Cartilha de Segurança da Informação

PNUD

CNJ CONSELHO NACIONAL DE JUSTIÇA

SÉRIE FAZENDO JUSTIÇA

Cartilha de Segurança da Informação

BRASÍLIA, 2023

CNJ (Conselho Nacional de Justiça)

Presidente: Ministro Luís Roberto Barroso
Corregedor Nacional de Justiça: Ministro Luis Felipe Salomão

Conselheiros
Ministro Luiz Philippe Vieira de Mello Filho
Mauro Pereira Martins
Richard Pae Kim
Salise Monteiro Sanchotene
Marcio Luiz Coelho de Freitas
Jane Granzoto Torres da Silva
Giovanni Olsson
João Paulo Santos Schoucair
Marcos Vinícius Jardim Rodrigues
Marcello Terto e Silva
Luiz Fernando Bandeira de Mello Filho

Secretária-Geral: Adriana Alves dos Santos Cruz
Secretário Especial de Programas, Pesquisas e Gestão Estratégica: Frederico Montedonio Rego
Diretor-Geral: Johaness Eck

Supervisor DMF/CNJ: Conselheiro Mauro Pereira Martins
Juiz Auxiliar da Presidência e Coordenador DMF/CNJ: Luís Geraldo Sant'Ana Lanfredi
Juiz Auxiliar da Presidência – DMF/CNJ: Edinaldo César Santos Junior
Juiz Auxiliar da Presidência – DMF/CNJ: Gabriel da Silveira Matos
Juiz Auxiliar da Presidência – DMF/CNJ: João Felipe Menezes Lopes
Juiz Auxiliar da Presidência – DMF/CNJ: Jônatas dos Santos Andrade
Juíza Auxiliar da Presidência – DMF/CNJ: Katia Herminia Martins L. Roncada
Diretora Executiva DMF/CNJ: Renata Chiarinelli Laurino
Chefe de Gabinete DMF/CNJ: Carolina Castelo Branco Cooper

PNUD BRASIL (Programa das Nações Unidas para o Desenvolvimento)

Representante-Residente: Claudio Providas
Representante-Residente Adjunto: Carlos Arboleda
Representante-Residente Assistente e Coordenadora da Área Programática: Maristela Baioni
Coordenadora da Unidade de Paz e Governança: Moema Freire
Coordenadora-Geral (equipe técnica): Valdirene Daufemback
Coordenador-Adjunto (equipe técnica): Talles Andrade de Souza
Coordenadora Eixo 4 (equipe técnica): Alexander Cambraia Nascimento Vaz

Coordenação Série Fazendo Justiça: Luís Geraldo Sant'Ana Lanfredi; Renata Chiarinelli Laurino; Carolina Cooper; Valdirene Daufemback; Talles Andrade de Souza; Débora Neto Zampier
Elaboração de conteúdo: João Batista Martins
Supervisão Geral: Alexander Cambraia Nascimento Vaz
Revisão: Tikinet Edição
Fotos: Freepik, Unsplash

SUMÁRIO

CONTEXTUALIZAÇÃO

Em decorrência da necessidade diária de acesso aos dispositivos móveis e a computadores e da consequente exposição aos diversos tipos de fragilidades e vulnerabilidades existentes no mundo virtual, devemos incentivar uma cultura de segurança da informação que diminua os riscos aos quais os(as) usuários(as) são expostos.

Assim, a segurança da informação permanece como uma área que permeia todas as demais atividades no Programa Fazendo Justiça, contribuindo para a continuidade das ações necessárias para a execução das tarefas.

Nesse escopo, esta cartilha visa elevar o nível de conscientização do(a) usuário(a) no que tange ao modo de utilização dos diversos recursos virtuais.

Objetivos da cartilha

- **Conceituar o termo segurança da informação e suas implicações;**
- **Relacionar dados resultantes de ameaças encontradas no mundo virtual e boas práticas para redução de danos.**

Dada a importância do tema e a existência da cartilha, viu-se que a contribuição será efetiva para o aumento/elevação do nível de conhecimento do(a) usuário(a) sobre a utilização dos recursos para acesso ao Sistema Eletrônico de Execução Unificado (SEEU), bem como outros sistemas relacionados, corroborando, ainda, a ideia de que se tem que 95% das violações de segurança cibernética são causadas por erro humano (WORLD ECONOMIC FORUM, 2020).

É na perspectiva deste esforço nacional que se apresenta o Manual de inspeções judiciais em programas e serviços de atendimento socioeducativo: meio aberto que propõe estratégias de abordagens para todas as etapas das inspeções, desde a sua preparação até encaminhamentos posteriores, Para tanto, apresenta o desenho da política socioeducativa no que tange às medidas em meio aberto, de forma a apontar os principais entes e órgãos envolvidos na sua execução e alguns conceitos centrais para o seu funcionamento.

Versões da cartilha

Data	Versão	Descrição	Autoria
06/09/2023	1.0	Cartilha de Segurança da Informação – FAJUS	NIT – Eixo 4/Segurança

1. SEGURANÇA DA INFORMAÇÃO

1.1. Definição

De acordo com a ISO/IEC 27000:2018, a segurança da informação garante a confidencialidade, disponibilidade e integridade das informações, com a aplicação de controles apropriados cujo objetivo é garantir o sucesso e a continuidade do negócio, minimizando as consequências de incidentes de segurança da informação (ISO 27.000, 2018).

A segurança da informação, para garantir a tríade dos atributos acima mencionados, deve ser capaz de aplicar controles para mitigar as vulnerabilidades que eventualmente possam ser exploradas por ameaças que se concretizam em ataques, resultando em riscos com impactos relevantes (VAKHTER e colab, 2021).

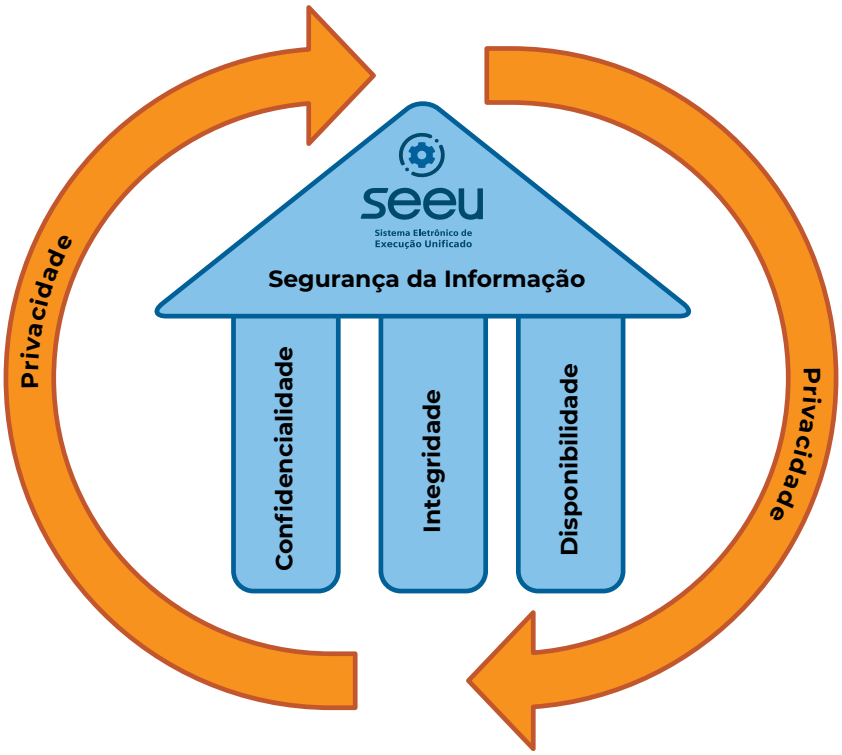
Ademais, os sistemas de Tecnologia da Informação (TI) devem se alinhar ao preconizado na ABNT NBR ISO/IEC 27.701, que foca na gestão da privacidade da informação, e ABNT NBR ISO/IEC 29100:2020 – Técnicas de segurança – Estrutura de Privacidade, que define as características da privacidade em sistemas de TI (ISO ABNT 29100:2020, 2020).

Dessa forma, a segurança da informação é um dos 11 princípios de privacidade enunciados pela ABNT NBR ISO/IEC 29100. O conceito “princípios de privacidade” refere-se ao conjunto de valores compartilhados que governam a proteção de privacidade de dados pessoais (DPs), quando tratados em sistemas de tecnologia da informação e comunicação (ISO ABNT 29100:2020, 2020).

Assim, o aumento da conscientização em segurança da informação, objetivo desta cartilha, é um eficiente controle para a mitigação das vulnerabilidades existentes nos sistemas informatizados, pois trata o elo mais frágil: o(a) usuário(a) (SASSE e colab., 2001)

1.2. Termos associados e suas implicações

Em função dos termos existentes na definição anterior, há, também, necessidade de conceituá-los.



1.2.1. Confidencialidade

Refere-se à propriedade de um sistema de não permitir que as informações sejam disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados (ISO 27.000, 2018). Assim, a confidencialidade visa preservar o acesso do conteúdo aos(às) usuários(as) explicitamente definidos(as).

1.2.2. Disponibilidade

Característica de um sistema que possibilita o acesso à informação sempre que o(a) usuário(a) necessitar (ISO 27.000, 2018). Sob esse enfoque, a disponibilidade visa manter as informações sempre acessíveis, por intermédio das aplicações e sistemas operacionais.

1.2.3. Integridade

Essa particularidade do sistema confere precisão e completude à informação, evitando que conteúdo informacional seja alterado ou corrompido. O backup e os métodos criptográficos contribuem para a manutenção da integridade das informações, evitando sua destruição e alteração, respectivamente (ISO 27.000, 2018)..

1.2.4. Privacidade

A Lei Geral de Proteção de Dados (LGPD), identificada como Lei n. 13.709/2018, aborda o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica, de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais (GOVERNO FEDERAL DO BRASIL, 2018).

Conforme a ABNT NBR ISO/IEC 29100:2020, a privacidade dos DPs deve ser garantida em sistemas informatizados, com ênfase nos dados pessoais sensíveis cuja natureza se relaciona à esfera mais íntima do titular dos DPs ou que podem ter um impacto significativo sobre ele.

Por isso, os sistemas informatizados devem implementar soluções técnicas que garantam a privacidade dos DPs existentes em suas bases de dados.

1.2.5. Controles

Os controles são ações realizadas para a mitigação dos riscos. Cada atividade desempenhada pela organização tem um risco associado, denominado risco inerente, que após a aplicação de controles poderá ter a probabilidade e/ou o impacto diminuídos, sendo denominado, então, risco residual (ABNT NBR ISO/IEC 27005, 2019).

1.2.6. Ameaças

Uma ameaça tem o potencial de comprometer ativos, tais como: informações, processos e sistemas e, por isso, também as organizações. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Convém que tanto as fontes das ameaças acidentais quanto das intencionais sejam identificadas. Uma ameaça pode surgir de dentro ou de fora da organização e pode se concretizar em um ataque (ABNT NBR ISO/IEC 27005, 2019).

1.2.7. Vulnerabilidades

Segundo a ISO/IEC 27000:2018, vulnerabilidade é a fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças (ISO 27.000, 2018). Sendo assim, as vulnerabilidades devem ser mapeadas e mitigadas para manter as aplicações e os sistemas seguros.

1.2.8. Risco

Risco é o efeito da incerteza no alcance dos objetivos. Um efeito é um desvio em relação ao esperado, podendo ser positivo e/ou negativo. O risco em segurança da informação é muitas vezes expresso em termos de uma combinação de consequências de um evento e a probabilidade de ocorrência.

O risco de segurança da informação está associado ao potencial de que as ameaças possam explorar as vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, consequentemente, causar dano a uma organização ou sistema (ABNT NBR ISO/IEC 27005, 2019).

1.3. Escopo da cartilha

Dentre os princípios que regem a Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), a Resolução n. 396, de 7 de junho de 2021, estabelece a educação e a inovação como alicerces fundamentais para o fomento da cultura em segurança cibernética, bem como define como um dos seus principais objetivos o fortalecimento da cultura de segurança cibernética no âmbito do Poder Judiciário (CNJ, 2021).

Assim sendo, esta cartilha visa alinhar-se ao preconizado na Resolução n. 396, disponibilizando conteúdo didático com boas práticas de segurança da informação (UC BERKELEY, 2023)

2. BOAS PRÁTICAS

2.1. Realização de backup

Backup é uma segunda cópia (ou mais) de seus arquivos digitais e pode protegê-lo contra a perda de dados. Você pode acessar esse backup caso seu dispositivo ou dados fiquem inacessíveis, destruídos ou danificados. A perda de dados pode ocorrer de várias maneiras: uma falha de computador ou hardware, um dispositivo perdido ou roubado, corrupção de dados ou malware (código malicioso) que os criptografa e os mantém inacessíveis. Por isso, jamais deixe de realizar seu backup para preservar suas valiosas informações.

2.1.1. Opções de backup

- Os serviços de sincronização em nuvem fazem backup de arquivos individuais, e não incluem aplicativos ou programas. Google Drive e OneDrive são exemplos de serviços de cópias sincronizadas de dados; e
- Os backups tradicionais se utilizam periodicamente de disco rígido externo de acordo com as modificações realizadas .

2.2. Trabalho remoto com segurança

2.2.1. Mantenha os dados de trabalho nos computadores de trabalho

Utilizar um dispositivo de propriedade pessoal para a realização de atividades de negócios pode aumentar a probabilidade de ataques. Caso não seja possível ter um computador de trabalho para usar em casa, siga estas práticas descritas a seguir, que são válidas também para os equipamentos corporativos:

Atualização e correção

Atualize tudo em seus dispositivos, incluindo sistemas operacionais, navegadores da web e aplicativos. Os invasores podem explorar vulnerabilidades em versões antigas de software.

Use um software antimalware e um firewall

Instale um software antimalware (*antispyware*, antivírus) e habilite um firewall (sistema de segurança que restringe o tráfego para proteção de acesso) em seu(s) dispositivo(s).

Evite redes sem fio pública e use a VPN da instituição

Não use rede sem fio (wireless) pública (hotéis, restaurantes, aeroportos, entre outros locais similares) ao fazer login nos sistemas da instituição ou fazer trabalhos associados. Em vez disso, use a rede virtual privada (VPN) ou seu telefone como um ponto de acesso pessoal.

Viagem com notebook

- Acomode o equipamento de forma segura, como em mochilas ou maletas transportadas como bagagem de mão;
- Mantenha-o sempre em seu campo de visão;
- Ao transportá-lo em automóveis, acomode-o em local não visível externamente e seguro contra furto;
- Em caso de roubo ou furto, registre boletim de ocorrência (BO) junto às autoridades policiais locais e notifique imediatamente a chefia.

Além dos procedimentos listados, mantenha ativado o mecanismo de bloqueio automático de tela por inatividade e bloqueie a tela sempre que se ausentar.

2.3. Celulares

Devido aos diversos sistemas acessíveis pelo aparelho celular, bem como às várias informações existentes nesses dispositivos móveis, em caso de roubo, furto ou extravio, deve-se registrar um BO na delegacia de polícia de sua cidade ou via internet, caso o local possua essa alternativa, bem como entrar em contato com a prestadora do serviço de telefonia para solicitar o bloqueio da linha (*simcard*) e do aparelho celular. O bloqueio da linha impede que seja utilizada em outro aparelho celular, gerando custos, e o bloqueio do aparelho celular impossibilita que o dispositivo acesse redes móveis brasileiras. Esse bloqueio é feito por meio da inclusão do *International Mobile Equipment Identity* (IMEI – Identificação Internacional de Equipamento Móvel) do aparelho celular no Cadastro de Estações Móveis Impedidas (CEMI), que é replicado para todas as prestadoras nacionais (GOVERNO FEDERAL DO BRASIL, 2023). Para saber seu número IMEI, acione a tela de discagem do celular e digite *#06#. O IMEI será exibido

imediatamente. Essa alternativa funciona em todos os aparelhos GSM, independentemente do sistema operacional ou fabricante.

Ademais, assim que possível, comunique o fato à sua chefia imediata e aos grupos de trabalho com os quais realiza suas atividades.

Por fim, em aparelhos celulares modernos, tem-se o recurso para a localização e o bloqueio remoto do equipamento, permitindo, ainda, que o(a) usuário(a) apague os dados armazenados, mantendo sua privacidade (GOVERNO FEDERAL DO BRASIL, 2023). Para isso, acesse os links abaixo:

Para dispositivos Android: https://www.android.com/find

Para dispositivos iOS: https://www.icloud.com/find

2.4. Seja cauteloso: *phishing*

Ataques phishing crescem diariamente e ainda conseguem elevado percentual de êxito. Por isso, a mitigação desse tipo de ataque requer principalmente a percepção do(a) usuário(a) em relação às informações e demandas oriundas de e-mails.

Mas o que é phishing? Trata-se de uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais como nome de usuário, senha e detalhes do cartão de crédito, por exemplo. Para cometer as fraudes eletrônicas, os criminosos utilizam mensagens eletrônicas aparentemente reais, por isso algumas iniciativas mitigam esse tipo de ataque, como as relacionadas a seguir (UC BERKELEY, 2023):

2.4.1. Como combater o *phishing*?

- Proteja suas credenciais. Se uma pessoa está pedindo informações confidenciais, não tenha medo de perguntar o porquê; geralmente as empresas não solicitam informações confidenciais por e-mail, mensagem de texto ou telefone;
- Cuidado com anexos e links, pois são comumente usados para enviar software mal-intencionado. Quando você receber uma mensagem com um anexo ou link, verifique sua legitimidade antes de clicar;
- Verifique o endereço de e-mail do remetente antes de responder ou clicar em links. Como os e-mails podem ser falsificados, passe o cursor sobre os endereços antes de responder para garantir que sejam legítimos. Qualquer correspondência de uma organização deve vir de um endereço de e-mail organizacional;
- Limite suas informações públicas. Os invasores usam informações pessoais e públicas sobre você para convencê-lo a responder. Quanto menos você compartilhar sobre si mesmo, menor será o alvo de um ataque de engenharia social. Os criminosos cibernéticos usam as informações que você publica online para saber como ganhar sua confiança;

- Não se pressione. E-mails que criam urgência e medo geralmente são falsos. Não se apresse, olhe todo o e-mail e seja cético(a): verifique novamente o endereço do remetente para ver se é legítimo; e
- Pare e reveja. Olhe o e-mail antes de responder. É inesperado? O pedido faz sentido? Em caso de dúvida, entre em contato com o remetente, separadamente, por telefone ou por e-mail (mas não responda ao e-mail suspeito).

2.5. Senhas

Durante a realização das tarefas cotidianas, a utilização de senhas é uma condicional para o acesso aos diversos sistemas e ambientes úteis, por isso evite usar senhas fracas. As senhas fracas podem ser facilmente adivinhadas, permitindo acessos às informações autorizadas ao perfil do(a) usuário(a). Conforme estudos, para quebrar senhas fracas os invasores gastam apenas um segundo. No Brasil, as senhas fracas mais utilizadas são: 123456, Brasil, 123456789, 12345, 12345678 e 102030 (NORDPASS, 2023).

Com o intuito de manter a confidencialidade, integridade e disponibilidade das informações acessíveis por intermédio de suas credenciais de acesso, pratique as seguintes boas práticas:

- Use senhas longas e complexas, com os seguintes caracteres de complexidade: uso de letras maiúsculas e minúsculas, números e símbolos (por exemplo, !@#$%^&*()_+|~-=\'{}[]:";'<>?,./'espaço'), tamanho mínimo de oito posições para acessos sem autenticação de dois fatores (2FA) e 14 caracteres para acessos sem 2FA (CIS 8, 2021). Isso evita que invasores usem técnicas para adivinhá-las;
- Muitos dispositivos são configurados com senha padrão. Realize a troca imediatamente após o primeiro acesso;
- Evite reutilizar suas senhas em contas diferentes. Além disso, verifique constantemente se você já foi vítima de um vazamento de dados, como disponibilizado no site minhasenha (2023). Nesse caso, altere suas senhas imediatamente;
- Configure suas senhas para serem alteradas com frequência. O ideal é a cada três meses pelo menos;
- Não anote, não guarde em local de fácil acesso nem compartilhe suas senhas com outras pessoas, evitando assim o acesso não autorizado;
- Utilize gerenciadores de senha com a credencial mestra de acesso com o nível de complexidade aqui recomendado, sendo exemplo de boas alternativas gratuitas: Dashlane, LastPass, Avira Password Manager e RoboForm (SAFETYDETECTIVES, 2023b);
- Use mecanismos de 2FA para adicionar uma camada de segurança às suas contas, como já ocorre no acesso aos sistemas existentes no Conselho Nacional de Justiça (CNJ); e
- Configure meios de recuperar o acesso, como incluindo números de telefone ou e-mails.

2.6. Sites não confiáveis

Muitas páginas hospedadas na internet funcionam como armadilha para infectar sistemas operacionais em computadores pessoais. Assim, sites de conteúdos inapropriados (adulto, racista, intolerante, violento e relacionado a manifestações contrárias aos direitos humanos) e softwares sem licenças devem ser evitados, pois esses procedimentos são proibidos em políticas de segurança organizacionais. Havendo dúvidas quanto à reputação do site, há opções confiáveis para a verificação online (CISCO, 2023).

2.7. Uso de mídias removíveis

Caso necessite utilizar um pendrive para copiar arquivos, não deixe de imunizá-los conforme demonstrado em TechT (2016). Tal procedimento torna-se necessário, pois alguns vírus executam comandos inadvertidamente, comprometendo, via USB, o computador pessoal. Ao realizar os procedimentos demonstrados na referência citada, o pendrive fica protegido contra possíveis vírus existentes em computadores.

2.8. Antivírus atualizado

Antivírus é um programa projetado para detectar e remover vírus e outros tipos de softwares maliciosos de computadores ou laptops. Software malicioso, denominado malware, é um código que pode danificar computadores e notebooks, bem como os dados neles contidos.

Dessa forma, os dispositivos podem ser infectados baixando inadvertidamente um malware em um anexo vinculado a um e-mail duvidoso ou oculto em uma unidade USB, ou simplesmente visitando um site duvidoso. Uma vez no dispositivo, o malware pode roubar os dados, criptografá-los impedindo o uso ou até apagá-los completamente (NCSC, 2023).

Por isso, instalar e manter um antivírus atualizado é uma prática básica e muito importante no combate às infecções em computadores. Assim sendo, há opções gratuitas (Avast, Avira, Panda, TotalAV e AVG) que atendem aos requisitos mínimos de segurança, como mencionado em SafetyDetectives (2023a).

2.9. ChatGPT

ChatGPT (Chat Generative Pre-Trained Transformer/Transformador Pré-Treinado de Gerador de Conversas) é um assistente virtual inteligente no formato chatbot[1] online com inteligência artificial desenvolvido pela OpenAI, sendo um aplicativo especializado em diálogo. O chatbot é um modelo de linguagem ajustado com técnicas de aprendizado supervisionado e por reforço (WIKIPEDIA, 2023).

1 Programa de computador que tenta simular um ser humano na conversação com as pessoas. O objetivo é responder as perguntas de tal forma que se tenha a impressão de conversar com outra pessoa, e não com um programa de computador (WIKIPEDIA, 2023b).

O ChatGPT é um protótipo de inteligência artificial que chamou a atenção por suas respostas detalhadas e articuladas, embora a precisão de suas informações tenha sido criticada (WIKIPEDIA, 2023). O aplicativo tem sido largamente utilizado para atender a diversas necessidades, tais como: elaboração de apresentações, artigos, sermões, fórmulas de planilhas eletrônicas, código de programas computacionais, cartas e demais atividades do cotidiano. Porém, como o aplicativo requer massa de informações para seu aprimoramento, o conteúdo inserido em sua plataforma poderá ficar acessível a outros usuários, que terão a possibilidade de usá-lo de forma indevida.

2.9.1. Como evitar ataques cibernéticos propiciados pelas informações no ChatGPT?

Boas práticas de configurações no ChatGPT têm sido disseminadas com o intuito de manter a privacidade das informações. Contudo, como se trata de uma ferramenta relativamente nova, a ameaça está evoluindo rapidamente. Por enquanto, existem algumas maneiras de se proteger contra possíveis ameaças (TECHNOLOGY, 2023).

- Nunca compartilhe informações confidenciais, como dados financeiros, objeti-vos estratégicos, metas da organização, indicadores, logins/senhas ou mesmo seu nome e endereço;
- Mantenha-se alerta a ataques de engenharia social;
- Não insira código-fonte no aplicativo;
- Permaneça atualizado com relação aos procedimentos de segurança propos-tos pela organização.

Por fim, tenha sempre em mente que situações semelhantes ao ocorrido com a Samsung recentemente, na qual informações confidenciais foram inseridas no ChatGPT, põe em risco as organizações e os sistemas corporativos (MASHABLE, 2023).

REFERÊNCIAS

ABNT NBR ISO/IEC 27005. Target Normas: ABNT NBR ISO/IEC 27005. Disponível em: <https://www.normas.com.br/visualizar/abnt-nbr-nm/27395/nbriso-iec27005-tecnologia-da-informacao-tecnicas-de-seguranca-gestao-de-riscos-de-seguranca-da-informacao>. Acesso em: 13 fev 2023.

CIS 8. CIS Critical Security Controls Version 8. Disponível em: <https://www.cisecurity.org/controls/v8>. Acesso em: 13 fev 2023.

CISCO. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence. Disponível em: <https://talosintelligence.com/>. Acesso em: 13 fev 2023.

CNJ. Resolução n. 396, de 7 de junho de 2021. Disponível em: <https://juslaboris.tst.jus.br/handle/20.500.12178/187311>. Acesso em: 13 fev 2023.

GOVERNO FEDERAL DO BRASIL. Celular Roubado. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/celular-legal/celular-roubado>. Acesso em: 11 jul 2023.

GOVERNO FEDERAL DO BRASIL. L13709. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 14 maio 2023.

ISO 27.000. ABNT Catálogo. Disponível em: <https://www.abntcatalogo.com.br/pnm.aspx?Q=azh4bE5RZHA5TUpVdCtLYWg3cTVvMUtwQUtXSW1sSjFWRnZQcUdNUmtZRT0=>. Acesso em: 12 fev 2023.

ISO ABNT 29100:2020. ABNT Catálogo. Disponível em: <https://www.abntcatalogo.com.br/pnm.aspx?Q=emxjYUlvTk5jeEVwTXVaNHRFZnJTWTBKcVdiOGhXWHZwWlNsYWd6ckFpRT0=>. Acesso em: 13 fev 2023.

MASHABLE. Samsung ChatGPT leak: Samsung workers accidentally leak trade secrets to the AI chatbot | Mashable. Disponível em: <https://mashable.com/article/samsung-chatgpt-leak-details>. Acesso em: 17 maio 2023.

MINHASENHA. Sua senha vazou? Disponível em: <https://minhasenha.com/>. Acesso em: 13 fev 2023.

MITRE. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. Disponível em: <https://www.cvedetails.com/>. Acesso em: 12 fev 2023.

NCSC. What is an antivirus product? Do I need one? - NCSC.GOV.UK. Disponível em: <https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product>. Acesso em: 13 fev 2023.

NORDPASS. Top 200 Most Common Password List 2022 | NordPass. Disponível em: <https://nordpass.com/most-common-passwords-list/>. Acesso em: 13 fev 2023.

SAFETYDETECTIVES. 7 melhores antivírus para Windows 2023. Disponível em: <https://pt.safetydetectives.com/blog/melhores-antivirus-gratis-mesmo-para-windows/>. Acesso em: 11 jul 2023a.

SAFETYDETECTIVES. Top 7 gerenciadores de senhas em 2023. Disponível em: <https://pt.safetydetectives.com/blog/the-best-free-password-managers-pt/>. Acesso em: 11 jul 2023b.

SASSE, M. A. e BROSTOFF, S. e WEIRICH, D. Transforming the “weakest link” - A human/computer interaction approach to usable and effective security. BT Technology Journal, v. 19, n. 3, p. 122–131, 2001. Disponível em: <https://www.researchgate.net/publication/2404434_Transforming_the_'Weakest_Link'_-_a_HumanComputer_Interaction_Approach_to_Usable_and_Effective_Security>. Acesso em: 9 abr 2023.

TECHNOLOGY, CFE Media and. RSA Conference 2023: The cybersecurity impact of AI tools like ChatGPT | Industrial Cybersecurity Pulse | Industrial Cybersecurity Pulse. Disponível em: <https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/rsa-conference-2023-the-cybersecurity-impact-of-ai-tools-like-chatgpt/>. Acesso em: 6 maio 2023.

TECHTUDO. Sem vírus: veja como proteger o pendrive e impedir que seja infectado | Dicas e Tutoriais | TechTudo. Disponível em: <https://www.techtudo.com.br/noticias/2016/02/sem-virus-veja-como-proteger-o-pendrive-e-impedir-que-seja-infectado.ghtml>. Acesso em: 13 fev 2023.

UC BERKELEY. Fight the Phish | Information Security Office. Disponível em: <https://security.berkeley.edu/education-awareness/fight-phish>. Acesso em: 13 fev 2023.

VAKHTER, Vladimir e colab. Security for Emerging Miniaturized Wireless Biomedical Devices: Threat Modeling with Application to Case Studies. Research on Biomedical EngineeringGate, 2021. Disponível em: <https://www.researchgate.net/publication/351575284_Security_for_Emerging_Miniaturized_Wireless_Biomedical_Devices_Threat_Modeling_with_Application_to_Case_Studies>. Acesso em: 13 fev 2023.

WIKIPÉDIA. ChatGPT – Wikipédia, a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/ChatGPT>. Acesso em: 6 maio 2023.

WORLD ECONOMIC FORUM. After reading, writing and arithmetic, the 4th “r” of literacy is cyber-risk | World Economic Forum. Disponível em: <https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education>. Acesso em: 12 fev 2023.

Acesse o código QR
e conheça outras
publicações do Programa
Fazendo Justiça

FAZENDO
JUSTIÇA

PNUD

CNJ CONSELHO NACIONAL DE JUSTIÇA