ORDEM DE SERVIÇO DTI Nº 011/2023

Dispõe sobre a política de resposta a incidentes cibernéticos 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 - Esta **OS** estabelece as ações, os procedimentos e as responsabilidades em caso de um incidente cibernético, com o objetivo de minimizar seus impactos e reduzir a probabilidade de recorrência no âmbito da **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;
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;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

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. **PRIC:** política de resposta a incidentes cibernéticos;
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. **incidente cibernético:** qualquer evento que possa comprometer a segurança da informação da organização;
XI. **ameaças cibernéticas:** ameaças que visam a segurança da informação da organização;
XII. **acesso:** ato ou permissão para ingressar, transitar, conhecer, consultar, manipular e utilizar os ativos de informação;
XIII. **controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;
XIV. ***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;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

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 – PRINCÍPIOS E OBJETIVOS

Artigo 5º - A **Fundação CASA/SP** reconhece a importância de proteger seus **ativos** e **recursos** de **TIC** contra ameaças cibernéticas. Esta **OS** estabelece as ações, os procedimentos e as responsabilidades em caso de um incidente cibernético, com o objetivo de minimizar seus impactos e reduzir a probabilidade de recorrência. Os princípios da **PRIC** incluem:

I. **Prontidão:** estar pronta para responder rapidamente a incidentes cibernéticos para minimizar seus impactos. Isso inclui ter equipes de segurança da informação e cibersegurança e **TIC** preparadas para lidar com incidentes;

II. **Detecção:** ter mecanismos de detecção de incidentes cibernéticos em seus **recursos de TIC** para identificar rapidamente quaisquer ameaças à segurança da informação e cibernética;

III. **Avaliação:** avaliar a gravidade dos incidentes cibernéticos e toma as medidas necessárias para lidar com eles;

IV. **Comunicação:** ter procedimentos claros para comunicar incidentes cibernéticos às partes interessadas, como gestores, **USUÁRIOs,** terceiros e autoridades regulatórias;

V. **Isolamento:** isolar rapidamente os **recursos de TIC** afetados por incidentes cibernéticos para evitar que o incidente se espalhe para outros;

VI. **Coleta de Evidências:** coletar evidências relevantes para investigar o incidente e identificar a causa raiz do incidente cibernético;

VII. **Remediação:** implementar as ações necessárias para remediar os **recursos de TIC** afetados pelo incidente cibernético e garantir que eles estejam seguros para uso novamente;

VIII. **Monitoramento:** monitorar continuamente os **recursos de TIC** para detectar novas ameaças cibernéticas e garantir que estejam seguros;

IX. **Revisão:** revisar regularmente a **PRIC** para garantir que ela esteja alinhada com as ameaças cibernéticas mais recentes e com as melhores práticas de segurança da informação;

X. **Treinamento:** fornecer treinamento regular à **SSI** sobre a **PRIC** e as melhores práticas de segurança da informação para garantir que eles estejam preparados para lidar com incidentes cibernéticos, se necessário.

Artigo 6º - Esses objetivos são alcançados por meio de uma abordagem estruturada e sistemática para detectar, avaliar e responder a incidentes cibernéticos. Esta **OS** estabelece os procedimentos e responsabilidades para lidar com incidentes cibernéticos e assegura que a **Fundação CASA/SP** esteja preparada para responder rapidamente a qualquer ameaça à segurança da informação e cibernética. A resposta eficaz a incidentes cibernéticos ajuda a minimizar os danos e reduz a probabilidade de recorrência de incidentes no futuro. A **PRIC** tem como objetivos:

I. Proteger os dados institucionais contra ameaças cibernéticas;

II. Minimizar o impacto de um incidente cibernético na organização e em seus **USUÁRIOs;**

III. Preservar a integridade dos **recursos de TIC** da instituição;

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

IV. Garantir a continuidade dos negócios institucionais;
V. Prevenir a recorrência de incidentes cibernéticos.

CAPÍTULO IV - DIRETRIZES

Artigo 7º - As diretrizes garantem uma abordagem estruturada e sistemática para detectar, avaliar e responder a incidentes cibernéticos, minimizando seus impactos e reduzindo a probabilidade de recorrência de incidentes no futuro. As diretrizes da **PRIC** são:

I. **Identificação e classificação de incidentes:** estabelecer um processo claro de identificação de incidentes cibernéticos, bem como uma escala de gravidade para classificar esses incidentes;
II. **Notificação e acionamento da equipe de segurança da informação:** definir quem deve ser notificado em caso de incidentes cibernéticos e os procedimentos para acionar a equipe de segurança da informação;
III. **Avaliação e investigação de incidentes:** estabelecer os procedimentos para avaliar a gravidade dos incidentes cibernéticos, coletar evidências e investigar a causa raiz do incidente;
IV. **Isolamento e contenção de incidentes:** estabelecer procedimentos para isolar rapidamente os sistemas afetados e conter o incidente para evitar que se espalhe para outros sistemas;
V. **Remediação e recuperação de sistemas:** estabelecer procedimentos para remediar os sistemas afetados pelo incidente cibernético e restaurar a normalidade das operações da organização;
VI. **Comunicação com as partes interessadas:** estabelecer procedimentos claros para comunicar o incidente às partes interessadas, como gestores, **USUÁRIOs,** terceiros e autoridades regulatórias;
VII. **Treinamento e conscientização:** incluir treinamento regular para à SSI sobre a **PRIC** e as melhores práticas de segurança da informação, se necessário;
VIII. **Revisão e atualização da política:** ser revisada e atualizada regularmente para garantir que ela esteja alinhada com as ameaças cibernéticas mais recentes e com as melhores práticas de segurança da informação;
IX. **Testes e exercícios de simulação de incidentes:** incluir testes e exercícios regulares de simulação de incidentes cibernéticos para avaliar a eficácia da política e garantir que a equipe esteja preparada para lidar com incidentes reais.

CAPÍTULO V - CLASSIFICAÇÃO DE INCIDENTES

Artigo 8º - A classificação de incidentes na **PRIC** é um processo importante que ajuda a avaliar a gravidade do incidente cibernético. A classificação direciona a priorização dos incidentes e determina a urgência da resposta. Também é fundamental para apontar o nível de comunicação necessária com as partes interessadas.

Artigo 9º - A classificação de incidentes geralmente envolve a avaliação de fatores como a natureza do incidente, a sensibilidade das informações afetadas, a quantidade de informações afetadas, o impacto no negócio institucional, a capacidade de recuperação e a probabilidade de recorrência. Uma escala de gravidade é usada para classificar os incidentes com base nesses fatores.

§ 1º - Incidente crítico: um incidente crítico é aquele que tem o potencial de causar danos graves a **Fundação CASA/SP,** como a perda de dados altamente sensíveis ou a interrupção das operações críticas. Seguem referências:

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

I. **Ataque de negação de serviço (DoS):** Um ataque de negação de serviço é um tipo de ataque cibernético que tem o objetivo de sobrecarregar um servidor ou rede com tráfego malicioso para torná-lo inoperável. Esse tipo de ataque pode afetar seriamente a disponibilidade de serviços críticos de negócios;
II. ***Ransomware:*** O *ransomware* é um tipo de malware que criptografa os arquivos do usuário e exige um resgate para desbloqueá-los. Um ataque de *ransomware* pode resultar na perda de dados importantes e causar um impacto financeiro significativo na organização;
III. **Roubo de dados:** O roubo de dados ocorre quando um invasor obtém acesso não autorizado a dados confidenciais da organização, como informações pessoais ou dados financeiros. Isso pode levar a violações de privacidade e a possíveis ações legais;
IV. **Invasão de rede:** Uma invasão de rede ocorre quando um invasor obtém acesso não autorizado a uma rede de computadores. Isso pode permitir que o invasor roube informações confidenciais, danifique sistemas e cause interrupções nas operações de negócios;
V. **Fraude financeira:** A fraude financeira ocorre quando um invasor usa informações roubadas para fazer transações fraudulentas em nome da organização. Isso pode levar a perdas financeiras significativas e afetar a reputação da organização;
VI. **Roubo de propriedade intelectual:** O roubo de propriedade intelectual ocorre quando um invasor rouba informações confidenciais da organização, como projetos de pesquisa e desenvolvimento ou segredos comerciais. Isso pode afetar a competitividade da organização e resultar em perda de receita;
VII. **Violação de segurança física:** Uma violação de segurança física ocorre quando um invasor obtém acesso não autorizado a um local de negócios ou a um dispositivo de armazenamento físico, como um disco rígido ou um servidor. Isso pode permitir que o invasor roube informações confidenciais ou danifique sistemas/aplicações;
VIII. **Ataque de *malware* avançado persistente (APTs):** Um ataque de *malware* avançado persistente é um tipo de ataque cibernético que tem o objetivo de se infiltrar em um sistema de computador e permanecer oculto por um longo período. Os APTs podem permitir que os invasores acessem informações confidenciais, roube propriedade intelectual e cause danos ao sistema;
IX. **Ataque de engenharia social:** Um ataque de engenharia social é um tipo de ataque cibernético que usa técnicas de manipulação psicológica para convencer os usuários a divulgar informações confidenciais ou a realizar ações prejudiciais. Isso pode levar à violação de dados e outras violações de segurança;
X. **Ataque de insider:** Um ataque de *insider* ocorre quando um funcionário ou outro indivíduo com acesso autorizado aos sistemas de uma organização usa esse acesso para realizar atividades maliciosas. Isso pode incluir o roubo de informações confidenciais, a realização de fraudes financeiras e outras atividades prejudiciais;
XI. **Ataque de *phishing*:** Um ataque de *phishing* é um tipo de ataque cibernético que usa e-mails fraudulentos ou sites da web para enganar os usuários a divulgar informações confidenciais ou realizar ações prejudiciais. Isso pode levar à violação de dados e outras violações de segurança;
XII. **Ataque de *malware* destrutivo:** Um ataque de *malware* destrutivo é um tipo de ataque cibernético que tem o objetivo de danificar ou destruir sistemas

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

de computador ou redes. Isso pode causar uma interrupção significativa nas operações de negócios e resultar em perda de dados e danos financeiros.

§ 2º - Incidente grave: um incidente grave é aquele que tem o potencial de causar danos significativos, como a perda de dados sensíveis ou a interrupção das operações importantes. Seguem referências:

I. **Vírus de computador:** Um vírus de computador é um tipo de malware que se espalha através de arquivos infectados e pode causar danos aos sistemas de computador. Isso pode resultar em perda de dados, interrupções nas operações de negócios e outros impactos;

II. **Ataques de engenharia social em massa:** Os ataques de engenharia social em massa são ataques que visam várias pessoas na organização, geralmente por meio de e-mails fraudulentos ou sites da web. Eles podem levar à violação de dados e outras violações de segurança;

III. **Invasões de rede limitadas:** Uma invasão de rede limitada ocorre quando um invasor obtém acesso não autorizado a uma parte limitada da rede de computadores da organização. Isso pode permitir que o invasor roube informações confidenciais e cause danos aos sistemas;

IV. **Roubo ou perda de dispositivos móveis:** O roubo ou a perda de dispositivos móveis, como laptops, smartphones e tablets, podem resultar em perda de dados e outros impactos financeiros na organização;

V. **Incidentes de segurança em sites de redes sociais:** Os incidentes de segurança em sites de redes sociais podem levar à violação de dados e outras violações de segurança. Eles ocorrem quando informações confidenciais são expostas devido a vulnerabilidades nos sistemas de segurança da rede social;

VI. **Ataques de *phishing* direcionados:** Os ataques de *phishing* direcionados são ataques que visam indivíduos específicos na organização, geralmente usando informações pessoais ou profissionais para convencer o destinatário a divulgar informações confidenciais ou realizar ações prejudiciais;

VII. **Acesso não autorizado a sistemas:** O acesso não autorizado a sistemas ocorre quando um indivíduo obtém acesso não autorizado a um sistema de computador ou rede. Isso pode permitir que o invasor roube informações confidenciais, danifique sistemas e cause interrupções nas operações de negócios;

VIII. **Ataques de *ransomware* limitados:** Um ataque de *ransomware* limitado é um ataque cibernético que criptografa os arquivos do usuário em uma parte limitada da rede da organização e exige um resgate para desbloqueá-los. Isso pode resultar na perda de dados importantes e causar um impacto financeiro significativo na organização;

IX. **Violação de dados:** A violação de dados ocorre quando informações confidenciais da organização são acessadas, expostas ou roubadas por um invasor. Isso pode levar à perda de informações financeiras e pessoais dos clientes, resultando em impactos financeiros e legais significativos para a organização;

X. **Violação de privacidade:** A violação de privacidade ocorre quando informações pessoais dos clientes são acessadas, expostas ou roubadas por um invasor. Isso pode resultar em violações de privacidade, danos à imagem da organização e ações legais.

§ 3º - Incidente moderado: um incidente moderado é aquele que tem o potencial de causar danos menores, como a perda de dados menos sensíveis ou a interrupção de operações menos críticas. Seguem referências:

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

I. **Spam:** O spam é uma forma de comunicação eletrônica não solicitada, geralmente em massa, que pode ser irritante para os usuários e consumir recursos do sistema;
II. **Ataques de força bruta:** Um ataque de força bruta é um tipo de ataque cibernético que usa uma tentativa de várias combinações de nomes de usuário e senhas para obter acesso a um sistema de computador. Isso pode resultar em tentativas frustradas de acesso e consumir recursos do sistema;
III. ***Phishing* genérico:** O *phishing* genérico é um tipo de ataque cibernético que usa e-mails fraudulentos ou sites da web para enganar os usuários a divulgar informações confidenciais ou realizar ações prejudiciais. Isso pode levar à violação de dados e outras violações de segurança;
IV. ***Malware:*** O *malware* é um tipo de software malicioso que é projetado para danificar ou controlar um sistema de computador. Isso pode resultar em perda de dados, interrupções nas operações de negócios e outros impactos;
V. **Ataques de *script*:** Os ataques de *script* são ataques que exploram vulnerabilidades em sites da web para inserir *scripts* maliciosos. Isso pode resultar em roubo de dados, interrupções nas operações de negócios e outros impactos;
VI. **Problemas de autenticação:** Os problemas de autenticação ocorrem quando os usuários têm problemas para acessar sistemas de computador devido a problemas com senhas ou outros problemas de autenticação. Isso pode resultar em interrupções nas operações de negócios e outros impactos;
VII. **Ataques de *spam*:** Um ataque de *spam* é um tipo de ataque cibernético que usa mensagens de spam para inundar uma rede ou sistema de computador com tráfego indesejado. Isso pode consumir recursos do sistema e reduzir a eficiência das operações de negócios;
VIII. **Ataques de injeção SQL:** Um ataque de injeção SQL é um tipo de ataque cibernético que explora vulnerabilidades em sites da web para inserir comandos SQL maliciosos. Isso pode resultar em roubo de dados, interrupções nas operações de negócios e outros impactos;
IX. **Ataques de *malware* em massa:** Os ataques de *malware* em massa são ataques que visam várias pessoas na organização, geralmente por meio de e-mails fraudulentos ou sites da web. Eles podem levar à violação de dados e outras violações de segurança;
X. **Ataques de *spam* em massa:** Os ataques de *spam* em massa são ataques que visam inundar uma rede ou sistema de computador com tráfego indesejado. Isso pode consumir recursos do sistema e reduzir a eficiência das operações de negócios;
XI. **Ataques de *sniffing*:** Um ataque de *sniffing* é um tipo de ataque cibernético que intercepta o tráfego de rede não criptografado para obter informações confidenciais. Isso pode resultar em roubo de dados e outras violações de segurança;
XII. **Ataques de negação de serviço limitados:** Um ataque de negação de serviço limitado é um tipo de ataque cibernético que visa interromper temporariamente a disponibilidade de um serviço ou sistema de computador. Isso pode afetar a eficiência das operações de negócios e resultar em perda de produtividade.

§ 3º - Incidente baixo: um incidente baixo é aquele que tem o potencial de causar danos mínimos, como a perda de dados de pouco valor ou a interrupção de operações não críticas. Seguem referências:

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

I. **Proteger Acesso não autorizado a uma área restrita:** O acesso não autorizado a uma área restrita ocorre quando alguém entra em uma área que é considerada restrita ou fora dos limites para a pessoa. Isso pode ser uma violação de política da empresa, mas geralmente tem pouco impacto na organização;
II. **E-mails não solicitados:** Os e-mails não solicitados são e-mails que são enviados sem consentimento do destinatário. Isso pode ser irritante para os usuários, mas geralmente tem pouco impacto na organização;
III. **Erros de configuração do sistema:** Os erros de configuração do sistema são erros de configuração que ocorrem em sistemas de computador ou dispositivos de rede. Isso pode causar problemas temporários, mas geralmente não tem um impacto significativo na organização;
IV. **Tentativas de login fracassadas:** As tentativas de login fracassadas ocorrem quando um usuário tenta fazer login em um sistema de computador sem sucesso. Isso pode ser uma indicação de um ataque de força bruta, mas geralmente não tem um impacto significativo na organização;
V. **Problemas de compatibilidade do navegador:** Os problemas de compatibilidade do navegador ocorrem quando o site da web não funciona corretamente em um navegador específico. Isso pode ser frustrante para os usuários, mas geralmente tem pouco impacto na organização;
VI. **Atualizações de *software*:** As atualizações de *software* são atualizações de rotina para sistemas de computador ou dispositivos de rede. Isso pode ser necessário para manter os sistemas seguros e funcionando corretamente, mas geralmente não tem um impacto significativo na organização;
VII. **Problemas de conexão com a Internet:** Os problemas de conexão com a Internet podem ser causados por problemas técnicos em sistemas de computador ou dispositivos de rede. Isso pode causar interrupções temporárias nas operações de negócios, mas geralmente tem pouco impacto na organização;
VIII. **Problemas com software de produtividade:** Os problemas com software de produtividade ocorrem quando o software usado para fins de produtividade, como processamento de texto ou planilhas, apresenta problemas técnicos. Isso pode ser frustrante para os usuários, mas geralmente tem pouco impacto na organização;
IX. **Problemas de instalação de software:** Os problemas de instalação de software ocorrem quando o software não pode ser instalado corretamente em um sistema de computador. Isso pode ser causado por problemas técnicos ou erros do usuário, mas geralmente tem pouco impacto na organização;
X. **Problemas de hardware:** Os problemas de hardware ocorrem quando o hardware de um sistema de computador ou dispositivo de rede apresenta problemas técnicos. Isso pode causar interrupções temporárias nas operações de negócios, mas geralmente tem pouco impacto na organização;
XI. **Atualizações de segurança:** As atualizações de segurança são atualizações para sistemas de computador ou dispositivos de rede que são necessárias para manter os sistemas seguros. Isso pode ser necessário para manter a integridade dos sistemas de computador, mas geralmente tem pouco impacto na organização;
XII. **Problemas com senhas:** Os problemas com senhas ocorrem quando os usuários esquecem suas senhas ou têm problemas para acessar um sistema de computador devido a problemas com senhas. Isso pode ser uma violação de política da empresa, mas geralmente tem pouco impacto na organização.

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

CAPÍTULO VI - PROCEDIMENTOS DE RESPOSTA

Artigo 10 - Os procedimentos de resposta nesta **OS** estabelecem os passos específicos que a **SSI, GSINF** e **GTAT** devem seguir para lidar com incidentes cibernéticos. Esses procedimentos são baseados na classificação do incidente e podem variar dependendo da natureza do incidente.

Artigo 11 - Esses procedimentos de resposta garantem uma abordagem sistemática e estruturada para lidar com incidentes cibernéticos, minimizando os impactos e reduzindo a probabilidade de recorrência. Os procedimentos de resposta incluem as seguintes etapas:

I. **Notificação:** notificar do incidente cibernético o mais rápido possível. A notificação pode vir de vários canais, como alertas de segurança, relatórios de usuários ou sistemas/aplicações de detecção de intrusão;
II. **Avaliação:** avaliar a gravidade do incidente cibernético e determinar o tipo de incidente. Isso envolve coletar informações sobre a natureza do incidente, os **recursos de TIC** afetados, o escopo do impacto e a causa raiz do incidente;
III. **Isolamento:** isolar o **recurso de TIC** afetado pelo incidente para evitar que o incidente se espalhe para outras plataformas. Isso pode envolver a desconexão, ou desligamento ou outra ação;
IV. **Coleta de evidências:** coletar evidências relevantes para investigar o incidente e determinar a causa raiz. Isso pode incluir *logs* de sistema/aplicações, *backups,* registros de atividades de **USUÁRIOs** e outros dados relevantes;
V. **Análise e investigação:** analisar as evidências coletadas e investigar a causa raiz do incidente. Isso envolve determinar como o incidente ocorreu, identificar as vulnerabilidades exploradas e avaliar o escopo do impacto;
VI. **Remediação:** implementar as ações necessárias para remediar os **recursos de TIC** afetados pelo incidente. Isso pode incluir a aplicação de *patches* de segurança, atualizações de *software,* reinstalação do sistema operacional ou restauração de *backup;*
VII. **Monitoramento e revisão:** monitorar continuamente os **recursos de TIC** para detectar quaisquer sinais de atividade maliciosa e revisar regularmente a **PRIC** para garantir que ela esteja alinhada com as ameaças mais recentes;
VIII. **Comunicação:** comunicar o incidente às partes interessadas de acordo com os procedimentos estabelecidos e a extensão da comunicação necessária e o conteúdo da mensagem;
IX. **Restauração das operações:** trabalhar para restaurar a normalidade das operações da instituição. Isso envolve garantir que os **recursos de TIC** estejam seguros para uso novamente e retomem suas operações normais.

CÁPITULO VII - DOS RESPONSÁVEIS E EXECUÇÕES

Artigo 12 - Os profissionais da **DTI** são responsáveis pela análise, execução, segurança e integridade dos serviços de **TIC** disponíveis no ambiente computacional da instituição:

I. garantir a aplicação das diretrizes desta **OS** na área de **TIC** da instituição;
II. gerir os processos de gestão e governança dos **recursos de TIC.**

Artigo 13 - No âmbito da presente **OS,** as responsabilidades na **PRIC** definem quem é responsável por executar cada etapa do processo de resposta a incidentes. As responsabilidades devem ser claras e bem definidas para garantir que a equipe esteja preparada para lidar com incidentes cibernéticos de maneira eficaz. Incluem:

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

I. **SSI:** é responsável por responder a incidentes cibernéticos e implementar os procedimentos estabelecidos na política de resposta a incidentes cibernéticos. Eles são responsáveis pela avaliação, investigação e remediação de incidentes cibernéticos, por implementar as ações necessárias para remediar os **recursos de TIC** afetados pelo incidente cibernético, para uso novamente e a retomada de suas operações normais;
II. **GSINF:** é responsável por garantir que a organização esteja preparada para responder a incidentes cibernéticos, por fornecer os recursos necessários para implementar a política de resposta a incidentes cibernéticos, por revisar e aprovar a **PRIC** junto com a **DTI** e garantir que ela esteja alinhada com as ameaças cibernéticas mais recentes e com as melhores práticas de segurança da informação;
III. **GTAT:** é responsável por detectar incidentes cibernéticos por meio da monitorização de sistemas e aplicativos, testar a eficácia da **PRIC** simulando incidentes para avaliação, por isolar sistemas/aplicações afetados, por bloquear o acesso de invasores e garantir que voltem a operar normalmente o mais rápido possível e por trabalhar em estreita colaboração com a **DTI** para identificar vulnerabilidades e mitigá-las antes que sejam exploradas por invasores;
IV. **Gestor imediato/USUÁRIOs:** têm a responsabilidade de relatar incidentes cibernéticos ao **gestor imediato** e a **DTI** assim que os detectarem, por meio dos canais oficiais de atendimento. Também devem seguir as **OS's** sobre políticas, procedimentos e gestão de **TIC** publicadas pela **DTI** e reportar quaisquer atividades suspeitas.

CÁPITULO VIII - COMUNICAÇÃO

Artigo 14 - A comunicação de incidentes é uma parte importante desta **OS.** Ela estabelece os procedimentos para comunicar o incidente cibernético às partes interessadas, como gestores, **USUÁRIOs,** terceiros e autoridades regulatórias. Colabora efetivamente com minimização os danos e mantem estabilidade do ambiente computacional. Etapas envolvidas na comunicação de incidentes incluem:

I. **Identificação das partes interessadas:** identificar as partes interessadas que precisam ser notificadas sobre o incidente cibernético. Isso pode incluir gestores, **USUÁRIOs,** terceiros e autoridades regulatórias;
II. **Determinação da extensão da comunicação:** determinar a extensão da comunicação necessária para cada parte interessada. Isso pode incluir o tipo de informação que deve ser comunicada e a frequência da comunicação;
III. **Preparação da mensagem:** preparar uma mensagem clara e precisa que explique o incidente cibernético e suas implicações. Também incluir informações sobre as medidas tomadas para remediar o incidente e as medidas de precaução tomadas para evitar a recorrência;
IV. **Escolha do canal de comunicação:** serão utilizados os canais oficiais de atendimento da **DTI;**
V. **Treinamento:** promover a cultura da segurança da informação regularmente na **PRIC** e nas melhores práticas de comunicação de incidentes.

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

CAPÍTULO IX – DISPOSIÇÕES FINAIS

Artigo 16 - 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.

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

Artigo 17 - 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 18 - 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 19 - 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 20 - 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 21 - 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 22 - Violações desta **OS** estarão sujeitas a ações disciplinares previstas nas Portarias Administrativas da **Fundação CASA/SP** específicas, e podem resultar em sanções e às penas previstas em lei.

§ 1º - A instituição adotará ações em consonância com as suas regulamentações, as leis federais, estaduais, municipais e às normas recomendadas pela **ABNT - Associação Brasileira de Normas Técnicas.**

Artigo 23 - Os casos de **não conformidade** serão avaliados pela **DTI** e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP.**

Artigo 24 - Esta **OS** entra em vigor na data de sua publicação.

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023

CAPÍTULO X - VERSIONAMENTO

VERSÃO	DATA	AUTOR	DESCRIÇÃO
1.0	19/04/2023	Julio Cesar Signorini	**Versão Inicial**
1.1	31/05/2023	Alex Christy Rogatti, Ana Paula Ribeiro, Aurélio Olímpio de Souza, 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	31/05/2023	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, 02 de junho de 2023.

DOCUMENTO ASSINADO DIGITALMENTE

ASSINADO DIGITALMENTE https://sistemas.fundacaocasa.sp.gov.br/e-casa/validar/12EA796F-202306-0151698
JULIO CESAR SIGNORINI 02/06/2023 | AURELIO OLIMPIO DE SOUZA 02/06/2023