ORDEM DE SERVIÇO DTI Nº 010/2023

Dispõe sobre a política de segurança da informação e cibernética no âmbito da Fundação CASA/SP - Centro de Atendimento Socioeducativo ao Adolescente do Estado de São Paulo.

A **Divisão de Tecnologia da Informação (DTI),** no uso das atribuições conferidas a este departamento, junto com suas gerências e seções, resolvem:

Artigo 1º - As regras e diretrizes aqui estabelecidas devem ser seguidas por todos os **USUÁRIOs,** sem quaisquer exceções.

Artigo 2º - A presente **OS** tem por finalidade estabelecer um conjunto de diretrizes, regras e procedimentos estabelecidos para a instituição proteger suas informações e **ativos de TIC,** minimizando os riscos associados à segurança da informação e às ameaças cibernéticas. Esta **Política de Segurança da Informação e Cibernética (PSIC)** define as responsabilidades dos envolvidos, estabelece padrões de conduta e promove a conscientização e a conformidade em toda a **Fundação CASA/SP.**

CAPÍTULO I - FUNDAMENTAÇÃO LEGAL E NORMATIVA

Artigo 3º - A presente **OS** está fundamentada nos seguintes instrumentos legais e normativos:

I. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991, e dá outras providências;
II. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
III. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;
IV. Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco civil da Internet;
V. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD);
VI. Lei nº 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública;
VII. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril (“GDPR”);
VIII. DN CGGDIESP-1, de 30 de dezembro de 2021, que traz boas práticas em segurança da informação, para privacidade e proteção de dados pessoais e para a gestão de dados e informações;
IX. DO SP V132/N259, de 29 de dezembro de 2022; IN PGDI-1, de 27 de dezembro de 2022, referente ao anexo II, 3 - Tabela de Providências Complementares e Responsáveis - Ativos da Informação: Orientação Técnica e Modelo - Inventário de Dados, da Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

X. Normas ABNT NBR ISO/IEC: Série ABNT NBR ISO/IEC 27000 (ABNT NBR ISO/IEC 27001 e 27002), fornecem diretrizes e melhores práticas internacionais para a gestão de segurança da informação;
XI. Ordens de Serviço publicadas pela Divisão de Tecnologia da Informação (Fundação CASA/SP).

CAPÍTULO II - CONCEITOS E DEFINIÇÕES

Artigo 4º - Para fins desta **OS,** considera-se que:

I. **OS:** Ordem de Serviço;
II. **Divisão de Tecnologia da Informação (DTI):** departamento com a responsabilidade de dispor, gerir e implementar todas as ações de gestão de **TIC** no âmbito institucional;
III. **Gerência de Segurança e Infraestrutura (GSINF)**: departamento com a responsabilidade de dispor, gerir e implementar ações e atividades operacionais relacionadas à segurança da informação e cibernética, e infraestrutura na organização;
IV. **Seção de Segurança da Informação (SSI):** departamento que implementa e executa atividades operacionais relacionadas à gestão de acessos e segurança da informação e cibernética;
V. **Grupo Técnico de Apoio Tecnológico (GTAT):** grupo especializado no desenvolvimento e implementação de soluções de *software*, como aplicações, sistemas e aplicativos móveis;
VI. **TIC:** tecnologia da informação e comunicação;
VII. **PSIC:** política de segurança da informação e cibernética;
VIII. **ativos de TIC:** são todos os itens, físicos ou virtuais, que compõem a infraestrutura de **TIC** da instituição. Ou seja, tudo que é hardware, software, redes e outras tecnologias fundamentais para a continuidade das operações de quase todo tipo de negócio;
IX. **recursos de TIC:** consideram-se recursos de **TIC** o conjunto formado pelos bens e serviços de **TIC** que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação. Entre os recursos estão:
    i. desktops/computadores/notebooks;
    ii. dispositivos móveis;
    iii. plataformas de colaboração e serviços de mensageria;
    iv. aplicações/sistemas/websites;
    v. projetores/data shows;
    vi. acesso à internet;
    vii. entre outros.
X. **controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;
XI. **administradores de TIC:** são as pessoas designadas formalmente, pela autoridade máxima da **DTI,** com atribuição principal de ser o responsável técnico pelos seus recursos de **TIC;**
XII. **gestor imediato:** é o responsável ou a pessoa designada formalmente de uma localidade/departamento, pela autoridade máxima da localidade/departamento, com a atribuição de representar seus **USUÁRIOs,** nos assuntos relacionados com a utilização dos recursos de **TIC** da **Fundação CASA/SP;**

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/valida/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

XIII. ***malwares:*** forma reduzida de *malicious software* (software malicioso), é um software usado por atacantes cibernéticos para comprometer a operação de um dispositivo computacional, colher informações sensíveis ou ganhar acesso a sistemas computacionais privados;

XIV. ***phishing:*** é uma técnica de ataque cibernético em que um indivíduo mal-intencionado tenta enganar uma vítima para que ela forneça informações confidenciais, como senhas, informações bancárias, números de cartão de crédito e outras informações pessoais;

XV. ***patches:*** são pequenas atualizações de *software* que visam corrigir problemas de segurança ou *bugs* em um programa existente;

XVI. **USUÁRIO:** é qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a **Fundação CASA/SP,** ou em condição autorizada, que utiliza, de qualquer forma, algum recurso de **TIC** da instituição.

CAPÍTULO III – INTRODUÇÃO

Artigo 5º - Propósito

§ 1º - Esta **OS** apresenta a **Política de Segurança da Informação e Cibernética (PSIC)**, que estabelece um conjunto abrangente de diretrizes, práticas e procedimentos destinados a proteger e garantir a confidencialidade, integridade e disponibilidade das informações e dos ativos digitais de uma organização. Essa política é fundamental para a gestão e o monitoramento de riscos relacionados à segurança da informação e cibernética, e tem como objetivo orientar os **USUÁRIOs** e terceiros envolvidos na aplicação das melhores práticas de segurança.

Artigo 6º - Escopo

§ 1º - A **OS** abrange todos os sistemas, redes, aplicativos, dados, informações e **ativos de TIC** da organização, bem como os **USUÁRIOs** e terceiros envolvidos no uso, acesso, processamento, armazenamento ou transmissão de informações.

CAPÍTULO IV – OBJETIVOS

Artigo 7º - Proteção de ativos e informações: Garantir a confidencialidade, integridade e disponibilidade dos **ativos de TIC** e informações, incluindo dados pessoais, propriedade intelectual, informações financeiras e outros dados confidenciais.

Artigo 8º - Conformidade legal e regulatória: Assegurar que a instituição cumpra todas as leis, regulamentações e normas aplicáveis relacionadas à segurança da informação e cibernética, como a **LGPD,** o Marco Civil da Internet e outros requisitos específicos do setor.

Artigo 9º - Gestão de riscos: Identificar, avaliar e tratar os riscos associados à segurança da informação e cibernética, implementando controles e medidas de segurança adequados para mitigar riscos e proteger a organização.

§ 1º - Implementar soluções e controles de segurança eficazes para prevenir, detectar e responder a ameaças e incidentes de segurança, minimizando o impacto e a probabilidade de ocorrência;

§ 2º - Estabelecer processos e procedimentos para lidar com incidentes de segurança da informação e cibernética, garantindo uma resposta rápida e eficaz, bem como a continuidade dos negócios e a recuperação após eventos de segurança;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

§ 3º - Monitorar continuamente a eficácia dos controles de segurança e a conformidade com a **PSIC,** identificando áreas de melhoria e atualizando esta **OS,** conforme necessidade, para se adaptar às mudanças nas ameaças, tecnologias e requisitos do negócio institucional;
§ 4º - Seguir as melhores práticas do setor e as normas internacionais, como as normas ISO/IEC 27000, para garantir uma abordagem robusta e eficaz para a gestão da segurança da informação e cibernética.

Artigo 10 - Conscientização e treinamento: Promover uma cultura de segurança da informação e cibernética por meio da conscientização e do treinamento, se necessário, dos **USUÁRIOs,** para garantir que todos compreendam suas responsabilidades e adotem práticas seguras.

CAPÍTULO V - PRINCÍPIOS BÁSICOS

Artigo 11 - Confidencialidade: Proteger as informações contra o acesso e divulgação não autorizados. A confidencialidade garante que apenas pessoas ou sistemas autorizados possam acessar e visualizar informações sensíveis, mantendo a privacidade e a segurança dos dados.

Artigo 12 - Integridade: Garantir a precisão e consistência dos dados ao longo de seu ciclo de vida. A integridade assegura que as informações sejam protegidas contra alterações não autorizadas, seja de forma maliciosa ou acidental, garantindo que os dados permaneçam íntegros e confiáveis.

Artigo 13 - Disponibilidade: Assegurar que as informações e os sistemas estejam acessíveis e funcionais para os **USUÁRIOs** e processos autorizados quando necessário. A disponibilidade inclui a implementação de medidas para prevenir interrupções nos sistemas/aplicações, proteger contra os ataques cibernéticos e garantir a continuidade dos negócios institucionais e a recuperação de desastres.

CAPÍTULO VI – ESTRUTURA ORGANIZACIONAL E RESPONSABILIDADES

Artigo 14 - Responsável pela **DTI:**

I. Planejar e solicitar recursos necessários junto à **Diretoria de Gestão Administrativa (DGA)** e outras instâncias, se preciso, recursos tecnológicos, financeiros e humanos necessários para implementar e manter as medidas de segurança da informação e cibernética;
II. Participar na elaboração, revisão e aprovação da **PSIC,** garantindo que as estratégias de **TIC** e segurança estejam alinhadas com os objetivos e diretrizes da organização;
III. Supervisionar e colaborar com a **GSINF, SSI** e outros departamentos e gestores para integrar a segurança da informação e cibernética em todos os aspectos das operações e processos institucionais;
IV. Supervisionar e garantir a implementação das medidas de segurança, políticas e procedimentos estabelecidos pela política de segurança da informação e cibernética, incluindo a proteção de infraestrutura, sistemas, redes e dados;
V. Garantir que os **administradores de TIC** esteja devidamente treinada e atualizada sobre as melhores práticas, normas e regulamentações de segurança da informação e cibernética;
VI. Estabelecer e manter uma estrutura de governança de **TIC** que inclua a segurança da informação e cibernética como um componente crítico, promovendo a responsabilidade e a conformidade em toda a organização;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

VII. Fomentar uma cultura de conscientização em segurança da informação e cibernética, garantindo que todos os **USUÁRIOs** compreendam e sigam as políticas e procedimentos estabelecidos;
VIII. Supervisionar e colaborar com a **GSINF** e a **SSI** na gestão e resposta a incidentes de segurança, garantindo a continuidade dos negócios institucionais e a recuperação após eventos de segurança;
IX. Monitorar e avaliar a eficácia das medidas de segurança da informação e cibernética, identificando áreas de melhoria e ajustando a estratégia conforme necessário;
X. Garantir que a organização esteja em conformidade com as leis, regulamentações e normas aplicáveis em matéria de segurança da informação e cibernética.

Artigo 15 - Responsável pela **GSINF:**

I. Garantir a implementação integral, monitoramento e atualização da **PSIC;**
II. Desenvolver, implementar e manter a **PSIC,** garantindo que a organização siga as melhores práticas e esteja em conformidade com as leis, regulamentações e normas aplicáveis;
III. Estabelecer e gerenciar o programa de segurança da informação, incluindo a definição de objetivos, estratégias e métricas de desempenho;
IV. Coordenar e liderar as iniciativas de segurança da informação em toda a organização, dando suporte à **DTI** e trabalhando com outras áreas da **Fundação CASA/SP;**
V. Identificar, avaliar e gerenciar riscos relacionados à segurança da informação e cibernética, desenvolvendo e implementando medidas de mitigação adequadas;
VI. Estabelecer e manter um processo eficaz de gestão de incidentes e resposta a incidentes, garantindo que a organização possa identificar, conter e resolver rapidamente os incidentes de segurança;
VII. Promover a conscientização e o treinamento em segurança da informação e cibernética para todos os **USUÁRIOs,** fornecendo informações, orientações e recursos necessários para garantir a conformidade com as políticas e os procedimentos de segurança;
VIII. Coordenar e supervisionar as atividades de monitoramento, detecção, prevenção e resposta a ameaças cibernéticas, incluindo a implementação de tecnologias e processos apropriados, como *firewalls,* sistemas de detecção de intrusões, soluções de antivírus, entre outras;
IX. Colaborar, se autorizado e possível, com outras organizações, entidades governamentais e grupos do setor para compartilhar informações e conhecimentos sobre ameaças à segurança, tendências e melhores práticas;
X. Participar do planejamento e da implementação de iniciativas junto com a **DTI,** relacionadas à continuidade de negócios institucionais e recuperação de desastres, garantindo que a organização possa retomar suas operações de maneira rápida e eficaz após um incidente de segurança ou outro evento disruptivo;
XI. Manter-se atualizado sobre as tendências e desenvolvimentos em segurança da informação e cibernética, garantindo que a organização possa adaptar-se e responder às ameaças emergentes.

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/valida/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

Artigo 16 - Responsável pela **SSI:**

I. Desenvolver e implementar a estratégia de segurança cibernética da organização junto com a **GSINF,** estabelecendo metas e objetivos específicos e alinhados com as metas;
II. Trabalhar em estreita colaboração com a **DTI, GSINF** e outros departamentos e gestores para integrar a segurança cibernética em todos os aspectos das operações e processos institucionais;
III. Liderar a equipe da **SSI,** supervisionando as atividades diárias, fornecendo orientação, treinamento e suporte aos membros da equipe;
IV. Coordenar a identificação, análise e mitigação de riscos cibernéticos, garantindo que as medidas de segurança apropriadas sejam implementadas e mantidas;
V. Implementar e manter as ferramentas, tecnologias e processos necessários para proteger os sistemas, redes e dados da organização contra ameaças cibernéticas;
VI. Estabelecer e manter um processo de gestão de incidentes de segurança cibernética, assegurando que a organização possa responder rapidamente e efetivamente a incidentes e violações de segurança;
VII. Fomentar uma cultura de conscientização e responsabilidade em segurança cibernética, garantindo que todos os **USUÁRIOs** compreendam e sigam as políticas e procedimentos de segurança cibernética;
VIII. Monitorar e analisar as tendências e desenvolvimentos no campo da segurança cibernética, adaptando a estratégia e as práticas da organização conforme necessário para enfrentar as ameaças emergentes;
IX. Manter-se atualizado sobre as tendências e desenvolvimentos em segurança da informação e cibernética, garantindo que a organização possa adaptar-se e responder às ameaças emergentes.

Artigo 17 - GTAT:

I. Incorporar práticas de segurança desde o início do processo de desenvolvimento de software, incluindo a revisão de requisitos de segurança, a implementação de controles e a realização de testes de segurança;
II. Considerar a segurança ao projetar e arquitetar soluções, garantindo que as aplicações e infraestrutura sejam projetadas de acordo com os princípios de segurança da organização e em conformidade com a **PSIC;**
III. Aplicar as melhores práticas de desenvolvimento seguro, como a revisão de código, a análise estática e dinâmica de segurança e o treinamento em segurança da equipe de desenvolvimento;
IV. Implementar e manter sistemas de gerenciamento de configuração e controle de versão seguros e eficazes, garantindo que as alterações na infraestrutura e no código sejam rastreadas e controladas adequadamente;
V. Garantir que as implantações e atualizações de aplicações e infraestrutura sejam realizadas de forma segura e controlada, minimizando o risco de interrupções ou exposição a vulnerabilidades;
VI. Estabelecer processos e sistemas de monitoramento contínuo de segurança para identificar e responder a incidentes e ameaças em tempo real, integrando-se com as equipes de segurança e operações da organização;
VII. Garantir a aplicação rápida e eficiente de patches de segurança e atualizações para aplicações e infraestrutura, mantendo-os protegidos contra vulnerabilidades conhecidas;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/valida/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

VIII. Implementar e manter sistemas e processos de gerenciamento de acessos e autenticação seguros, garantindo que apenas usuários e sistemas autorizados possam acessar e modificar os ativos da organização;
IX. Desenvolver e manter planos de continuidade de negócios e recuperação de desastres, garantindo que a organização possa se recuperar rapidamente de interrupções ou incidentes de segurança;
X. Trabalhar em conjunto com a **DTI** e em conformidade, para garantir que as práticas e políticas de segurança sejam aplicadas de forma consistente em todo o ambiente computacional.

Artigo 18 - Gestor imediato:

XI. Compreender e cumprir as diretrizes estabelecidas nesta **OS,** garantindo que sua área de responsabilidade esteja em conformidade com as regras e procedimentos, bem como as **OS's** publicadas pela **DTI;**
XII. Incentivar e assegurar que os **USUÁRIOs** subordinados sigam as diretrizes estabelecidas nesta **PSIC,** bem como as **OS's** publicadas pela **DTI;**
XIII. Monitorar a conformidade com esta **OS** em sua área de responsabilidade, identificando e abordando eventuais desvios ou violações;
XIV. Colaborar com os responsáveis da **DTI** e outros gestores na resposta a incidentes de segurança, contribuindo para a continuidade dos negócios institucionais e a recuperação após eventos de segurança.
XV. Apropriar das revisões e atualizações das **OS's** publicas pela **DTI,** fornecendo feedback e informações sobre a eficácia das medidas de segurança e áreas de melhoria;
XVI. Estabelecer e manter um diálogo aberto e contínuo com a equipe da **SSI,** garantindo que as preocupações e questões de segurança sejam devidamente abordadas e resolvidas;
XVII. Garantir que as políticas e procedimentos de segurança da informação e cibernética sejam levados em consideração ao adotar novas tecnologias, ferramentas ou processos em sua área de responsabilidade.

Artigo 19 - USUÁRIO:

I. Aderir e seguir as práticas de segurança estabelecidas nesta política;
II. Reportar qualquer incidente de segurança ou violação da política à **DTI** e ao **gestor imediato.** Usar os canais de atendimento oficiais da **DTI;**
III. Conhecer e compreender a **PSIC** da organização, bem como as **OS's** publicadas pela **DTI,** quaisquer procedimentos e diretrizes relacionadas;
IV. Cumprir as regras, procedimentos e diretrizes estabelecidas esta **OS,** incluindo o uso adequado de sistemas, dispositivos e informações;
V. Participar de treinamentos e sessões de conscientização em segurança da informação e cibernética, mantendo-se atualizado sobre as melhores práticas e ameaças emergentes, quando houver;
VI. Proteger a confidencialidade, integridade e disponibilidade das informações e ativos de **TIC,** garantindo que sejam acessados, processados e armazenados de forma segura e conforme as diretrizes estabelecidas;
VII. Adotar medidas de segurança, como a criação e manutenção de senhas fortes, o bloqueio de dispositivos quando não estiverem em uso e a não divulgação de informações confidenciais a terceiros não autorizados;
VIII. Relatar imediatamente qualquer suspeita de incidente de segurança, violação ou atividade suspeita à **SSI;**

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

IX. Ser vigilante quanto a possíveis ameaças cibernéticas, como *phishing*, *malware* e outras formas de ataque, e **não clicar** em *links* ou anexos suspeitos;
X. Respeitar as políticas de uso aceitável de dispositivos e sistemas/aplicações da organização, evitando o acesso a *sites*, aplicativos ou conteúdos potencialmente perigosos ou não autorizados;
XI. Cumprir as políticas e diretrizes de segurança física da organização, como o uso de crachás de identificação, o controle de acesso a áreas restritas e a proteção de dispositivos e documentos quando fora do local de trabalho;
XII. Contribuir para a cultura de segurança da organização, incentivando colegas a adotarem práticas seguras e a agirem de acordo com as políticas e procedimentos de segurança da informação e cibernética.

CAPÍTULO VII – CONTROLES E MEDIDAS DE SEGURANÇA

Artigo 20 - Controle de Acesso:
I. Implementação de políticas de autenticação, autorização e monitoramento de acesso aos sistemas e informações;
II. Uso de sistemas de gerenciamento de identidade e acesso (IAM) para garantir a aplicação das políticas de acesso;
III. Implementação de mecanismos de autenticação multifator (MFA) para acessos críticos e de alto risco;
IV. Revisão periódica das permissões de acesso dos usuários e remoção de privilégios desnecessários;
V. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

Artigo 21 - Segurança em Redes e Sistemas/Aplicações:
I. Configuração e manutenção de *firewalls* para proteger a rede interna de ameaças externas;
II. Implementação de soluções de detecção e prevenção de intrusões (IDS/IPS) para identificar atividades suspeitas e bloquear ataques;
III. Instalação e atualização de soluções de cibersegurança em todos os dispositivos da organização;
IV. Aplicação de *patches* e atualizações de segurança em sistemas operacionais e aplicativos, seguindo um cronograma de manutenção preestabelecido;
V. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

Artigo 22 - Criptografia:
I. Uso de criptografia de ponta a ponta para proteger dados sensíveis em trânsito e em repouso;
II. Implementação de protocolos de comunicação seguros e padrões criptográficos reconhecidos pela indústria, como TLS, HTTPS e AES;
III. Gestão segura de chaves criptográficas, incluindo armazenamento, distribuição e rotação periódica de chaves;
IV. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

Artigo 23 - Gestão de Incidentes e Resposta a Incidentes:

I. Desenvolvimento e manutenção de um plano de resposta a incidentes de segurança, que contemple a identificação, contenção, erradicação, recuperação e comunicação dos incidentes;
II. Estabelecimento de um processo de notificação e reporte de incidentes de segurança, que envolva todas as partes interessadas e promova a ação rápida e efetiva na resolução de problemas;
III. Realização de análises pós-incidente para identificar as causas e implementar medidas preventivas;
IV. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

Artigo 24 - Segurança Física:

I. Implementação de medidas de segurança para proteger o acesso a áreas críticas e dispositivos físicos que armazenam ou processam informações, como câmeras de segurança, controle de acesso e alarmes;
II. Estabelecimento de diretrizes para a destruição segura de mídias físicas e dispositivos de armazenamento de informações;
III. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

Artigo 25 - Conscientização e Treinamento:

I. Desenvolvimento e implementação de programas de treinamento e conscientização sobre segurança da informação e cibernética para todos os colaboradores;
II. Atualização periódica dos treinamentos e avaliação da eficácia dos programas de conscientização;
III. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

CAPÍTULO VIII – POLÍTICAS E PROCEDIMENTOS ESPECÍFICOS

Artigo 26 - A **PSIC** deve ser complementada por políticas e procedimentos específicos que abordem áreas críticas de segurança, como:

§ 1º - Gestão de Senhas:

I. Definição de requisitos mínimos para a criação de senhas, como comprimento, complexidade e variedade de caracteres;
II. Implementação de políticas de expiração de senhas e proibição do reuso de senhas recentes;
III. Utilização de gerenciadores de senhas para armazenar e gerenciar credenciais de acesso de forma segura;
IV. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

§ 2º - Uso Aceitável de Recursos de **TIC:**

I. Definição de diretrizes claras sobre o uso adequado de recursos de **TIC,** incluindo dispositivos, redes, software e sistemas;
II. Estabelecimento de políticas de uso pessoal de recursos de **TIC,** delimitando os limites e as restrições aplicáveis;
III. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

§ 3º - Segurança em Dispositivos Móveis e Trabalho Remoto:

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

I. Desenvolvimento de políticas específicas para a segurança de dispositivos móveis, como smartphones, tablets e laptops;
II. Implementação de medidas de segurança adicionais para o trabalho remoto, como o uso de redes privadas virtuais (VPNs) e autenticação multifator (MFA);
III. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

§ 4º - Política de Backup e Recuperação de Desastres:
I. Definição de diretrizes para a realização de backups periódicos de dados e informações críticas;
II. Estabelecimento de um plano de recuperação de desastres que inclua procedimentos para restaurar sistemas e dados em caso de falhas ou incidentes de segurança;
III. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

§ 5º - Gestão de Riscos e Análise de Vulnerabilidades:
I. Implementação de um processo contínuo de identificação, avaliação e tratamento de riscos relacionados à segurança da informação e cibernética;
II. Realização periódica de testes de penetração e análise de vulnerabilidades para identificar e corrigir falhas nos sistemas e redes;
III. Observar e cumprir de forma integral as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

Artigo 27 - Monitoramento e Revisão:
I. Monitorar regularmente a conformidade com a **PSIC** e investigar violações ou incidentes;
II. Realizar auditorias internas e/ou externas para garantir a eficácia das medidas de segurança;
III. Atualizar a **PSIC** periodicamente para garantir sua relevância e efetividade em face das mudanças tecnológicas e ameaças emergentes.

Artigo 28 - Legislação e Regulamentação:
§ 1º - Esta **OS** deve estar em conformidade com as leis, regulamentações e normas aplicáveis, incluindo, mas não se limitando a, leis de privacidade e proteção de dados, leis de propriedade intelectual e normas de segurança da indústria, também em consonância com as **OS's** publicadas por esta **DTI** sobre políticas, procedimentos e gestão de **TIC.**

Artigo 29 - Implementação e Comunicação:
§ 1º - Esta **OS** deve ser comunicada a todos os **USUÁRIOs,** fornecedores, parceiros e terceiros envolvidos no uso, acesso, processamento, armazenamento ou transmissão de informações da organização;
§ 2º - A adesão à **PSIC** é mandatória para todos os **USUÁRIOs** e demais partes interessadas;
§ 3º - Violações da **PSIC** podem resultar em ações disciplinares, conforme as normas internas da organização e/ou as leis e regulamentações aplicáveis.

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

CAPÍTULO IX – DISPOSIÇÕES FINAIS

Artigo 30 - A **DTI** pode alterar o teor desta **OS** a qualquer momento, conforme a finalidade ou necessidade, tal qual para adequação e conformidade legal de disposição de lei ou norma que tenha força jurídica equivalente, cabendo ao **USUÁRIO** verificá-la sempre que efetuar o acesso aos sites e sistemas web.

§ 1º - Ocorrendo atualizações significativas neste documento e que demandem coleta de consentimento, a instituição notificará o **USUÁRIO** pelo e-mail fornecido.

Artigo 31 - Caso haja alguma dúvida sobre as condições estabelecidas nesta **OS** ou qualquer documento, o **USUÁRIO** pode entrar em contato por meio dos canais de atendimento supramencionados.

Artigo 32 - Caso alguma disposição desta **OS** seja considerada ilegal ou ilegítima por autoridade da localidade em que o **USUÁRIO** resida ou da sua conexão à rede local e Internet, as demais condições permanecerão em pleno vigor e efeito.

Artigo 33 - O **USUÁRIO** reconhece que toda comunicação realizada por e-mail (aos endereços por ele informados), SMS, aplicativos de comunicação instantânea ou qualquer outra forma digital, virtual e digital também são válidas como prova documental, sendo eficazes e suficientes para a divulgação de qualquer assunto que se refira aos serviços prestados pela **Fundação CASA/SP,** bem como às condições de sua prestação, ressalvadas as disposições expressamente diversas previstas nesta **OS.**

Artigo 34 - Esta **OS** e a relação decorrente das ações aqui compreendidas, assim como qualquer disputa que surja em virtude disto será regulada exclusivamente pela legislação brasileira.

Artigo 35 - Fica eleita a **Assessoria Jurídica (AJ)** da **Fundação CASA/SP** para dirimir qualquer questão envolvendo o presente documento, renunciando as partes a qualquer outro, por mais privilegiado que seja ou venha a ser.

Artigo 36 - Os casos de **não conformidade** serão avaliados pela **DTI** e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP.**

Artigo 37 - Esta **OS** entra em vigor na data de sua publicação.

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

CAPÍTULO X - VERSIONAMENTO

VERSÃO	DATA	AUTOR	DESCRIÇÃO
1.0	18/04/2023	Julio Cesar Signorini	**Versão Inicial**
1.1	16/05/2023	Alex Christy Rogatti, Ana Paula Ribeiro, Anna Carolina Oliveira Vello, Aurélio Olímpio de Souza, Fabiana Paes Rosa Mentone, Julio Cesar Signorini, Luciano Soares da Costa, Luiz Fernando Souza Gomes da Silva, Marcelo Pereira da Silva, Odenilson dos Santos Bonfim, Patricia Tsutsumi Dias, Paulo Cesar Crusca Junior, Rafael Mengel Souza, Rodrigo Braoios Vilhora e Sergio Aparecido Macário	**Revisões e Sugestões**
1.2	16/05/2023	AJ (Assessoria Jurídica), DGA (Diretoria de Gestão Administrativa), DTI (Divisão de Tecnologia da Informação), GP (Gabinete da Presidência), GTAJ (Grupo Técnico de Apoio Jurídico) e GTAT (Grupo Técnico de Apoio Tecnológico)	**Versão Final**

DTI, 16 de maio de 2023.

DOCUMENTO ASSINADO DIGITALMENTE

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/valida/r/573666AF-202306-0151584
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023