

***Política de Segurança da Informação***

CREFITO 11

CONSELHO REGIONAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL DA 11° REGIÃO

**Sumário**

[**1 - Sobre a Política de Segurança da Informação (PSI)** 4](#_Toc168684157)

[**2 - Conceitos e Definições** 4](#_Toc168684158)

[**3 - Objetivos da Política de Segurança da Informação** 7](#_Toc168684159)

[**4 - Aplicação da Política de Segurança da Informação** 9](#_Toc168684160)

[**5 - Princípios da Política de Segurança da Informação** 9](#_Toc168684161)

[**6 - Requisitos da Política de Segurança da Informação** 10](#_Toc168684162)

[**7 - Monitoramento e Auditoria** 10](#_Toc168684163)

[**8 - Responsabilidades Específicas Dos Usuários em geral** 12](#_Toc168684164)

[**9 - Política de Senhas** 13](#_Toc168684165)

[**10 - Acesso à rede** 14](#_Toc168684166)

[**11 - Segmentação de ambiente, Publicações internas e externas** 15](#_Toc168684167)

[**12 - Dos Gestores/Gerentes** 16](#_Toc168684168)

[**13 - Back-up** 17](#_Toc168684169)

[**14 - Gestão de mudanças** 17](#_Toc168684170)

[**15 - Do Comitê Consultivo** 18](#_Toc168684171)

[**16 - Da Inovação e Uso de Novas Tecnologias** 18](#_Toc168684172)

[**17 - Da Proteção à propriedade intelectual** 19](#_Toc168684173)

[**18 – Considerações Finais** 21](#_Toc168684174)

[**19 - Referencias** 21](#_Toc168684175)

# **1 - Sobre a Política de Segurança da Informação (PSI)**

A politica de segurança da informação é um elemento essencial para todos os processos de negócio de qualquer organização, por tanto, é o ativo mais valioso da organização, e deve ser protegido e cuidado, esse cuidado se dá por meio de regras, normas, procedimentos e políticas, essas informações podem ser alvo de uma série de ameaças com a finalidade de explorar as vulnerabilidades e causar prejuízos consideráveis.

O CREFITO 11 é uma instituição onde se circula um grande número de informações sensíveis, sejam de cunho pessoal ou de servidores, ou até movimentações financeiras internas e externas, faz necessário implementar uma Política de Segurança da Informação de modo a reduzir as chances de perda de dados, fraudes ou invasões indevidas.

#

# **2 - Conceitos e Definições**

Ativo: Todo e qualquer bem do ambiente de TI que tem valor para a organização e precisa ser protegido. Exemplos incluem hardware, software, dados e redes.

Ativo Crítico e Sensível: Ativo cuja perda, comprometimento ou indisponibilidade pode causar grande impacto nas operações da organização, incluindo prejuízos financeiros, reputacionais ou de conformidade legal.

Cavalo de Troia (Trojan horse): Tipo de malware que se disfarça como software legítimo ou inofensivo, mas ao ser executado, permite ao atacante obter controle sobre o sistema afetado.

Código Executável: Conjunto de instruções em linguagem de máquina que podem ser diretamente executadas pela CPU de um computador. Exemplos incluem arquivos com extensões como .exe, .dll, .com.

Código Malicioso: Qualquer tipo de código desenvolvido com a intenção de causar danos, roubar informações ou comprometer a segurança de sistemas e dados. Exemplos incluem vírus, worms, trojans e ransomwares.

Colaborador Interno: Funcionário ou pessoa que trabalha diretamente para a organização, incluindo empregados permanentes e temporários.

Colaborador Externo: Pessoa ou entidade que presta serviços ou fornece bens para a organização, mas não é empregada diretamente por ela. Exemplos incluem consultores, fornecedores e contratados.

Confidencialidade: Propriedade que assegura que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.

Comunicadores Instantâneos: Ferramentas de comunicação digital que permitem troca de mensagens em tempo real entre os usuários. Exemplos incluem WhatsApp, Telegram e Microsoft Teams.

Custodiante: Entidade ou pessoa responsável pela proteção, manutenção e gerenciamento de dados ou ativos de informação em nome do proprietário desses ativos.

Cyberbullying: Ato de assediar, ameaçar ou humilhar uma pessoa por meio de tecnologias digitais, como redes sociais, e-mails, mensagens instantâneas, etc.

Dados Pessoais: Informações relacionadas a uma pessoa natural identificada ou identificável. Exemplos incluem nome, endereço, número de telefone e informações de identificação.

Dados Pessoais Sensíveis: Subconjunto de dados pessoais que requerem maior proteção devido ao seu potencial de causar discriminação ou prejuízo aos direitos e liberdades dos indivíduos. Exemplos incluem dados de saúde, orientação sexual, dados biométricos, e informações religiosas.

Disponibilidade: Propriedade que assegura que a informação e os recursos de TI estejam acessíveis e utilizáveis sob demanda por uma entidade autorizada.

Informação: Dados processados, organizados ou formatados de maneira a terem significado e valor para quem os utiliza.

Informação Sensível: Informações que, se divulgadas sem autorização, podem causar prejuízos à organização ou a indivíduos. Inclui dados pessoais sensíveis, segredos comerciais, e informações confidenciais de negócios.

Integridade: Propriedade que assegura que a informação é precisa e completa, e que não foi alterada de maneira não autorizada.

Parceiros: Entidades ou indivíduos que colaboram com a organização para atingir objetivos comuns, incluindo alianças estratégicas, joint ventures e outros tipos de colaborações.

Peer to Peer: Modelo de rede de computadores onde cada participante (peer) tem capacidades e responsabilidades equivalentes, compartilhando recursos diretamente uns com os outros sem a necessidade de um servidor central.

Segurança da Informação: Conjunto de práticas e políticas destinadas a proteger a informação e os sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição.

Spam: Mensagens eletrônicas não solicitadas e geralmente em massa, muitas vezes de natureza comercial, enviadas sem o consentimento dos destinatários.

Usuário: Pessoa que utiliza um sistema de informação, seja ele um sistema operacional, aplicativo, rede ou banco de dados.

Vírus: Tipo de código malicioso que, quando executado, se replica inserindo cópias de si mesmo em outros programas ou arquivos, geralmente causando danos ao sistema ou corrompendo dados.

Worm: Tipo de malware que se replica automaticamente de um computador para outro, explorando vulnerabilidades de rede sem a necessidade de interação humana, frequentemente causando sobrecarga de rede e outros danos.

# **3 - Objetivos da Política de Segurança da Informação**

Estabelecer diretrizes: Definir normas e procedimentos claros para a proteção dos ativos de informação da organização. Essas diretrizes servem como base para todas as ações relacionadas à segurança da informação, garantindo uma abordagem consistente e sistemática.

Nortear: Fornecer orientação para a tomada de decisões e a execução de ações de segurança da informação. A política serve como um guia para os colaboradores, ajudando-os a entender suas responsabilidades e a agir de acordo com as melhores práticas e padrões estabelecidos.

Prevenir: Implementar medidas proativas para evitar incidentes de segurança da informação, como vazamentos de dados, ataques cibernéticos e acessos não autorizados. A prevenção é fundamental para manter a integridade, confidencialidade e disponibilidade das informações.

Garantir a normalidade e a continuidade: Assegurar que as operações da organização possam continuar de forma ininterrupta, mesmo em caso de incidentes de segurança. Planos de contingência e recuperação de desastres são essenciais para manter a continuidade dos negócios.

Atender aos requisitos legais, regulamentares e contratuais: Cumprir todas as leis, regulamentações e acordos contratuais pertinentes à segurança da informação. Isso inclui proteger dados pessoais e confidenciais conforme as legislações vigentes e garantir que a organização esteja em conformidade com normas setoriais.

Minimizar os riscos de danos, perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades: Reduzir a probabilidade e o impacto de incidentes de segurança que possam prejudicar a organização. A gestão de riscos é crucial para proteger os ativos e a reputação da empresa.

Assegurar o treinamento contínuo: Promover a educação e a conscientização dos colaboradores sobre a importância da segurança da informação e as melhores práticas a serem seguidas. O treinamento contínuo é vital para que todos estejam preparados para identificar e responder a ameaças de segurança.

Garantir que todas as responsabilidades da Segurança da Informação sejam claramente definidas e preservadas: Estabelecer e comunicar claramente as responsabilidades de cada membro da organização em relação à segurança da informação. Isso inclui a designação de funções específicas e a garantia de que todos entendam e cumpram suas obrigações para proteger os ativos de informação.

# **4 - Aplicação da Política de Segurança da Informação**

As diretrizes estabelecidas nesta Política de Segurança da Informação (PSI) devem ser rigorosamente seguidas por todos os funcionários, prestadores de serviços, estagiários e demais colaboradores. Seu objetivo é proteger as informações e garantir o uso seguro dos recursos tecnológicos da organização.

Cada usuário é responsável por manter-se informado e atualizado sobre esta política e suas normas associadas. Em caso de dúvidas sobre a aquisição ou descarte de informações, é essencial que busquem orientação junto ao gestor ou à Gerência de Tecnologia da Informação (GTI). O comprometimento de todos é fundamental para assegurar a eficácia da segurança da informação na organização.

# **5 - Princípios da Política de Segurança da Informação**

Assegurar que a Política de Segurança da Informação do CREFITO 11 seja amplamente conhecida e plenamente compreendida por todos os colaboradores. É essencial conscientizá-los sobre os riscos e responsabilidades associados à segurança da informação, bem como instruí-los sobre as medidas a serem adotadas em caso de incidentes. Esse entendimento é crucial para alcançar a máxima proteção dos dados e assegurar a integridade das operações organizacionais.

A Política de Segurança da Informação (PSI) é fundamentada em princípios essenciais que orientam a proteção dos ativos de informação da organização. Estes princípios são pilares que sustentam todas as práticas e ações de segurança, garantindo a integridade, confidencialidade e disponibilidade das informações.

# **6 - Requisitos da Política de Segurança da Informação**

A Política de Segurança da Informação deve ser divulgada a todos os colaboradores, prestadores de serviços, estagiários e demais envolvidos. O objetivo é garantir a eficácia e promover uma cultura sólida de uso ético e legal dos recursos tecnológicos, além de assegurar a proteção da informação da EMPRESA.

# **7 - Monitoramento e Auditoria**

Para garantir a conformidade com as regras estabelecidas nesta Política de Segurança da Informação (PSI) e para fins de segurança e prevenção à fraude, A EMPRESA reserva-se o direito de:

**Monitoramento Contínuo:**

-Realizar o monitoramento contínuo do uso dos sistemas e redes de TI da organização.

-Verificar o acesso e o uso de informações sensíveis para identificar atividades suspeitas ou não autorizadas.

**Auditorias Regulares:**

-Conduzir auditorias periódicas dos sistemas de informação e processos relacionados à segurança.

-Avaliar a eficácia das políticas e controles de segurança implementados.

**Revisão de Logs e Registros:**

-Analisar logs de acesso, uso de recursos e registros de atividades dos usuários.

-Identificar e investigar qualquer atividade que possa indicar uma violação de segurança ou uso indevido.

**Inspeções de Conformidade:**

-Realizar inspeções para garantir que todas as práticas e procedimentos estejam em conformidade com a PSI e os requisitos legais.

-Verificar a aderência às políticas de uso aceitável e outras diretrizes de segurança.

**Testes de Vulnerabilidade e Penetração:**

-Executar testes de vulnerabilidade e penetração regularmente para identificar e corrigir possíveis falhas de segurança.

-Assegurar que os sistemas estejam protegidos contra ameaças externas e internas.

**Avaliação de Riscos:**

-Realizar avaliações de riscos contínuas para identificar novas ameaças e ajustar as medidas de segurança conforme necessário.

-Priorizar recursos e esforços para mitigar riscos significativos.

**Investigação de Incidentes:**

-Investigar todos os incidentes de segurança relatados para determinar a causa e a extensão da violação.

-Tomar ações corretivas para prevenir recorrências futuras.

# **8 - Responsabilidades Específicas Dos Usuários em geral**

Funcionários, prestadores de serviços, estagiários e afins da empresa CREFITO 11, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvam a instituição.

É de inteira responsabilidade do usuário qualquer prejuízo ou dano sofrido ou causado A EMPRESA e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

As normas e procedimentos que complementam está Política de Segurança da Informação, abordam os seguintes aspectos: segurança física e logica:

Cabe a todos os usuários as seguintes práticas:

-Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento;

-Buscar orientação do superior quando houver dúvidas relacionadas à Segurança da Informação;

-Segurança Física;

-Política de Senhas;

-Acesso à Rede;

-Estação de Trabalho;

-Equipamentos Particulares e Dispositivos Móveis;

-Home Office/Teletrabalho;

-E-mail Corporativo;

-Gestão de Contas de Usuários;

-Back-up;

-Gestão de Mudanças;

-Privacidade;

-Gestão de Incidentes;

-Criptografia;

# **9 - Política de Senhas**

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do servidor, evitando que uma pessoa, se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade). Com o objetivo de orientar a criação de senhas seguras, ficam estabelecidas as seguintes regras:

I. A senha é de total responsabilidade do servidor, sendo proibida a sua divulgação ou empréstimo, devendo a mesma, ser imediatamente alterada no caso de suspeita de uso indevido;

 II. A senha inicial será fornecida pela Gerencia de Redes e Monitoramento via e-mail institucional no ato da posse do servidor, solicitado pela Gestão de Pessoas – CREFITO 11, o servidor empossado será informado via correio eletrônico das credências e forma de acesso;

III. As credenciais não poderão ser fornecidas por telefone, comunicador instantâneo ou outra forma que não assegure a identidade do servidor;

IV. É obrigatório aos servidores, zelarem pela confidencialidade de sua senha de acesso, podendo ser responsabilizados pelas operações realizadas com a utilização de suas credenciais;

V. A equipe técnica do Crefito11 deverá possuir contas e senhas individualizadas com privilégios administrativos e somente deverão utilizar essas contas para o desempenho de suas atividades;

VI. As senhas de acesso à rede de computadores e aos sistemas informatizados devem ser alteradas, à cada 75(setenta e cinco) dias;

VII. Fica proibido o compartilhamento de “login” para funções de administração de sistemas;

VIII. As senhas sob hipótese alguma devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);

 IX. As senhas deverão seguir os seguintes pré-requisitos:

 • Tamanho mínimo de 08 (oito) caracteres;

• Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais.

# **10 - Acesso à rede**

Todos os servidores, membros de conselhos e colaboradores (estagiários) estão autorizados e poderão fazer uso dos recursos da rede corporativa dentro do domínio CREFITO 11, tais como:

 I - Correio eletrônico (e-mail);

 II - Internet, intranet;

 III - compartilhamento e armazenamento de arquivos;

 IV - Estações de trabalho;

V - Softwares e sistemas de informação; e

VI – Serviços de impressão.

- Os servidores, membros de conselho e colaboradores terão acesso unicamente e exclusivamente àqueles recursos da rede corporativa CREFITO 11 que lhe forem indispensáveis à realização de suas atividades.

- Os serviços e sistemas autenticados serão disponibilizados para os usuários

registrados e identificados pelo seu login e senha.

 - Manter, obrigatoriamente, os dados críticos da sua Unidade Administrativa em compartilhamentos de rede disponibilizados pela área de TI;

 - A inclusão de acesso será realizada automaticamente quando houver novo

usuário na unidade de lotação;

 - Sob nenhuma hipótese os servidores que utilizam os recursos de rede disponibilizados pelo CREFITO 11 poderão utilizá-los para fazer o download ou distribuição de software pirateados, atividade considerada delituosa de acordo com a legislação nacional vigente;

 -É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela Gerência de suporte ao usuário e telecomunicação.

 - O CREFITO 11, disponibilizará o acesso à rede de internet sem fio (wi-fi) a seus visitantes e colaboradores, o ingresso a rede se dará mediante cadastro quando solicitado o acesso. A rede de internet sem fio (wi-fi) será segregada, garantido assim o isolamento da rede interna.

# **11 - Segmentação de ambiente, Publicações internas e externas**

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do CREFITO 11, e utilizados pelos servidores no desempenho de suas atividades funcionais. Assim recomendamos algumas medidas de segurança que devem ser adotadas quanto à utilização das estações de trabalho:

 I. Não sejam instalados softwares sem a autorização;

 II. Só sejam utilizados softwares devidamente licenciados;

 III. A utilização de software não licenciado ou considerado “pirata” constitui infração prevista na Lei no 9.609/1998;

 IV. Fica proibido remover ou modificar qualquer software, ou hardware sem a autorização da área de Tecnologia do CREFITO 11, pois, tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;

 V. Ao se ausentar da estação de trabalho, efetue o bloqueio ou “logoff” da mesma, evitando assim os acessos indevidos de outra pessoa a estação de trabalho através do seu usuário (login);

 VI. A liberação do dispositivo móvel (notebook) será permitida após os solicitantes assinarem o acordo de conhecimento das suas responsabilidades (quanto a proteção física, atualização do software, entre outros), renunciando direitos autorais dos dados, que permita a exclusão remota dos dados pela CREFITO 11;

 VII. Em caso de furto/roubo ou perda do dispositivo móvel, o servidor deverá comunicar imediatamente as autoridades policiais registrando, assim um boletim de ocorrência e deverá ainda comunicar a equipe de TI do CREFITO 11;

 VIII. Utilização da estação somente para fins profissionais

# **12 - Dos Gestores/Gerentes**

Cabe a todo gestor de área:

* Assegurar a adoção de métodos eficazes para o descarte seguro das informações;
* Adotar uma postura exemplar em relação à Segurança da Informação, servindo como modelo de comportamento para funcionários, prestadores de serviços, estagiários e outros sob sua supervisão;
* Obedecer a esta política, assim como às normas e procedimentos de Segurança da Informação estabelecidos;
* Garantir que todos tenham acesso a esta política e compreendam as normas e procedimentos definidos nela.

# **13 - Back-up**

Backup e restore são cópias de segurança, tendo por objetivo que os usuários se resguardem de uma ocasional perda de arquivos originais, seja por ações mau funcionamento dos sistemas ou ainda despropositadas pelo próprio usuário, permitindo assim a restauração das informações ou dados eventualmente perdidos..

# **14 - Gestão de mudanças**

Todas as mudanças devem ser constituídas, no mínimo, pelas fases de identificação, registro, planejamento, teste preliminar, aprovação, implementação e verificação dos potenciais impactos das mesmas por tanto:

* I. Toda e qualquer proposta de mudança deve ser aprovada formalmente pela alta gestão juntamente com a equipe técnica competente;
* II.Toda mudança realizada no Iprev/DF deverá ser devidamente comunicada à todas as partes interessadas;
* III. Deverá ser amplamente divulgada, visando a redução de eventuais resistências e dificuldades de implementação das mesmas;
* IV. Toda mudança, antes de ser implementada, deve contar com um plano de recuperação emergencial, incluindo procedimentos e responsabilidades para interrupção e recuperação, em caso de insucesso ou na ocorrência de eventos inesperados.

# **15 - Do Comitê Consultivo**

O Comitê Consultivo deve ter um perfil multidisciplinar e contar com a participação de gestores de diferentes áreas da empresa CREFITO 11.

# **16 - Da Inovação e Uso de Novas Tecnologias**

 Todos os servidores do CREFITO 11, deverão receber treinamento, educação e

conscientização apropriados, e as atualizações regulares das políticas, normas e procedimentos institucionais relevantes para a realização de suas funções.

Recomenda-se que o treinamento e educação em segurança da informação deve contemplar aspectos gerais, como:

 I. O comprometimento da alta gestão com a segurança da informação;

 II. Tornar conhecido e estar em conformidade com as obrigações e regras de segurança da informação aplicáveis, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos.

 III. Responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter seguro ou para proteger a informação que pertença a organização e partes externas.

 IV. O treinamento e a educação em segurança da informação devem ser realizados periodicamente. Treinamento e educação iniciais se aplicam aqueles que são transferidos para novas posições ou atribuições com requisitos de segurança da informação completamente diferentes, e não apenas para os novos iniciantes e deve ser realizado antes das pessoas assumirem os seus papéis, ou o mais rápido que possível.

 V. Procedimentos de segurança da informação básicos (tais como, notificação de incidente de segurança da informação) e controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa).

 VI. A organização deve desenvolver o programa de treinamento e educação com o objetivo de conduzir a educação e treinamento de forma eficaz. O programa deve estar alinhado com as políticas e procedimentos relevantes de segurança da informação da organização, levando em consideração as informações da organização a serem protegidas e os controles que devem ser implementados para proteger a informação. Recomenda-se que o programa considere diferentes formas de educação e treinamento, tais como, leituras ou auto estudos.

# **17 - Da Proteção à propriedade intelectual**

 Todos os procedimentos apropriados devem ser implementados para garantir

a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de softwares. Incluído os direitos de propriedade intelectual os direitos autorais de software ou documento, direitos de projetos, marcas, patentes e licenças de código fonte.

Produtos de softwares proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições da licença, como por exemplo, limitar o uso dos produtos em máquinas especificadas ou limitar a reprodução apenas para a criação de cópias de backup. É recomendado que a importância e a conscientização dos direitos de propriedade intelectual de software sejam comunicadas aos responsáveis pelo desenvolvimento de software na organização.

Requisitos legais, regulamentares e contratuais podem colocar restrições sobre a cópia de material proprietário. Em particular, eles podem exigir que apenas o material que é desenvolvido pela organização ou que está licenciado ou fornecido pelo desenvolvedor para a organização, pode ser utilizado. Violação de direitos autorais pode levar a ação judicial e pode envolver multas e processos criminais.

Recomendado que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

I. Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de software e de informação;

 II. Adquirir software somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não está sendo violado;

 III. Manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

 IV. Manter de forma adequada os registros de ativos, e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

 V. Manter provas e evidências da propriedade de licenças, discos-mestres, manuais etc.;

 VI. Implementar controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não está excedido;

 VII. Conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados;

 VIII. Estabelecer uma política para a manutenção das condições adequadas de licenças;

 IX. Estabelecer uma política para disposição ou transferência de software para outros;

 X. Cumprir termos e condições para software e informação obtidos a partir de redes públicas;

 XI. Não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral;

 XII. Não copiar no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral

# **18 – Considerações Finais**

É crucial ressaltar que as violações desta Política de Segurança da Informação (PSI) e das Normas de Segurança da Informação são tratadas com extrema seriedade. Toda e qualquer infração está sujeita a medidas disciplinares, as quais podem variar desde uma simples advertência até a demissão por justa causa, dependendo da gravidade da situação.

A adoção de uma postura rigorosa em relação à segurança da informação reflete o compromisso da organização com a proteção de seus ativos e a preservação da confiança de clientes, colaboradores e parceiros. Portanto, é responsabilidade de cada indivíduo compreender e seguir as diretrizes estabelecidas nesta PSI, contribuindo para a construção de um ambiente seguro e confiável para todos.

É essencial que todos os colaboradores estejam plenamente cientes das consequências de suas ações e compreendam a importância de proteger a integridade, confidencialidade e disponibilidade das informações da organização. Somente através do comprometimento e da conformidade de todos, podemos garantir uma segurança da informação eficaz e manter a reputação e os interesses da empresa protegidos.

Portanto, ao encerrar estas considerações finais, reforçamos a importância da observância estrita desta PSI e das normas de segurança estabelecidas, assegurando a proteção contínua dos ativos de informação da organização e o cumprimento dos mais elevados padrões de segurança.

# **19 - Referencias**

1 - Sobre a Política de Segurança da Informação (PSI)

ABNT NBR ISO/IEC 27001:2013: Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação dentro do contexto da organização.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n.º 13.709, de 14 de agosto de 2018: Estabelece regras sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais no Brasil.

Resolução CFM nº 1.821/2007: Define normas técnicas para digitalização e uso de sistemas informatizados para a guarda e manuseio de prontuário médico.

2 - Conceitos e Definições

ABNT NBR ISO/IEC 27002:2013: Fornece diretrizes para as práticas de gestão de segurança da informação, incluindo a seleção, implementação e gestão de controles levando em consideração o ambiente de risco de segurança da informação.

Glossário de Segurança da Informação (IT Governance): Define termos comuns usados em segurança da informação.

Cartilha de Segurança para Internet (CERT.br): Oferece definições e explicações sobre diversos tipos de ameaças, como vírus, worms, trojans, e práticas de segurança.

3 - Objetivos da Política de Segurança da Informação

Guia de Boas Práticas em Segurança da Informação (CGI.br): Orienta sobre a criação de políticas de segurança da informação, destacando a importância de diretrizes claras, prevenção de incidentes e continuidade das operações.

Manual de Segurança da Informação (Governo Federal): Documento que aborda os objetivos da política de segurança da informação, incluindo prevenção, atendimento aos requisitos legais e minimização de riscos.

4 - Aplicação da Política de Segurança da Informação

Manual de Segurança da Informação para Instituições Financeiras (Febraban): Detalha a importância da aplicação rigorosa das diretrizes de segurança da informação por todos os colaboradores.

Política de Segurança da Informação (Banco Central do Brasil): Documento que especifica a necessidade de adesão à PSI por todos os funcionários e colaboradores.

5 - Princípios da Política de Segurança da Informação

ABNT NBR ISO/IEC 27001:2013: Apresenta os princípios fundamentais que devem orientar a proteção dos ativos de informação de uma organização.

Cartilha de Segurança para Internet (CERT.br): Fornece orientações sobre os princípios de confidencialidade, integridade e disponibilidade.

6 - Requisitos da Política de Segurança da Informação

Lei Geral de Proteção de Dados (LGPD): Especifica os requisitos legais relacionados à proteção da informação e privacidade de dados.

Guia de Implementação de Políticas de Segurança da Informação (CERT.br): Documenta os requisitos necessários para garantir a eficácia da PSI.

7 - Monitoramento e Auditoria

Norma Complementar nº 14/IN01/DSIC/GSIPR: Estabelece os procedimentos de auditoria e monitoramento em segurança da informação para órgãos e entidades da administração pública federal.

Manual de Auditoria em Segurança da Informação (TCU): Guia de auditoria para verificar a conformidade com as políticas de segurança da informação.

8 - Responsabilidades Específicas Dos Usuários em Geral

Política de Segurança da Informação (Banco do Brasil): Documento que detalha as responsabilidades dos usuários em relação ao cumprimento das normas de segurança.

Manual de Segurança da Informação para Colaboradores (Bradesco): Define as responsabilidades dos funcionários para garantir a segurança da informação.

9 - Política de Senhas

ABNT NBR ISO/IEC 27002:2013: Fornece orientações sobre a gestão de senhas e a importância da criação de senhas seguras.

Guia de Boas Práticas em Segurança da Informação (CGI.br): Recomendações para criação e gestão de senhas seguras.

10 - Acesso à rede

Política de Segurança da Informação (SERPRO): Estabelece diretrizes para o acesso seguro à rede corporativa.

Norma Complementar nº 02/IN01/DSIC/GSIPR: Normas sobre a gestão de acessos e uso de redes.

11 - Segmentação de ambiente, Publicações internas e externas

Guia de Implementação de Políticas de Segurança da Informação (CERT.br): Orientações sobre segmentação de redes e boas práticas para publicações internas e externas.

Manual de Segurança da Informação (SERPRO): Medidas de segurança recomendadas para estações de trabalho e uso de dispositivos móveis.

12 - Dos Gestores/Gerentes

ABNT NBR ISO/IEC 27001:2013: Define as responsabilidades dos gestores em relação à implementação e manutenção da segurança da informação.

Guia de Boas Práticas em Segurança da Informação (CGI.br): Enfatiza o papel dos gestores na promoção e cumprimento das políticas de segurança.

13 - Back-up

ABNT NBR ISO/IEC 27002:2013: Orientações sobre a realização de backups e recuperação de dados.

Guia de Boas Práticas em Segurança da Informação (CGI.br): Recomendações para a implementação de políticas eficazes de backup.

14 - Gestão de mudanças

ABNT NBR ISO/IEC 27001:2013: Procedimentos para a gestão de mudanças em sistemas de informação.

Manual de Gestão de Mudanças (SERPRO): Documentação sobre práticas de gestão de mudanças no ambiente de TI.

15 - Do Comitê Consultivo

Guia de Boas Práticas em Segurança da Informação (CGI.br): Importância da criação de comitês consultivos multidisciplinares.

Política de Segurança da Informação (Banco do Brasil): Definição e papel dos comitês consultivos na segurança da informação.

16 - Da Inovação e Uso de Novas Tecnologias

Manual de Segurança da Informação (SERPRO): Treinamento e educação continuada em segurança da informação.

Guia de Boas Práticas em Segurança da Informação (CGI.br): Programas de educação e treinamento em segurança da informação.

17 - Da Proteção à propriedade intelectual

Lei nº 9.609/1998 (Lei de Software): Regulamenta a proteção da propriedade intelectual de software.

Política de Propriedade Intelectual (INPI): Orientações sobre proteção e conformidade com os direitos de propriedade intelectual.

18 – Considerações Finais

ABNT NBR ISO/IEC 27001:2013: Enfatiza a importância da adesão às políticas de segurança da informação e as consequências das violações.

Manual de Segurança da Informação (Governo Federal): Reitera a seriedade das infrações e as medidas disciplinares aplicáveis.