventual.

4. USO DE EQUIPAMENTOS PARA O TRABALHO REMOTO

4.1 Diretrizes Gerais

O acesso remoto ao ambiente computacional da **CASA DA ESPERANÇA DE SANTOS®** deve ser feito somente por colaboradores autorizados e por equipamentos disponibilizados pela C**ASA DA ESPERANÇA DE SANTOS®** que atendam aos padrões normativos de segurança.

- Equipamentos portáteis não podem ser deixados desprotegidos em áreas públicas e não devem ser utilizados em área de circulação de pessoas, tal como aeroportos, *hall* de hotéis, restaurantes e bares.

4. 2 Liberação Para Trabalho Remoto

O trabalho remoto deve ser autorizado, justificado e aprovado pela Gerência imediata e deve seguir os padrões de acesso remoto, de acordo com as diretrizes:

- Os equipamentos utilizados no trabalho remoto devem ser acessíveis apenas ao usuário da

empresa, utilizando mecanismos de travamento de tela controlados por senha ou por outro mecanismo de autenticação similar;
- Manter os controles praticados na empresa no tratamento de informações.

5. PROTEÇÃO CONTRA SOFTWARE MALICIOSO

Todos os equipamentos de processamento da informação que têm a capacidade de armazenar dados, estabelecer conexões externas e interagir com outros sistemas e redes devem possuir *softwares* de proteção contra *software* malicioso instalado.

- O software de antivírus instalado nos equipamentos deve ser homologado pela **CASA DA ESPERANÇA DE SANTOS®**;
- O *software* de antivírus deve ser mantido ativo e atualizado;
- Os *links* recebidos pelo usuário devem ser verificados antes de serem acessados, a fim de reduzir os riscos de infecção por códigos executáveis maliciosos.

6. DIRETIVA DE SEGURANÇA PARA USO DA INTERNET

O uso de conexões aos sistemas de Internet é permitido para atender apenas propósitos de operação da **CASA DA ESPERANÇA DE SANTOS®**, tendo a empresa o direito, a qualquer momento, de:

- Suspender o acesso do colaborador;
- Restringir o *download* e *upload* de arquivos ou acesso a conteúdo que não sejam de interesse da empresa;
- Monitorar os acessos;
- Tomar medidas disciplinares ou judiciais (em caso de violações, se aplicável);
- Tomar cuidado ao compartilhar informações pessoais, da **CASA DA ESPERANÇA DE SANTOS®** ou de clientes via Internet;
- Utilizar sempre que possível o duplo fator de autenticação em sites internos e externos.

É expressamente vetado o uso não justificado dos recursos da **CASA DA ESPERANÇA DE SANTOS®** para:

- Acessar ou veicular conteúdo relacionado à pedofilia;
- Veicular conteúdos de cunho: Político, Religioso, Jogos, Racial, Orientação Sexual, Terrorista, Pornográfico e Ilegal (pirataria de *software*, comércio de ilícitos etc.);
- Efetuar *downloads* de programas de entretenimento, ilegais ou jogos não são permitidos;

- Quaisquer outras atividades consideradas inapropriadas, indevidas ou desvinculadas às atividades desempenhadas na empresa;
- Publicar, postar, carregar, distribuir ou divulgar quaisquer tópicos, nomes, materiais ou informações que incentivem a discriminação, ódio ou violência com relação a uma pessoa ou a um grupo;
- Utilizar identificação falsa ou assumir, sem autorização, a identidade de outro usuário;
- Utilizar-se da Internet e outros serviços disponibilizados com o intuito de cometer fraude;
- Utilizar os serviços, para de qualquer modo reproduzir ou infringir direitos de terceiros, sejam imagens, áudio, fotografias, vídeos, *softwares* ou qualquer material protegido por lei de propriedade intelectual, incluindo, lei de direitos autorais, marcas ou patentes, a menos que o usuário tenha as licenças necessárias para fazê-lo, ou seja, o titular de tais direitos;
- Praticar atos ilícitos, tais como: atividades *hackers, crackers,* bombas, falsidade ideológica, entre outros sem a devida autorização.

Somente usuários, dispositivos e equipamentos homologados, autorizados e que atendam aos requisitos de segurança devem possuir acesso à Rede da **CASA DA ESPERANÇA DE SANTOS®**.

Toda conexão com rede externa deve ser analisada e expressamente autorizada pela área de Tecnologia da Informação da **CASA DA ESPERANÇA DE SANTOS®**. As conexões com redes externas devem ser obrigatoriamente protegidas por um *firewall*.

7.USO DE CORREIO ELETRÔNICO (E-mail)

O sistema de correio eletrônico deverá ser utilizado somente para a troca de mensagens que atendam os propósitos de negócio da organização sendo legítimo à empresa:

- Suspender o serviço de um ou vários usuários;
- Não fornecer o serviço àqueles que não sejam de interesse da empresa;
- Monitorar destinatários, inspecionar conteúdo e registrar o tipo de uso dos e-mails manipulados pelos usuários;
- Solicitar dos usuários justificativas por uso indevido do recurso;
- Monitorar e bloquear tráfego de informações que não estejam em conformidade com a normativa de Classificação da Informação da **CASA DA ESPERANÇA DE SANTOS®**;

Adicionalmente, medidas devem ser tomadas quanto ao uso do correio eletrônico, sendo estas:

- Todo *e-mail* com endereço corporativo da **CASA DA ESPERANÇA DE SANTOS®** deve ser configurado de acordo com os padrões de identificação e segurança vigentes e homologados pela empresa;
- Toda caixa postal, independentemente da plataforma tecnológica, deverá ser acessada através da devida autenticação e autorização no ambiente de Rede Corporativa;
- A utilização do serviço de correio eletrônico deve ser sempre por meio de equipamentos que estejam em conformidade com as normativas de Segurança da Informação da C**ASA DA ESPERANÇA DE SANTOS®**;

- A utilização de serviços de correio eletrônico da **CASA DA ESPERANÇA DE SANTOS®**, através do acesso à internet, somente deve ser feito a partir de equipamentos que estejam em conformidade com a Política de Segurança da Informação (PSI);
- Cada usuário será responsável pela manutenção e uso consciente de suas contas de *e-mails*;
- Atentar-se na seleção correta dos destinatários;
- Caso tenha que adicionar um novo destinatário, avalie a pertinência do conteúdo presente no histórico do *e-mail;*
- Não repasse mensagens como correntes, divulgação de produtos ou qualquer outra que não agregue valor ao negócio;
- Não abra mensagens de remetentes desconhecidos e com arquivos anexos cujo envio não seja de seu conhecimento;
- Não permita acesso de terceiros ao correio eletrônico através de sua senha.

8. GESTÃO DE ACESSO LÓGICO DOS USUÁRIOS

Os acessos devem ser concedidos aos usuários com base no princípio do mínimo privilégio, garantindo que somente o acesso necessário para o exercício de sua função.

Toda solicitação e revogação de acesso aos recursos de sistema e rede da **CASA DA ESPERANÇA DE SANTOS®**, independentemente do nível de criticidade, deve ser devidamente documentada e não deve ser executada antes de passar pelo fluxo de aprovação.

O processo formal de solicitação e revogação de acesso aos recursos de sistema e rede da **CASA DA ESPERANÇA DE SANTOS®** devem ser realizados por meio de abertura de chamado para o setor de TI.

8.1 Uso de Credenciais de acesso (Login nas Máquinas)

Cada usuário terá sua própria credencial de acesso, não sendo permitido seu compartilhamento. O proprietário da credencial de acesso é responsável pelas atividades realizadas através da sua senha de acesso, por este motivo o usuário deve tomar todas as precauções necessárias para cuidar da sua credencial de acesso e protegê-la contra acesso não autorizado.

Todas as credenciais de acesso devem ter senhas fortes, de difícil dedução (complexidade e tamanho mínimo).

9. REQUISITOS DE SEGURANÇA NO USO DE SENHAS

- As senhas de acesso aos recursos tecnológicos utilizados na CASA DA ESPERANÇA DE SANTOS® são pessoais e intransferíveis. Sempre manter senhas, que não forem passíveis de memorização, armazenadas em meios seguros;
- Nunca utilize como senha nomes de familiares, datas comemorativas (aniversários) ou outras palavras de fácil associação a sua pessoa ou atividade;
- Não deixe lembretes de senhas anotados, em arquivos ou outros.

Devem ser adotados os parâmetros de configuração de senhas a seguir:

- Devem conter no mínimo 8 caracteres;
- Combinação de caracteres maiúsculos, minúsculos, numéricos e especiais;
- Evite repetição sequencial (por exemplo: abc,12345678, etc.);
- Não utilize informações que possam ser descobertas facilmente (por exemplo: seu nome, data de nascimento, número de documentos etc.).

10. PROTEÇÃO DE EQUIPAMENTO DE USUÁRIO SEM MONITORAÇÃO

Os equipamentos desassistidos devem possuir sistema de proteção de tela protegido por senha, bloqueando o uso do equipamento e somente deve ser desbloqueado com a inserção da senha pelo responsável pelo uso do equipamento em questão.

Se o equipamento for permanecer sem uso por períodos longos, deverá ser realizado o *logoff* do usuário. No encerramento do expediente e das atividades do usuário, o equipamento deverá ser desligado.

11. POLÍTICA DE MESA LIMPA E TELA LIMPA

Todos os colaboradores são responsáveis por manterem de forma segura suas credenciais, equipamentos e informações manuseadas, seja em formato eletrônico ou físico, sendo de responsabilidade do colaborador seguir as diretrizes abaixo:

11.1 Tela Limpa

- Mantenha a proteção de tela ativa com senha sempre quando estiver fora da sua área de trabalho e desligue-o de forma adequada ao término da jornada;
- Evite visualizar informações sensíveis em locais públicos e/ou de grande movimentação, observe o ambiente ao seu redor.

11. 2 Mesa Limpa

- Documentos não devem ficar sobre a mesa ou outro mobiliário, especialmente ·quando o escritório estiver desocupado.

12. REPORTAR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

É responsabilidade de todo colaborador reportar incidentes de segurança ou suspeitas através do Setor de Tecnologia da Informação.

As fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços de informação da organização devem ser reportadas da mesma forma e pelo mesmo meio dos incidentes de segurança da informação.

13. POLÍTICA DE PRIVACIDADE DE DADOS

13.1 Privacidade de Dados Pessoais

A **CASA DA ESPERANÇA DE SANTOS®** deve respeitar as disposições vigentes na Legislação Brasileira e demais legislações aplicáveis sobre a proteção de dados pessoais. A coleta de informações que não tenham relação com seus processos de negócio e atividades de trabalho é proibida.

Entende-se como dados pessoais, qualquer informação referente a pessoas identificadas ou identificáveis que a **CASA DA ESPERANÇA DE SANTOS®** obtenha de seus clientes, fornecedores e colaboradores, tais como: Nome completo, CPF, endereço e demais dados que identifique a pessoa.

A política de privacidade da **CASA DA ESPERANÇA DE SANTOS®** também está publicada no site oficial da organização.

13.2 Tratamento de Dados Pessoais

A obtenção e tratamento de dados pessoais deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular.

Devem ser utilizadas medidas de proteção dos dados pessoais, proporcionais à natureza das informações tratadas a fim de evitar acessos não autorizados e de situações acidentais ou ilícitas.

Quando da verificação de que a finalidade foi alcançada ou de que os dados pessoais deixaram de ser necessários, os dados devem ser descartados e deverá ser empregados métodos de descarte adequados.

13.3 Compartilhamento de Dados Pessoais

Todas as pessoas ou empresas que obtiverem acesso aos dados pessoais mantidos ou transmitidos pela **CASA DA ESPERANÇA DE SANTOS®** devem seguir os requisitos de Segurança da Informação estabelecidos neste documento.

Os registros relevantes devem ser protegidos de perda, destruição e falsificação, de acordo com requisitos estatutários, regulatórios, contratuais e requisitos de negócio.

13.4 Uso de Recursos de Processamento da Informação

Se qualquer atividade não autorizada for identificada por processo de monitoração ou outros meios deverá ser levada ao conhecimento do gestor responsável para que sejam aplicadas as devidas ações disciplinares e/ou legais pertinentes.

14. USO DE DISPOSITIVOS MÓVEIS PESSOAIS

O conceito de "Traga seu próprio dispositivo" (comumente chamado de TSPD), pode fornecer maior flexibilidade e eliminar a necessidade de o funcionário levar mais de um dispositivo regularmente.

No entanto, o conceito de permitir que um funcionário use seu(s) próprio(s) dispositivo(s) para fins comerciais pode resultar na necessidade de tais dispositivos estarem sujeitos a controles adicionais.

Problemas comuns e desafios de segurança com TSPD:

- Uso do dispositivo por outros membros da família;
- Armazenamento padrão de dados e instalações de backup em nuvem;
- Aumento da exposição a potenciais perdas em ambientes sociais, p. na praia, em um bar;
- Acesso potencial a sites que não atendem à política de uso aceitável das organizações;
- Conexão a redes inseguras, por ex. pontos de acesso sem fio inseguros;
- Proteção antivírus e com que frequência o dispositivo é corrigido;
- Instalação de aplicativos potencialmente mal-intencionados no dispositivo (geralmente sem que o usuário saiba que é malicioso).

Essas questões devem ser consideradas ao avaliar a adequação de qualquer dispositivo como apto para conter dados específicos pertencentes à organização.

É uma decisão conjunta entre a organização e o proprietário do dispositivo. Esse uso não é obrigatório, e o funcionário tem o direito de decidir se os controles adicionais colocados no dispositivo pela organização são aceitáveis e se eles optam por usar o dispositivo para fins comerciais.

É importante que os controles definidos nesta política sejam observados em todos os momentos, no uso e no transporte de dispositivos móveis TSPD.

Os indivíduos não devem usar seus próprios dispositivos para manter e processar informações da empresa, a menos que tenham enviado uma solicitação para fazê-lo, e essa solicitação tenha sido formalmente aprovada. É política da **CASA DA ESPERANÇA DE SANTOS®** avaliar cada solicitação TSPD para estabelecer:

- A identidade da pessoa que faz a solicitação;
- O motivo comercial da solicitação;
- Os dados que serão mantidos ou tratados no dispositivo;
- O dispositivo específico que será usado.

As solicitações devem ser enviadas para o Setor de Tecnologia da Informação e Inovação.
O princípio geral desta política é que o grau de controle exercido pela organização sobre o dispositivo TSPD seja apropriado para a sensibilidade dos dados contidos nela.

Para garantir que seus dados sejam protegidos adequadamente, é importante que a **CASA DA ESPERANÇA DE SANTOS®** possa monitorar e auditar o nível de conformidade com essa política. O nível de monitoramento e auditoria será deve ser apropriado para cada informação armazenada no dispositivo.

Os métodos e o tempo de monitoramento e auditoria deverão respeitar a privacidade do proprietário do dispositivo, em conformidade com a legislação aplicável. Em geral, o monitoramento do uso fora do horário comercial será evitado.

No caso de perda ou roubo do dispositivo, o proprietário deve informar o Setor de Tecnologia da Informação e Inovação o mais rápido possível, fornecendo detalhes sobre as circunstâncias da perda e a sensibilidade das informações comerciais armazenadas nele. **A CASA DA ESPERANÇA DE SANTOS®** reserva o direito de apagar remotamente o dispositivo, sempre que possível, como medida de segurança. Isso pode envolver a exclusão de dados não comerciais pertencentes ao proprietário do dispositivo.

Ao sair da organização, o proprietário do dispositivo deve permitir que o dispositivo seja auditado e todos os dados e aplicativos relacionados ao negócio sejam removidos.

CES®

CASA DA ESPERANÇA DE SANTOS

R. Imperatriz Leopoldina, 15
Ponta da Praia • Santos
13 3278.7800

@casadaesperancadesantos
@CasaEsperancaSt
YouTube Casa da Esperança de Santos