1. OBJETIVO

1.1. Dispõe sobre a Política de Segurança de Informações (PSI) do Instituto Nacional de Tecnologia e Saúde. Visando garantir a continuidade do negócio, os dados e ativos de informação sob sua administração.

1.2. O compromisso oficial do INTS Região SACA de proteger as informações que são de sua propriedade ou sob sua guarda. Portanto, todos os seus colaboradores, fornecedores, clientes e parceiros comerciais devem seguir esta política. Garantindo a utilização segura e consciente dos seus ativos de informação para garantir processos em conformidade.

1.3. Fortalecer a cultura de segurança da informação do INTS Região SACA e desenvolver uma perspectiva abrangente.

1.4. Adotar uma perspectiva que facilite a gestão de riscos e segurança da informação.

1.5. Estabelecer padrões para o processo de gestão da segurança da informação que as partes envolvidas devem seguir ao adotar procedimentos, requisitos legais e práticas para garantir que a segurança da informação esteja alinhada com a estratégia organizacional e as recomendações dos órgãos reguladores; difundir a importância e incentivar a melhoria contínua; e promover a proteção de informações sensíveis preservando informações sobre:

a) Integridade: garantia de que as informações permaneçam no estado original quando guardadas ou transmitidas, para evitar alterações intencionais ou inesperadas;

b) Confidencialidade: garante que as informações só sejam acessadas por pessoas autorizadas;

c) Disponibilidade: garante que os usuários autorizados possam acessar as informações e ativos relevantes sempre que necessário.

1.6. O INTS Região SACA no uso de suas funções e responsabilidades, reconhece que as informações geradas, obtidas ou coletadas pelo INTS Região SACA e suas unidades sob gestão são geradas, obtidas ou coletadas de forma legítima e acessível, e que essas informações devem ser mantidas limpas e seguras quando necessário.

1.7. CONSIDERANDO que a Política de Segurança da Informação (PSI) do INTS Região SACA deve se ajustar às Diretrizes para a Gestão de Segurança da Informação e às normas NBR ISO/IEC em relação à proteção da informação;

1.8. O INTS Região SACA tem como objetivo nesta Política de Segurança da Informação orientar os colaboradores e definir os procedimentos e controles do INTS Região SACA em relação à segurança cibernética, os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, estando em conformidade com a legislação vigente. Destaca-se que todos os fornecedores de tecnologia da informação relevantes devem estar em conformidade com esta Política.

2. RESPONSABILIDADES

2.1 ELABORAÇÃO E REVISÃO: Tecnologia da Informação.

2.2 EXECUÇÃO: Todas as áreas do INTS Região SACA, todos os administradores e demais colaboradores do INTS Região SACA, com a recomendação de serem diligentes no cumprimento

das diretrizes definidas pelo INTS Região SACA referentes ao processo de compras, locação e o respectivo acompanhamento dos prestadores de serviços e fornecedores do INTS Região SACA.

Alta Gestão e Diretorias: Análise final e discussão sobre o que fazer.

Setor de TI: Monitorar os sistemas para identificar possíveis não conformidades a esta política.

Conforme permitido pelas leis brasileiras, esta política informa todas as partes interessadas sobre a possibilidade de monitoramento e gravação de documentos, ambientes, sistemas, computadores e redes sob administração direta e indireto pelo INTS Região SACA.

3. DEFINIÇÕES

3.1. Ativo: Todo e qualquer bem do INTS Região SACA que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento;

3.2. Ativo Crítico e Sensível: Todo ativo considerado essencial para o INTS Região SACA, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido podem causar danos à instituição;

3.3. Ativo de informação: Patrimônio intangível do INTS Região SACA, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal, natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao INTS Região SACA por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do INTS Região SACA ou por infraestrutura externa contratada pela instituição, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física;

3.4. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do INTS Região SACA, que tem por finalidade tratar questões ligadas à Segurança da Informação;

3.5. Confidencialidade: Propriedade dos ativos da informação do INTS Região SACA, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas;

3.6. Integridade: Propriedade dos ativos da informação do INTS Região SACA, de serem exatos e completos;

3.7. Disponibilidade: Propriedade dos ativos da informação do INTS Região SACA, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas;

3.8. Controle: Medida de segurança adotada pelo INTS Região SACA para o tratamento de um risco específico;

3.9. Diretriz: Conjunto de instruções ou indicações que orientam o que deve ser feito para se alcançar os objetivos estabelecidos na política;

3.10. Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;

3.11. Usuário da informação: Colaboradores com vínculo empregatício de qualquer área do INTS Região SACA ou terceiros alocados na prestação de serviços para o INTS Região SACA, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do INTS Região SACA para o desempenho de suas atividades profissionais;

3.12. Política de Segurança da Informação: documento aprovado pelo INTS Região SACA, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

3.13. Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do INTS Região SACA;

3.14. Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação do INTS Região SACA;

3.15. Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do INTS Região SACA;

3.16. Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com o INTS Região SACA com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte;

3.17. Usuário: Todo funcionário, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pelo INTS Região SACA;

3.18. Log: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional;

3.19. VPN (Virtual Private Network) – (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas;

3.20. Wireless (rede sem fio) - rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

3.21. Ameaça: Causa potencial de um incidente, que pode vir a prejudicar o INTS Região SACA;

3.22. Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do INTS Região SACA;

3.23. Vírus: Programa malicioso que se propaga e infecta o computador;

3.24. Worms: Programa semelhante ao vírus, que infecta o sistema, tendo como característica a autor replicação.

4. DIRETRIZ

O INTS Região SACA tem como missão prover à administração pública soluções de gestão e tecnologia na área de saúde, educação e ação social buscando a satisfação das partes interessadas, assim como, a conformidade com as legislações aplicáveis.

O INTS Região SACA entende que a informação institucional é um bem essencial para suas atividades e para resguardar a qualidade na gestão de serviços de saúde, educação e ações sociais destacando-se pela qualidade, aprimoramento e modernização dos seus serviços.

O INTS Região SACA compreende que a manipulação de suas informações passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações institucionais.

Dessa forma, O INTS Região SACA estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

4.1. PROPÓSITO

Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores do INTS Região SACA adotar padrões de comportamentos seguros, adequados a missão, visão e valores do INTS;

Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

Resguardar as informações do INTS Região SACA, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus colaboradores, fornecedores e parceiros comerciais;

Minimizar os riscos de vazamento de dados, uso indevido de ativos, garantindo confiança do seu processo organizacional ou de qualquer outro impacto negativo nos contratos do INTS Região SACA como resultado de falhas de segurança.

4.2. ESCOPO

Esta política se aplica a todos os usuários da informação do INTS Região SACA, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com o INTS Região SACA, tais como empregados, ex-empregados, prestadores de serviço, ex- prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações do INTS Região SACA e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do INTS Região SACA.

O objetivo da gestão de Segurança da Informação do INTS Região SACA é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

A Diretoria e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação no INTS Região SACA. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da instituição. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades do INTS Região SACA.

Esta política e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, no contexto de uso de informações e recursos de Tecnologia da Informação, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização do Comitê Gestor de Segurança da Informação (CGSI) do INTS Região SACA, devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

4.3. É POLÍTICA DO INTS REGIÃO SACA

4.3.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação do INTS Região SACA sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

4.3.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Colaboradores, terceiros contratados e, onde pertinente, clientes.

4.3.3. Garantir a educação e conscientização sobre as práticas adotadas pelo INTS Região SACA de segurança da informação para colaboradores, terceiros contratados e, onde pertinente, clientes.

4.3.4. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

4.3.5. Tratar integralmente incidentes de segurança da informação, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

4.3.6. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

4.3.7. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da instituição.

4.4. PROCEDIMENTOS E CONTROLES ADOTADOS

É de extrema importância a disseminação da cultura de segurança cibernética para garantir a integridade, confiabilidade e disponibilidade das informações. Para garantir o cumprimento dos princípios dispostos acima, o INTS Região SACA utiliza diversos meios como as políticas internas, instruções normativas, comunicados corporativos e a realização de treinamentos periódicos de segurança da informação.

4.4.1. TRATAMENTO DAS INFORMAÇÕES

Os ativos de informação da instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados.

Todo ativo de informação deve possuir um responsável explicitamente identificado e classificadas dentro dos critérios e normativos técnicos.

a) Pública - É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

b) Interna - É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

c) Confidencial - É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

d) Secreta - É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado por seus diretores ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

4.4.2. CONTROLE DE ACESSO E GERENCIAMENTO

A prática de Controle de Acesso e Gerenciamento tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade das informações. O INTS Região SACA segue as boas práticas no sentido de orientar que todos os usuários devem possuir acesso à informação de acordo com as necessidades de negócio. O INTS Região SACA possui procedimentos formalizados e a descrição dos fluxos operacionais para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso. Adicionalmente, os procedimentos de Concessão e Alteração devem ser aprovados pelo Setor de Tecnologia da Informação, Diretoria Executiva e Segurança da informação. O INTS Região SACA realiza periodicamente a revisão de acessos, conforme política, que tem como objetivo a atualização dos acessos e permissões, procedimento este, que é coordenado pela área de Segurança da Informação.

Todos os ambientes do INTS Região SACA, devem ter funções separadas. A segregação de funções permite que funções e áreas de responsabilidades conflitantes sejam separadas para evitar alterações imprevistas e evitar o mal-uso intencional ou não intencional dos ativos de informação. Faz-se necessário o uso de controles adicionais de segurança em casos de exceção, seja por restrições técnicas ou comerciais.

4.4.3. GERENCIAMENTO DE RISCOS E TECNOLOGIA DA INFORMAÇÃO

O INTS Região SACA verifica periodicamente o controle de acessos à internet e controla os aplicativos instalados nos computadores. Vale ressaltar que nenhum usuário poderá possuir acesso de administrador local, impossibilitando a instalação de qualquer aplicativo.

Somente podem ser instalados aplicativos previamente testados e autorizados por Tecnologia da Informação.

Deve ser adotada a gestão de riscos de segurança da informação, segundo critérios a serem definidos pela área de Segurança da Informação, para a identificação e implementação das medidas de proteção necessárias para a mitigação ou eliminação dos riscos.

O INTS Região SACA realiza o monitoramento da rede por meio de software específico e dispositivos de monitoramento de rede.

4.4.4. SEGURANÇA DE REDE

A segurança é realizada através do monitoramento e gerenciamento da infraestrutura, sendo que todo acesso às redes internas e acessos à internet são controlados por Tecnologia da Informação.

Fica instituído que todo tráfego de acesso a rede internet deverá ser feito através de protocolos seguros e dispositivos de Firewall, IPS e IDS na rede a fim mitigar os riscos internos e externos.

Os acessos externos as instalações do INTS Região SACA deverão ser impreterivelmente feitas através de VPN (Virtual Private Network) e registrado os logs de acessos. Na impossibilidade de acesso fica o setor de Tecnologia da Informação responsável pela avaliação da melhor forma de acesso.

4.4.5. SEGURANÇA E GERENCIAMENTO DE ATIVOS DE SISTEMAS

Quando disponível, o acesso aos sistemas de informação do INTS Região SACA é integrado com o AD (Active Directory), que possui as suas especificidades definidas em políticas.

Para os Sistemas de Informação que não estão integrados com AD, existe um pré-requisito mínimo para as parametrizações de senhas definido em política. Referente ao gerenciamento das parametrizações de segurança, somente a área de Tecnologia da Informação tem acesso para alterar as configurações de acesso e segurança nos Sistemas de Informação.

4.4.6. GESTÃO DE AMEAÇAS E VULNERABILIDADES DE TI

O ambiente possui instalado software de antivírus para a proteção contra vírus, arquivos e softwares maliciosos, atualizados periodicamente. Todas as atualizações de segurança do Windows e Linux são gerenciadas e atualizadas frequentemente.

4.4.7. TRATAMENTO DE INCIDENTES DE REDES

Os incidentes de segurança da informação devem ser registrados e gerenciados.

Deve ser definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, segundo critérios a serem definidos pela área de Segurança da Informação do INTS Região SACA, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais no órgão responsável.

4.4.8. DISPOSITIVOS E CONTROLES DE MÍDIA

O termo mídia removível; refere-se a dispositivos como CDs, DVDs, Disquetes, Pen Drives, cartões de memória, HDs portáteis, telefones celulares e outros que são capazes de ler e gravar dados. Por

seu um ponto de vulnerabilidade dentro das instalações do INTS Região SACA, o seu uso é proibido e somente pessoas previamente autorizadas pela Tecnologia da Informação e Diretoria tem acesso as mídias removíveis no equipamento de trabalha computador.

A liberação das portas USB dos desktops e notebooks é feita somente se o uso for justificado e aprovado pela gerência do colaborador solicitante. O INTS não disponibiliza mídias removíveis para seus colaboradores exceto nos seguintes casos:

a) Solicitação do setor Jurídico para demandas externas;

b) Solicitação do setor de Licitações para demandas externas;

c) Solicitação da alta gestão e diretoria

Todos os dados gerados nas instalações do INTS Região SACA sugerem-se que, se dê preferência ao armazenamento nos diretórios da rede e repositório.

4.4.9. SEGURANÇA FÍSICA

Os recursos e instalações de processamento de informações críticas para as atividades do INTS Região SACA são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso. Os equipamentos críticos possuem proteção contra desastre físico e recursos para combate a incêndio. O INTS Região SACA possui sistema para controle do acesso dos colaboradores, prestadores de serviços ou fornecedores aos locais restritos, que são monitorados por câmeras.

É disponibilizado para cada profissional, um posto de trabalho, composto de equipamentos e softwares, para que este desempenhe suas funções.

O usuário é responsável pelas informações armazenadas na sua estação de trabalho. Para isso deve seguir diretrizes e práticas de segurança de Informação definidas nos Procedimentos Operacionais (PO) da Tecnologia da Informação para minimizar e evitar a exposição de informações consideradas sensíveis para a organização, clientes e parceiros.

4.4.10. SEGURANÇA LÓGICA

Fica decidido incluir toda e qualquer informação relacionada às atividades do INTS Região SACA no backup. Os servidores usarão o planejamento da TI para programar e executar automaticamente esses backups.

Após a conclusão dos backups, eles serão catalogados em formulários de registro para garantir que as informações sejam protegidas pelo INTS. O setor de TI é responsável por verificar a integridade das copias de segurança.

Qualquer alteração nas práticas de backup deve ser aprovada pela Gerência de Tecnologia da Informação para reduzir os riscos.

4.4.11. TELEFONIA FIXA E MÓVEL

Fica a cargo do usuário o uso consciente e gestão da linha de telefonia móvel, respeitando as diretrizes e procedimentos da instituição.

A telefonia fixa nas dependências do INTS Região SACA é de uso exclusivo para execução de suas atividades diárias, sendo vetado o uso para fins próprios.

Como o serviço de telefonia do INTS Região SACA é essencialmente uma ferramenta de trabalho, poderá ser gravado os ramais telefônicos sem avisar o usuário em caso de suspeitas de ameaças à segurança, fraude ou desvio de conduta profissional. O conteúdo das gravações é considerado sigiloso e não deve ser divulgado a ninguém fora do INTS Região SACA salvo no caso de decisão judicial.

O setor de Tecnologia da Informação deverá efetuar a implementação de procedimentos e/ou registros a fim de normatizar o uso.

4.5. PAPÉIS E RESPONSABILIDADES

4.5.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI (necessário implantar)

Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos, Jurídico, Comunicação Núcleo de Informação e Planejamento e Assessoria Técnica.

É responsabilidade do CGSI:

a) Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

b) Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

c) Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PSI;

d) Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do INTS Região SACA.

4.5.2. GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

É responsabilidade da Gerência de Tecnologia da Informação:

a) Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

b) Apoiar o CGSI em suas deliberações;

c) Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PSI;

d) Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

e) Tomar as ações cabíveis para se fazer cumprir os termos desta política;

f) Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

4.5.3. GESTORES DA INFORMAÇÃO

É responsabilidade dos Gestores da Informação:

a) Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo INTS Região SACA;

b) Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo INTS Região SACA;

c) Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário;

d) Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

e) Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo INTS Região SACA.

4.5.4. USUÁRIOS DA INFORMAÇÃO

É responsabilidade dos Usuários da Informação:

a) Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

b) Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

c) Comunicar à Gerência de Tecnologia da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do INTS Região SACA;

d) Assinar o Termo de Uso de Sistemas de Informação e/ou equipamentos computacionais do INTS Região SACA, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

e) Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

4.5.5. TECNOLOGIA DA INFORMAÇÃO

É responsabilidade da Tecnologia da Informação:

A área de tecnologia da informação do INTS Região SACA tem como pilar três preceitos básicos, que são: pessoas, processos e tecnologia. As pessoas são fundamentais do tratamento das informações, os processos são responsáveis por estruturar a área de TI e a tecnologia é que oferece suporte aos processos.

O departamento de TI é responsável por garantir a criação, manutenção e implementação de políticas e/ou soluções de tecnologia que podem:

a) Ampliar a produtividade do negócio;

b) Garantir a segurança das informações;

c) Implementar a infraestrutura necessária para o funcionamento integral da empresa;

d) Publicar e promover as verses da política de segurança da informação.

e) Promover a conscientização dos colaboradores em relação a relevância da segurança da informação conforme DT.TIC.001-Diretriz- Orientações e Restrições;

f) Analisar criteriosamente os incidentes recorrentes junto com os usuários;

g) Realizar inspeção físicas ou logica nos recursos tecnológicos (Manutenção Preventiva);

h) Gerenciamento da equipe de TI;

i) Alinhamento do uso das tecnologias da informação aos objetivos estratégicos da empresa;

j) Controle de todos os serviços de sistemas operacionais e de banco de dados da empresa;

k) Definição das regras para a correta utilização dos sistemas;

l) Suporte aos processos do INTS Região SACA; gerenciamento de riscos do setor de TI;

m) Administração da infraestrutura física e lógica dos locais informatizados do INTS Região SACA.

4.6. SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave;

No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao INTS Região SACA, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

4.6.1. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação;

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do INTS Região SACA adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações do INTS Região SACA.

5. DOCUMENTOS COMPLEMENTARES/REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.

ABNT NBR ISO/IEC 27701:2019 – Tecnologia da Informação – Técnicas de segurança – gestão da privacidade da informação — Requisitos e diretrizes

Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

Lei de Acesso à Informação (LAI) 12.527 de 18/11/2011.

DT.TIC.001 - Diretriz- Orientações e Restrições

6. HISTÓRICO DE ALTERAÇÕES

Revisão	Elaborado/revisado por	Data	Histórico de alteração	Aprovado por	Data
00	Ricardo Souza	24.05.2023	Emissão inicial	Marcelo Souza Ribeiro	02.06.2023

7. ANEXOS

Não aplicável.