ANA PAULA MONTEIRO ALMEIDA CHAGAS

MANUAL DE BOAS PRÁTICAS
DE SEGURANÇA DA INFORMAÇÃO

Copyright © 2023 Ana Paula Monteiro Almeida Chagas

Todos os direitos reservados. Nenhuma parte deste manual pode ser reproduzida ou transmitida em nenhuma forma e por nenhum meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou qualquer sistema de armazenamento de informação, sem permissão por escrito do autor.

ÁREA DE CONCENTRAÇÃO
Gestão da informação e do conhecimento e sociedade

LINHA DE PESQUISA
Produção, organização e comunicação da informação

TEMA
Segurança da informação

ORIENTADORA
Profa. Dra. Telma de Carvalho

PLANEJAMENTO GRÁFICO E DIAGRAMAÇÃO
Bárbara Costa

ILUSTRAÇÕES
Designed by Freepik

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

C426m Chagas, Ana Paula Monteiro Almeida

Manual de boas práticas de segurança da informação / Ana Paula Monteiro Almeida Chagas. – São Cristóvão, 2023.
30 f.: il ; color.

Orientadora: Profa. Dra. Telma de Carvalho

Produto da Dissertação (Mestrado Profissional em Gestão da Informação e do Conhecimento) – Universidade Federal de Sergipe, Programa de Pós-graduação em Ciência da Informação, Mestrado Profissional em Gestão da Informação e do Conhecimento, 2023.

1. Segurança da Informação. 2. Usuários dos Sistemas. I. Carvalho, Telma de, orient. II. Título.

CDU 65.012.4:007
CDD 65.012.4.007

Ficha elaborada pela bibliotecária Shirley dos Santos Ferreira (CRB-5/001862/0).

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

PRODUTO EDUCACIONAL DO MESTRADO PROFISSIONAL EM GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

UNIVERSIDADE FEDERAL DE SERGIPE

SUMÁRIO

01 APRESENTAÇÃO 4

02 PRINCIPAIS CONCEITOS EM SEGURANÇA DA INFORMAÇÃO 5

03 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO 6

04 VISÃO PRÁTICA DOS TRÊS PRINCIPAIS PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO 8

05 PROTAGONISMO, IDENTIFICAÇÃO E PERCEPÇÃO DOS USUÁRIOS QUANTO A SEGURANÇA DA INFORMAÇÃO NO USO DOS SISTEMAS DE INFORMAÇÃO 11

06 NORMATIVAS DE SEGURANÇA DA INFORMAÇÃO 13

07 MAPEAMENTO DAS AMEAÇAS, CONTROLE E BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO 16

08 DICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NBR ISO/IEC 27001:2022 23

09 CONSIDERAÇÕES FINAIS 26

REFERÊNCIAS 27

01 APRESENTAÇÃO

O presente Manual de Boas Práticas de Segurança da Informação é o resultado de uma pesquisa de intervenção conduzida na Procuradoria da União no Estado de Sergipe (PU/SE), um órgão vinculado à Advocacia-Geral da União (AGU). Essa pesquisa foi realizada como parte do Mestrado Profissional em Gestão da Informação e do Conhecimento, com o título **GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA: INTERFACE, USUÁRIO, TECNOLOGIA E SISTEMA**, desenvolvido pelo Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Sergipe (UFS).

O objetivo geral da pesquisa foi analisar o comportamento dos servidores da Procuradoria da União em Sergipe em relação às interfaces entre usuário, tecnologia e sistemas, com um enfoque especial na segurança da informação, com o propósito de elaborar um Manual de Boas Práticas de Segurança da Informação.

Pretende-se com este manual apresentar diretrizes e recomendações práticas que possam aprimorar significativamente a percepção e a compreensão das práticas de segurança da informação por parte dos usuários dos sistemas. Estas orientações têm como objetivo estabelecer um padrão institucionalizado de segurança, fornecendo um conjunto de diretrizes de fácil aplicação para garantir a proteção dos ativos de informação da Procuradoria da União no Estado de Sergipe (PU/SE). Através deste manual, esperamos capacitar os usuários a adotarem boas práticas de segurança em suas atividades diárias, contribuindo assim para um ambiente mais seguro e protegido contra ameaças cibernéticas.

MANTENHA-SE UM PASSO À FRENTE
DAS AMEAÇAS CIBERNÉTICAS.

BOA LEITURA!

02 PRINCIPAIS CONCEITOS EM SEGURANÇA DA INFORMAÇÃO

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Brasil, 2021).

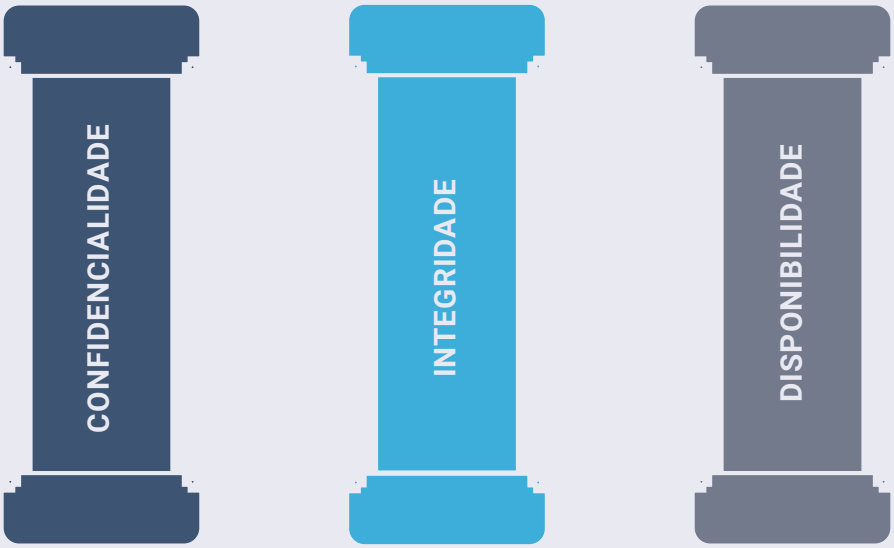
A proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (Associação Brasileira de Normas Técnicas, 2012, n.p.).

A segurança da informação é uma área de conhecimento voltada à proteção da informação e dos ativos associados contra indisponibilidade, alterações indevidas e acessos não autorizados" (Sêmola, 2014, p. 41).

A Segurança da Informação desempenha um papel vital na defesa de informações valiosas contra uma série de ameaças, incluindo hackers, vírus, malware, roubo de dados e acesso não autorizado. Em nosso mundo cada vez mais digitalizado, as informações se tornaram ativos extremamente valiosos, não apenas para organizações, mas também para indivíduos. Portanto, a implementação de medidas de segurança da informação é indispensável para assegurar um ambiente digital seguro e confiável.

SUA INFORMAÇÃO,
SUA RESPONSABILIDADE.
PROTEJA-A!

03 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO



São três os pilares que constituem os princípios básicos da segurança da informação e formam a base desse campo. Eles orientam o desenvolvimento de políticas, práticas e tecnologias para proteger ativos de informação contra ameaças e riscos.

CONFIDENCIALIDADE

Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada (Sêmola, 2014, p. 27).

Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento (Brasil, 2012, p. 9).

INTEGRIDADE

Toda informação deve ser mantida na mesma condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais (Sêmola, 2014, p. 28).

A integridade consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados. (Brasil, 2012, p. 9).

DISPONIBILIDADE

Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível para seus usuários, no momento em que eles necessitam delas para qualquer finalidade (Sêmola, 2014, p. 28).

Garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito (Brasil, 2012, p. 10).

04 VISÃO PRÁTICA DOS TRÊS PRINCIPAIS PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

CONFIDENCIALIDADE

OBJETIVO:

Garantir que as informações sensíveis sejam acessíveis apenas para pessoas autorizadas, mantendo-as protegidas contra acessos não autorizados.

SINAL DE ALERTA:

Acontece quando há uma violação ou comprometimento da privacidade e proteção das informações sensíveis.

CAUSAS:

Acesso não autorizado a dados confidenciais, vazamento de informações, compartilhamento inadequado de senhas, entre outras situações em que a confidencialidade dos dados é comprometida.

AÇÕES PARA MANTER OS PRINCÍPIOS DE CONFIDENCIALIDADE:

Políticas de acesso; controle de acesso; criptografia; treinamento; monitoramento, classificação de grau de sigilo; políticas claras sobre o compartilhamento das informações confidenciais, principalmente.

INTEGRIDADE

OBJETIVO:

Garantir que as informações sensíveis sejam acessíveis apenas para pessoas autorizadas, mantendo-as protegidas contra acessos não autorizados.

SINAL DE ALERTA:

Ocorre quando há suspeitas de alterações indevidas nas informações, exigindo investigação e correção imediatas para evitar problemas decorrentes de dados incorretos.

CAUSAS:

Falhas de hardware ou software, ataques cibernéticos, erros humanos, armazenamento inadequado de dados e corrupção de arquivos. Esses fatores podem resultar na modificação não autorizada ou na corrupção de informações, comprometendo a integridade dos dados.

AÇÕES PARA MANTER OS PRINCÍPIOS DE INTEGRIDADE:

Controle de acesso; realizar backups; verificar regularmente a integridade dos arquivos e dados por meio de algoritmos de HASH.; educação dos usuários para práticas seguras de manipulação e armazenamento das informações; atualização regular de software e monitoramento de tráfego de rede.

DISPONIBILIDADE

OBJETIVO:

Garantir que as informações e recursos necessários estejam disponíveis e acessíveis quando necessário, assegurando a continuidade das operações e a capacidade de uso dos sistemas e dados pela organização.

SINAL DE ALERTA:

Ocorre quando há interrupções não planejadas nos sistemas, impedindo o acesso a informações e recursos cruciais, prejudicando as operações e a eficiência dos serviços da organização.

CAUSAS:

Ocorrência de incidentes de segurança, como ataques cibernéticos, falhas técnicas ou desastres naturais, que resultam na inacessibilidade dos recursos de informação essenciais.

AÇÕES PARA MANTER OS PRINCÍPIOS DE DISPONIBILIDADE:

Criar cópias de segurança, manter a infraestrutura de TI, treinar os usuários para reconhecer ameaças, promover conscientização e desenvolver planos de contingência são práticas essenciais.

Textos baseados na obra de Ferreira (2017).

05 PROTAGONISMO, IDENTIFICAÇÃO E PERCEPÇÃO DOS USUÁRIOS QUANTO A SEGURANÇA DA INFORMAÇÃO NO USO DOS SISTEMAS DE INFORMAÇÃO

PROTAGONISMO

Os usuários não devem ser apenas consumidores passivos de tecnologia, mas sim agentes ativos na promoção da eficiência, segurança e inovação no ambiente de trabalho.

QUEM SÃO

Usuário da informação é pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade (Brasil, 2021, n. p.).

PERCEPÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO NO USO DE SISTEMAS DE INFORMAÇÃO

Conscientização e Responsabilidade: compreender os riscos associados e como suas ações podem afetar a segurança da informação.

Educação e Treinamento: adquirir conhecimentos e habilidades para identificar ameaças, reconhecer práticas inseguras e saber como reagir a incidentes.

Comportamentos Seguros: desempenhar um papel vital ao adotar práticas seguras, como criar senhas robustas, manter o software atualizado, evitar clicar em links suspeitos e relatar incidentes de segurança.

Feedback e Melhoria Contínua: fornecer feedback sobre possíveis vulnerabilidades e problemas de segurança pode ajudar na melhoria contínua das políticas e procedimentos de segurança.

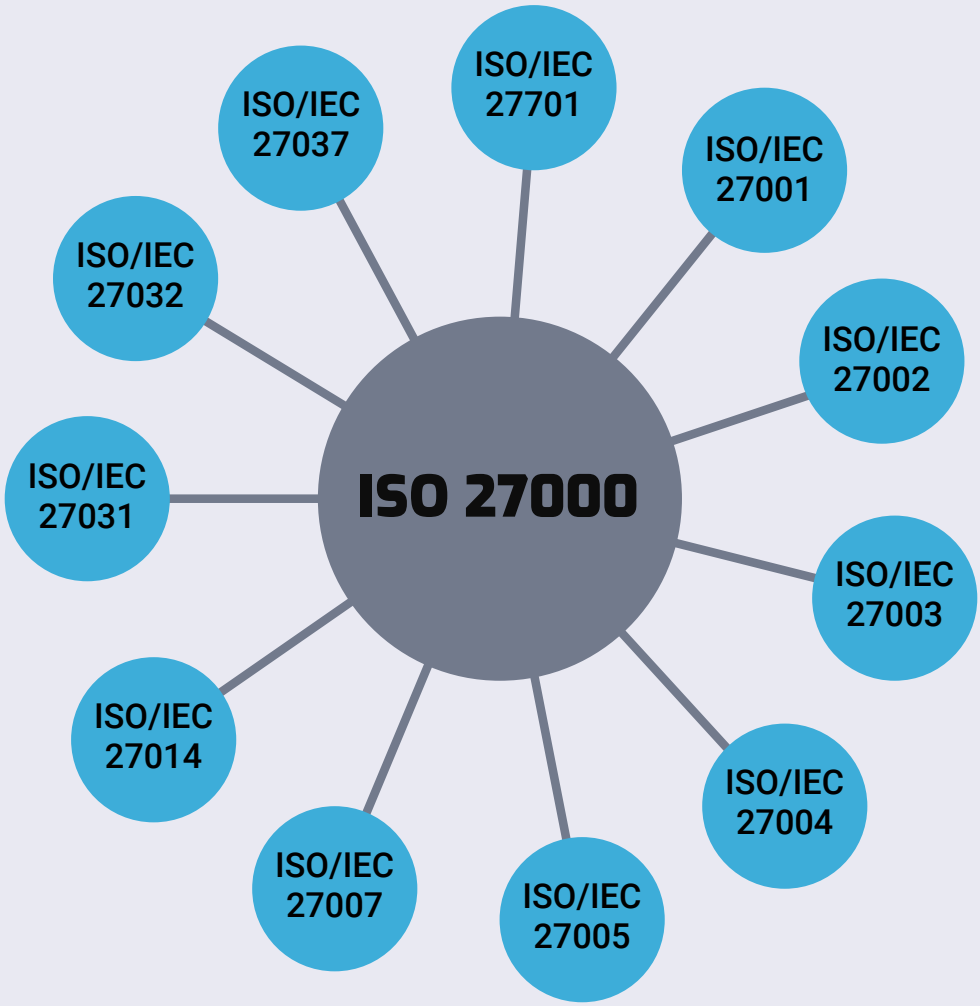
Compartilhamento de Responsabilidade: compreender que a segurança da informação não é apenas responsabilidade da equipe de TI, mas de todos na organização. Todos têm um papel a desempenhar.

Sensibilização para Ameaças Emergentes: reconhecer as ameaças cibernéticas em constante evolução e as táticas utilizadas pelos cibercriminosos.

Elaborado pela autora a partir dos dados da pesquisa (2023).

06 NORMATIVAS DE SEGURANÇA DA INFORMAÇÃO

A família ISO 27000 é uma série de normas internacionais que se concentra na gestão da segurança da informação. Essas normas são desenvolvidas pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC) e são projetadas para ajudar as organizações a estabelecerem, implementarem e manterem sistemas de gestão de segurança da informação eficazes.



Normas de Segurança da Informação família ISO 27000

ISO/IEC 27001 — Estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI) e sua certificação.

Diretrizes e requisitos para a segurança da informação em organizações, incluindo um conjunto de controles e boas práticas. — **ISO/IEC 27002**

ISO/IEC 27003 — Orientações para a implementação de um sistema de gestão de segurança da informação em uma organização.

Norma para medir e avaliar a segurança da informação. — **ISO/IEC 27004**

ISO/IEC 27005 — Norma que trata de gerenciamento de riscos de segurança da informação.

Norma que fornece diretrizes para auditorias internas de sistemas de gestão de segurança da informação. — **ISO/IEC 27007**

ISO/IEC 27014 — Norma que fornece diretrizes para governança de segurança da informação.

ISO/IEC 27031

Norma que aborda a continuidade de negócios e a gestão de segurança da informação.

ISO/IEC 27032

Trata da cibersegurança, fornecendo diretrizes e princípios gerais para proteger sistemas, redes e informações contra ameaças cibernéticas.

ISO/IEC 27037

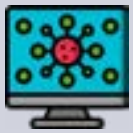
Trata de diretrizes e princípios para identificar, coletar e preservar evidências digitais em investigações de segurança da informação.

ISO/IEC 27701

Norma sobre privacidade da informação.

07 MAPEAMENTO DAS AMEAÇAS, CONTROLE E BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

AMEAÇAS

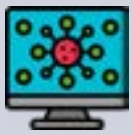
ELEMENTOS INDICADORES DE FALHAS	OCORRÊNCIA	CONTROLE
		
Vírus/programas maliciosos	Anexos de e-mail infectados, downloads de sites não confiáveis, dispositivos USB ou outras mídias removíveis	Manter o sistema e aplicativos atualizados com patches de segurança e ter precaução ao abrir anexos de e-mail ou baixar arquivos de fontes desconhecidas

BOAS PRÁTICAS

ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO	RESPONSÁVEIS
Gerenciamento de senhas	Organização e usuários dos sistemas

AMEAÇAS

ELEMENTOS INDICADORES DE FALHAS



Uso de sites livres para compressão, conversão e outras atividades de arquivos

OCORRÊNCIA

Distribuição de malware, como vírus ou programas maliciosos, roubo de dados, uso indevido de dados e violação dos direitos e proteção dos dados

CONTROLE

Verificar se o site usa uma conexão segura (HTTPS) e evitar compartilhar informações pessoais ou confidenciais em sites de terceiros. Manter um software antivírus atualizado em seu dispositivo para proteção adicional

BOAS PRÁTICAS

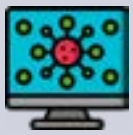
ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO

Uso de sites confiáveis e manter um antivírus atualizado

RESPONSÁVEIS

Organização e usuários dos sistemas

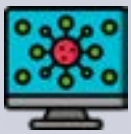
AMEAÇAS

ELEMENTOS INDICADORES DE FALHAS	OCORRÊNCIA	CONTROLE
 **Senhas**	Senhas fracas, compartilhamento de senhas ou falta de atualização das senhas podem comprometer a segurança dos sistemas	Desenvolver políticas de senhas com requisitos de complexidade, comprimento, expiração e diretrizes para os usuários

BOAS PRÁTICAS

ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO	RESPONSÁVEIS
Gerenciamento de senhas	Organização e usuários dos sistemas

AMEAÇAS

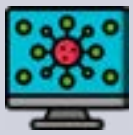
ELEMENTOS INDICADORES DE FALHAS	OCORRÊNCIA	CONTROLE
		
Treinamento	Golpes de phishing, instalação de malware, vazamento de informações confidenciais	Capacitar os funcionários a reconhecer e mitigar ameaças cibernéticas, com práticas seguras e conscientização

BOAS PRÁTICAS

ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO	RESPONSÁVEIS
Treinamento contra ameaças cibernéticas e uso seguro dos sistemas	Organização

AMEAÇAS

ELEMENTOS INDICADORES DE FALHAS



Falta de comunicação de incidentes cibernéticos

OCORRÊNCIA

Pode abranger diversos tipos de incidentes, desde violações de dados até malware, phishing, intrusões, fraudes e muito mais

CONTROLE

Estabelecer um canal de incidentes bem divulgado, de fácil acesso, seguro, confidencial e com processos de resposta bem definidos

BOAS PRÁTICAS

ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO

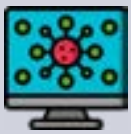
Disseminação e conscientização do uso de um canal de incidentes

RESPONSÁVEIS

Organização e usuários dos sistemas

AMEAÇAS

ELEMENTOS INDICADORES DE FALHAS



Suporte técnico em teletrabalho em dispositivos pessoais

OCORRÊNCIA

Perda de dados confidenciais, roubo de informações críticas ou comprometimento da rede

CONTROLE

Garantir aos dispositivos pessoais dos servidores o mesmo nível de proteção de segurança do existente nos equipamentos da organização

BOAS PRÁTICAS

ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO

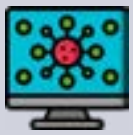
Suporte técnico abrangente para o teletrabalho, independentemente da propriedade dos dispositivos utilizados

RESPONSÁVEIS

Organização

AMEAÇAS

ELEMENTOS INDICADORES DE FALHAS



Conscientização

OCORRÊNCIA

A falta de uma cultura consciente dos riscos da segurança da informação aumenta a fragilidade dos sistemas e redes digitais diante de ameaças e ataques cibernéticos

CONTROLE

Manter uma cultura dialógica e pesquisas sobre o perfil de risco e adoção de medidas de segurança mais eficazes

BOAS PRÁTICAS

ESTRATÉGIAS ALTERNATIVAS DE SEGURANÇA DA INFORMAÇÃO

Promover uma cultura de segurança cibernética

RESPONSÁVEIS

Organização e usuários dos sistemas

08 DICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NBR ISO/IEC 27001:2022

USUÁRIO, REDOBRE A ATENÇÃO!
Sua vigilância é a primeira linha de defesa na segurança da informação.

1. **Use o bom senso.** Se algo parece suspeito ou muito bom para ser verdade, é provavelmente uma ameaça.

2. **Se você suspeitar de uma violação de segurança ou atividade maliciosa, relate-a imediatamente** ao suporte de TI ou à equipe de segurança da sua organização.

3. **Configure bloqueios de tela** nos seus dispositivos para evitar o acesso não autorizado.

4. **Mantenha-se atualizado sobre as últimas ameaças de segurança** e práticas recomendadas por meio de fontes confiáveis. A educação contínua é fundamental.

5 **Ative alertas de conta sempre que possível.** Isso pode ajudar a identificar atividades suspeitas em suas contas.

6 **Proteja seus dispositivos móveis com senhas ou PINs**, ative a localização e o rastreamento remoto em caso de perda ou roubo e instale aplicativos somente de fontes confiáveis.

7 **Limite a quantidade de informações pessoais compartilhadas em redes sociais** e ajuste as configurações de privacidade para controlar quem pode ver suas postagens.

8 **Faça backups regulares dos seus dados importantes, armazenando cópias em locais seguros.** Isso pode ajudar a recuperar informações em caso de perda devido a ataques de ransomware ou falhas no sistema.

9 **Proteja seus dispositivos móveis** com senhas ou PINs, ative a localização e o rastreamento remoto em caso de perda ou roubo e instale aplicativos somente de fontes confiáveis.

10 **Mantenha um programa antivírus e antimalware atualizado** e faça verificações regulares no seu dispositivo.

11

Evite acessar informações sensíveis ou fazer transações financeiras em redes Wi-Fi públicas não seguras. Use uma rede VPN (Rede Virtual Privada) se precisar de acesso seguro.

12

Esteja ciente de tentativas de phishing, em que os golpistas tentam enganá-lo para revelar informações pessoais ou financeiras. Verifique sempre a legitimidade dos e-mails, URLs e remetentes.

13

Tenha cautela ao abrir e-mails de remetentes desconhecidos ou suspeitos. Não clique em links ou baixe anexos de fontes não confiáveis. Esteja especialmente atento a e-mails de phishing.

14

Sempre que possível, ative a autenticação em dois fatores nas suas contas. Isso adiciona uma camada extra de segurança, exigindo um código temporário ou confirmação adicional, além da senha para acessar a conta.

15

Use senhas fortes e exclusivas para suas contas online. Evite senhas óbvias, como datas de nascimento, nomes próprios ou sequências numéricas. Considere o uso de frases de senha ou gerenciadores de senhas para criar e armazenar senhas seguras.

09 CONSIDERAÇÕES FINAIS

Esse Manual de Boas Práticas de Segurança da Informação representa um marco significativo na jornada em direção a um ambiente digital mais seguro e consciente. Os valiosos insights obtidos por meio da pesquisa aplicada, que originaram este manual, serviram como base sólida para sua criação. Este documento não se limita a informar, mas tem o propósito de ser uma ferramenta educacional projetada para capacitar os usuários a desempenharem um papel ativo na proteção da segurança da informação.

Ao explorar as páginas desse manual, os colaboradores encontrarão orientações práticas, dicas relevantes e diretrizes que ajudaram a compreender os desafios e responsabilidades associados à segurança da informação na organização.

Reconhece-se que a segurança da informação é uma responsabilidade compartilhada e esse manual é um passo importante para a construção de uma cultura de segurança sólida e resiliente. Incentiva-se todos os usuários a adotarem as práticas descritas aqui e a se tornarem protagonistas na proteção dos ativos informacionais. Compromete-se a fornecer os recursos e a educação necessários para que os colaboradores se tornem defensores da segurança da informação em todas as atividades.

A segurança da informação é uma responsabilidade que recai sobre todos e acredita-se que, com o conhecimento adquirido por meio desse manual, cada leitor poderá contribuir significativamente para a construção de um ambiente mais seguro e consciente na organização. Expressa-se gratidão a todos que participaram desse processo e reafirma-se a convicção de que, juntos, é possível construir um futuro mais seguro para a organização e todas as partes envolvidas.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 2700 de 11/2022**: segurança da informação, segurança cibernética e proteção à privacidade - sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro: ABNT, 2022. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/abnt-nbriso-iec27001-tecnologia-da-informacao-tecnicas-de--seguranca-sistemas-de-gestao-da-seguranca-da-informacao-requisitos. Acesso em: 12 dez. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022.** Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2022. Disponível em: https://www.abntcatalogo.com.br/grd.aspx. Acesso em: 20 set. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013.** Tecnologia da informação-Técnicas de segurança-Código de prática para a gestão da segurança da informação (Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799). Rio de Janeiro: ABNT, 2005. Disponível em: https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf. Acesso em: 20 set. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27003:** tecnologia da informação – técnicas de segurança – diretrizes para implantação de um sistema de gestão da segurança da informação Exemplar para uso exclusivo - ABNT - Associação Brasileira de Normas Técnicas - 33.402.892/0001-06. Disponível em: https://pdfcoffee.com/27003pdf-pdf-free.html. Acesso em: 20 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27004:2010:** tecnologia da informação - técnicas de segurança - gestão da segurança da informação - medição. Disponível em: https://www.skoob.com.br/livro/pdf/abnt-nbr-isoiec-27004/348487/edicao:391122. Acesso em: 20 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2008:** tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação. Disponível em: https://iso31000.net/riscos-cibernetticos/.Acesso em: 20 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27007:2021:** segurança da informação, segurança cibernética e proteção da privacidade: diretrizes para auditoria de sistemas de gestão da segurança da informação. Disponível em: https://www.normas.com.br/visualizar/artigo-tecnico/1591/nbr-iso-iec-27007-as-diretrizes-para-auditoria-da-seguranca-da-informacao. Acesso em: 12 set. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27014:2021:** segurança da informação, segurança cibernética e proteção de privacidade: governança da segurança da informação. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/33225/nbriso-iec27014-seguranca-da-informacao-seguranca-cibernetica-e-protecao-da-privacidade-governanca-da-seguranca-da-informacao. Acesso em: 20 set. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27031:2021:** tecnologia da informação, técnica de segurança, diretrizes para a prontidão para a continuidade de negócios da tecnologia da informação e comunicação. Disponível em: https://www.target.com.br/produtos/normas-tecnicas/43619/nbriso-iec27031-tecnologia-da-informacao-tecnicas-de-seguranca-diretrizes-para-a-prontidao-para-a-continuidade-de-negocios-da-tecnologia-da-informacao-e-comunicacao. Acesso em: 20 set. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27032:2021:** tecnologia da informação, técnicas de segurança, diretrizes para segurança cibernética. Disponível em: https://www.target.com.br/produtos/normas-tecnicas/43726/nbriso-iec27032-tecnologia-da-informacao-tecnicas-de-seguranca-diretrizes-para-seguranca-cibernetica. Acesso em: 20 set. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27037:2021:** tecnologia da informação, técnicas de segurança, diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/33821/nbriso-iec27037-tecnologia-da-informacao-tecnicas-de-seguranca-diretrizes-para-identificacao-coleta-aquisicao-e-preservacao-de-evidencia-digital. Acesso em: 20 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019:** técnicas de segurança, extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação: requisitos e diretrizes. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/11548/nbriso-iec27701-tecnicas-de-seguranca-extensao-da-abnt-nbr-iso-iec-27001-e-abnt-nbr-iso-iec-27002-para-gestao-da-privacidade-da-informacao-requisitos-e-diretrizes. Acesso em: 20 ago. 2023.

BRASIL. Presidência da República. **Glossário de segurança da informação.** Brasília: Presidência da República, 26 nov. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em: 20 jul. 2022.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** 4. ed. Brasília: TCU: Secretaria de Fiscalização de Tecnologias da Informação, 2012. 103 p.

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas; BEZERRA, Edson Kowask. **Gestão da segurança da informação:** NBR 27001 e NBR 27002. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2014.

FERREIRA, Sérgio da Costa. **Sistemas de informação em segurança.** Londrina: Editora e Distribuidora Educacional S.A., 2017. 224 p.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

PRODUTO EDUCACIONAL DO MESTRADO PROFISSIONAL EM GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

UNIVERSIDADE FEDERAL DE SERGIPE