3º Webinário de Segurança da Informação

Secretaria de Segurança da Informação e Cibernética – SSIC

Departamento de Segurança da Informação - DSI

Departamento de Segurança Cibernética - DSC

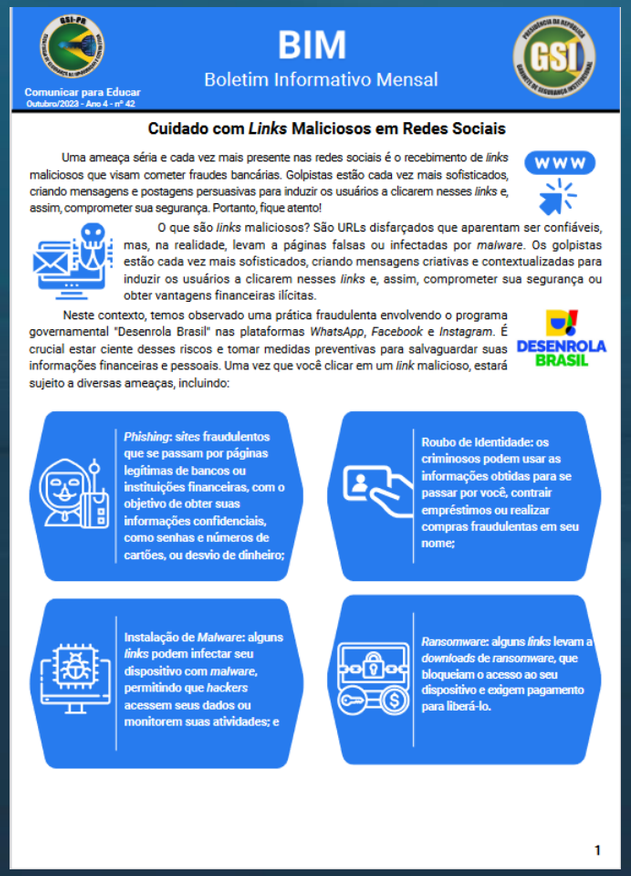
AÇÕES DE CONSCIENTIZAÇÃO

3º Webinário de Segurança da Informação

SUMÁRIO

3º Webinário de Segurança da Informação

Boletim Informativo Mensal - BIM



BIM
Boletim Informativo Mensal

Comunicar para Educar
Outubro/2023 - Ano 4 - nº 42

Cuidado com *Links* Maliciosos em Redes Sociais

Uma ameaça séria e cada vez mais presente nas redes sociais é o recebimento de *links* maliciosos que visam cometer fraudes bancárias. Golpistas estão cada vez mais sofisticados, criando mensagens e postagens persuasivas para induzir os usuários a clicarem nesses *links* e, assim, comprometer sua segurança. Portanto, fique atento!

O que são *links* maliciosos? São URLs disfarçados que aparentam ser confiáveis, mas, na realidade, levam a páginas falsas ou infectadas por *malware*. Os golpistas estão cada vez mais sofisticados, criando mensagens criativas e contextualizadas para induzir os usuários a clicarem nesses *links* e, assim, comprometer sua segurança ou obter vantagens financeiras ilícitas.

Neste contexto, temos observado uma prática fraudulenta envolvendo o programa governamental "Desenrola Brasil" nas plataformas *WhatsApp*, *Facebook* e *Instagram*. É crucial estar ciente desses riscos e tomar medidas preventivas para salvaguardar suas informações financeiras e pessoais. Uma vez que você clicar em um *link* malicioso, estará sujeito a diversas ameaças, incluindo:

- ***Phishing*: *sites* fraudulentos que se passam por páginas legítimas de bancos ou instituições financeiras, com o objetivo de obter suas informações confidenciais, como senhas e números de cartões, ou desvio de dinheiro;**
- **Roubo de Identidade: os criminosos podem usar as informações obtidas para se passar por você, contrair empréstimos ou realizar compras fraudulentas em seu nome;**
- **Instalação de *Malware*: alguns *links* podem infectar seu dispositivo com *malware*, permitindo que *hackers* acessem seus dados ou monitorem suas atividades; e**
- ***Ransomware*: alguns *links* levam a *downloads* de *ransomware*, que bloqueiam o acesso ao seu dispositivo e exigem pagamento para liberá-lo.**

1

BIM
Boletim Informativo Mensal

Comunicar para Educar
julho/2023 - Ano 4 - nº 41

Privacidade no mundo digital

O mundo está ao alcance de um clique. Nessa imensidão virtual, é fundamental estabelecermos uma prioridade essencial: a privacidade. À medida que exploramos a *Internet*, devemos estar conscientes dos perigos e proteger nossos dados pessoais.

No ambiente digital em constante expansão, a proteção da privacidade torna-se um aspecto de extrema importância. À medida que navegamos na *Internet* e utilizamos os serviços *on-line*, é imperativo estarmos cientes das ameaças existentes e adotarmos medidas para salvaguardar nossos dados pessoais.

Ao priorizarmos a privacidade, estamos fortalecendo nossa proteção no mundo virtual. Veja algumas formas de se proteger:

a. Controle a privacidade nas redes sociais
As redes sociais são como janelas para nossas vidas, permitindo que nos conectemos com o mundo. No entanto, é crucial estabelecer limites para proteger nossas informações pessoais. Descubra como ajustar as configurações de privacidade em suas contas, garantindo que apenas as pessoas certas tenham acesso aos seus dados. Aprenda a identificar e evitar perfis falsos e a compartilhar conteúdo com cuidado, protegendo sua privacidade enquanto interage em um ambiente social digital;

b. Uso de Redes Virtuais Privadas (VPN)
Ao navegar na *internet*, os rastros que deixamos podem revelar muito sobre nós. Explore como uma VPN pode proteger seus dados, criptografando sua conexão e mantendo suas atividades *on-line* em sigilo. Aprenda sobre os benefícios de usar uma VPN ao se conectar a redes *Wi-Fi* públicas, como escolher o provedor certo para garantir sua privacidade e sobre a importância de usar *firewalls* pessoais;

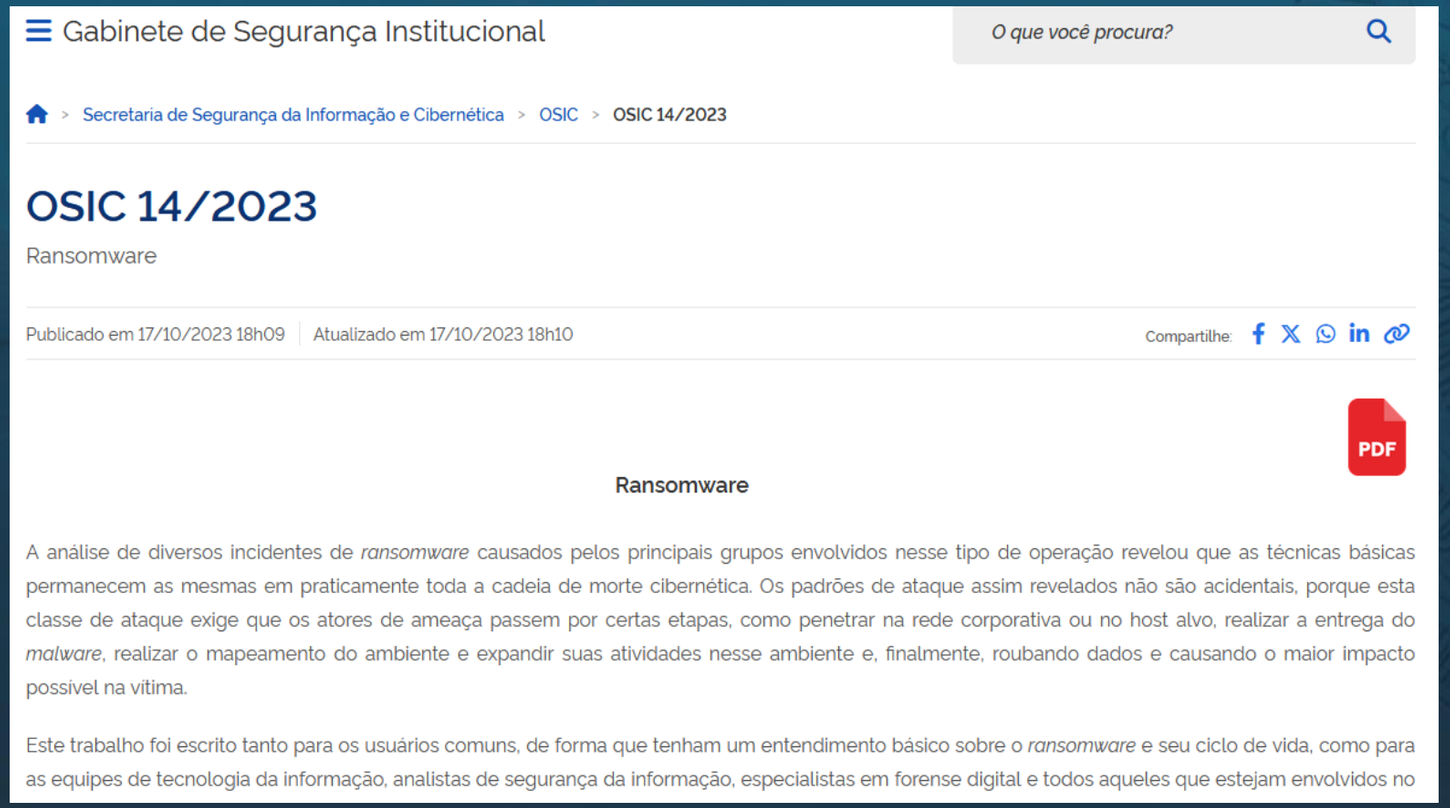
c. Cuidado com o compartilhamento de dados
Em um mundo cada vez mais interconectado, compartilhar informações pessoais é comum. No entanto, é crucial ser seletivo e cauteloso ao compartilhar dados sensíveis. Fique atento sobre como identificar situações em que é apropriado compartilhar informações pessoais e como evitar fornecer dados desnecessários. Aprenda a navegar por *e-mails* suspeitos, *links* duvidosos e a proteger-se contra esquemas de *phishing* que visam roubar suas informações pessoais.

Esperamos que você compreenda a importância da privacidade em primeiro lugar em seu mundo digital. Proteger seus dados pessoais permite que você aproveite ao máximo os recursos da *internet*, mas com segurança e tranquilidade. Lembre-se sempre de controlar suas configurações de privacidade, considerar o uso de uma VPN confiável e compartilhar informações com cautela.

1

3º Webinário de Segurança da Informação

Orientações de Segurança da Informação e Cibernética – OSIC



Gabinete de Segurança Institucional

O que você procura?

> Secretaria de Segurança da Informação e Cibernética > OSIC > OSIC 14/2023

OSIC 14/2023

Ransomware

Publicado em 17/10/2023 18h09 | Atualizado em 17/10/2023 18h10

Compartilhe:

PDF

Ransomware

A análise de diversos incidentes de *ransomware* causados pelos principais grupos envolvidos nesse tipo de operação revelou que as técnicas básicas permanecem as mesmas em praticamente toda a cadeia de morte cibernética. Os padrões de ataque assim revelados não são acidentais, porque esta classe de ataque exige que os atores de ameaça passem por certas etapas, como penetrar na rede corporativa ou no host alvo, realizar a entrega do *malware*, realizar o mapeamento do ambiente e expandir suas atividades nesse ambiente e, finalmente, roubando dados e causando o maior impacto possível na vítima.

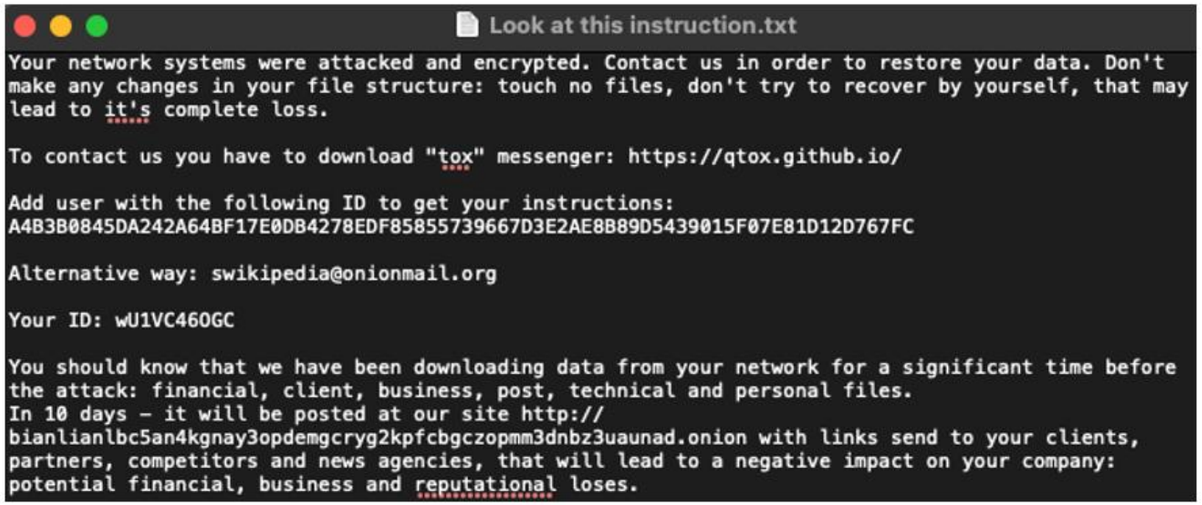
Este trabalho foi escrito tanto para os usuários comuns, de forma que tenham um entendimento básico sobre o *ransomware* e seu ciclo de vida, como para as equipes de tecnologia da informação, analistas de segurança da informação, especialistas em forense digital e todos aqueles que estejam envolvidos no

3º Webinário de Segurança da Informação

Orientações de Segurança da Informação e Cibernética – OSIC

Curiosamente, agora em 2023, foi observada uma nova evolução nas técnicas de ataque de *ransomware*, com o grupo de *ransomware* BianLian abandonando seus esforços de criptografia e se concentrando apenas na extorsão em função da exfiltração de dados.

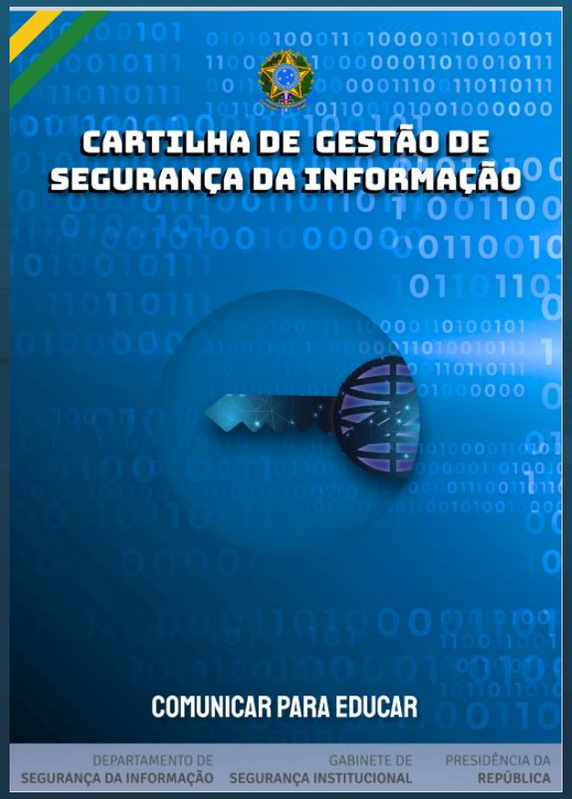
Originalmente, as campanhas do BianLian usavam a extorsão dupla, como pode ser visto na nota de resgate da figura abaixo.

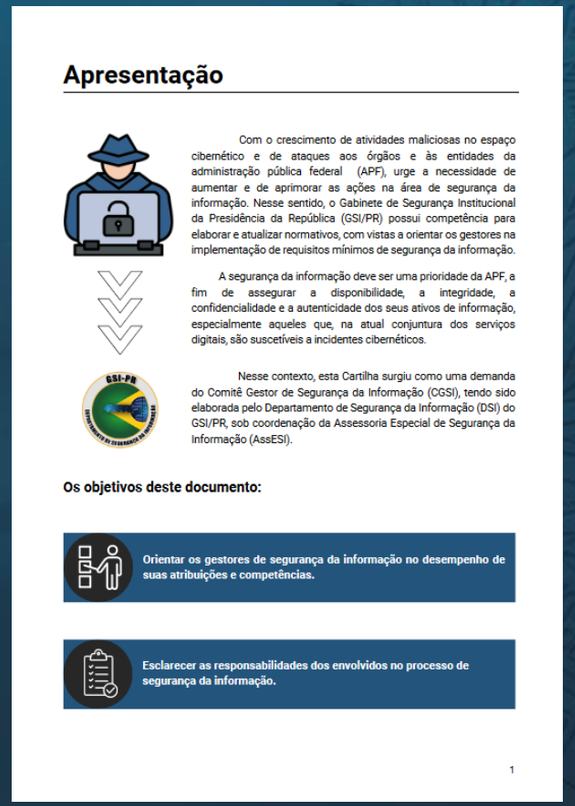


Fonte: https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye

3º Webinário de Segurança da Informação

Cartilha de Gestão de Segurança da Informação





Apresentação

Com o crescimento de atividades maliciosas no espaço cibernético e de ataques aos órgãos e às entidades da administração pública federal (APF), urge a necessidade de aumentar e de aprimorar as ações na área de segurança da informação. Nesse sentido, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) possui competência para elaborar e atualizar normativos, com vistas a orientar os gestores na implementação de requisitos mínimos de segurança da informação.

A segurança da informação deve ser uma prioridade da APF, a fim de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos seus ativos de informação, especialmente aqueles que, na atual conjuntura dos serviços digitais, são suscetíveis a incidentes cibernéticos.

Nesse contexto, esta Cartilha surgiu como uma demanda do Comitê Gestor de Segurança da Informação (CGSI), tendo sido elaborada pelo Departamento de Segurança da Informação (DSI) do GSI/PR, sob coordenação da Assessoria Especial de Segurança da Informação (AssESI).

Os objetivos deste documento:

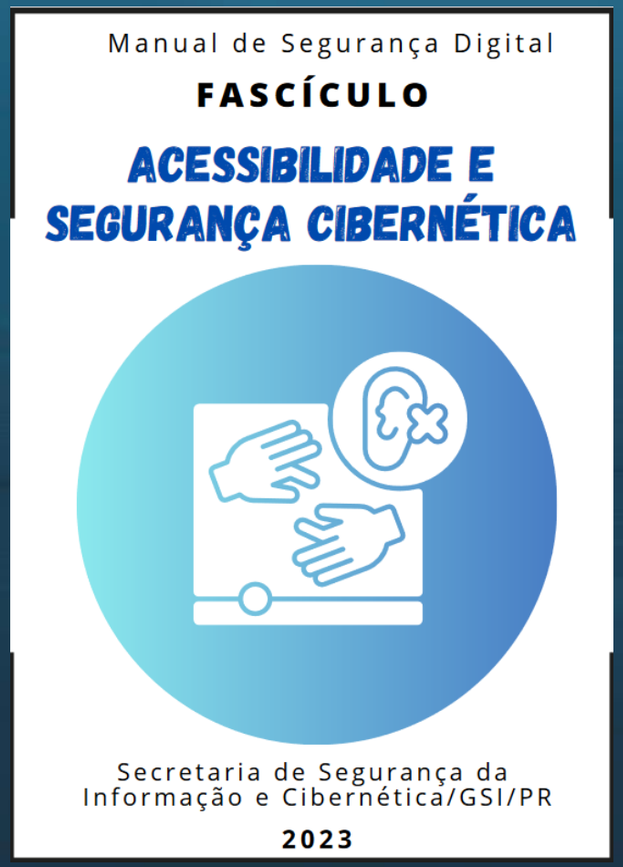
Orientar os gestores de segurança da informação no desempenho de suas atribuições e competências.

Esclarecer as responsabilidades dos envolvidos no processo de segurança da informação.

1

3º Webinário de Segurança da Informação

Fascículos



3º Webinário de Segurança da Informação

Alertas e recomendações

ALERTA 15/2023

Vulnerabilidade crítica no BIG-IP

Publicado em 27/10/2023 15h29 Compartilhe:

[TLP:CLEAR]

1. Foi publicada vulnerabilidade crítica da solução BIG-IP da empresa F5 Networks, que pode permitir que um usuário malicioso não autenticado execute, remotamente, comandos arbitrários no sistema.

2. Detalhes da Common Vulnerabilities and Exposures (CVE) relacionada ao caso (CVE-2023-46747) podem ser verificados em:

- https://nvd.nist.gov/vuln/detail/CVE-2023-46747

3. Versões do BIG-IP que foram consideradas vulneráveis:

- 17.1.0 (corrigido em 17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG)
- 16.1.0 - 16.1.4 (corrigido em 16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG)
- 15.1.0 - 15.1.10 (corrigido em 15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG)
- 14.1.0 - 14.1.5 (corrigido em 14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG)
- 13.1.0 - 13.1.5 (corrigido em 13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG)

3. O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) orienta às instituições que verifiquem no registro de ativos a existência de sistemas BIG-IP vulneráveis, conforme item anterior, e recomenda que realizem as ações de mitigação, conforme as orientações do fabricante contidas no seguinte endereço:

- https://my.f5.com/manage/s/article/K000137353

3º Webinário de Segurança da Informação

Alertas e recomendações

RECOMENDAÇÃO 15/2023

Vulnerabilidades no Confluence Server e Confluence Data Center

Publicado em 16/10/2023 17h36 Compartilhe:

[TLP:CLEAR]

1. Foram identificadas vulnerabilidades no Confluence Server e Confluence Data Center, software de colaboração desenvolvido pela empresa Atlassian. Sistemas vulneráveis podem ser explorados remotamente e um atacante pode obter acesso ao servidor, conforme a Common Vulnerabilities and Exposures:

- https://nvd.nist.gov/vuln/detail/CVE-2023-22515

2. O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) recomenda às instituições da Administração Pública Federal (APF) que utilizam o Confluence Server / Data Center a atualização imediata da aplicação. Informações técnicas e maiores detalhes a respeito da atualização podem ser consultados em:

- https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

3º Webinário de Segurança da Informação

Campanha Cidadania Digital

3º Webinário de Segurança da Informação

Sites

CTIRGov

https://www.gov.br/ctir

3º Webinário de Segurança da Informação

Sites

CTIRGov

https://www.gov.br/ctir

3º Webinário de Segurança da Informação

Sites

Secretaria de Segurança da Informação e Cibernética

Boletins Informativos Mensais

BIM nº 42
Cuidado com Links Maliciosos em Redes Sociais. Cartilha de Gestão de Segurança da Informação. Credenciamento de Segurança.

BIM nº 41
Privacidade no mundo digital. Tratamento de informações sigilosas. 1ª Reunião Ordinária do Comitê Gestor da Segurança da Informação.

BIM nº 40
Audiência Pública sobre a PNCiber. Proteja suas senhas contra os perigos do mundo virtual. Sigilo das informações pessoais tratadas no serviço público.

BIM nº 39
DIC. Promulgada a Convenção sobre o Crime Cibernético. Restrição de acesso à informação sobre pesquisa e desenvolvimento. Postura de Segurança Cibernética

Orientações de Seg. Info. e Cibernética

OSIC 14/2023
Ransomware

OSIC 13/2023
Vulnerabilidades do tipo Broken Object Level Authorization (BOLA)

OSIC 12/2023
Ataques cibernéticos contra usuários em trabalho remoto.

OSIC 11/2023
Autenticação Multifator (Multi-factor Authentication – MFA) e seus desafios

Notícias

3º Webinário de Segurança da Informação - 2023


III Diálogo Digital Brasil - Reino Unido


SSIC participa da 2ª edição da Caravana Federativa, no estado do Rio de Janeiro.

https://www.gov.br/gsi/dsic

3º Webinário de Segurança da Informação

Sites

Secretaria de Segurança da Informação e Cibernética

https://www.gov.br/gsi/dsic

3º Webinário de Segurança da Informação

Sites

Secretaria de Segurança da Informação e Cibernética

https://www.gov.br/gsi/dsic

3º Webinário de Segurança da Informação

Sites

Secretaria de Segurança da Informação e Cibernética

https://www.gov.br/gsi/dsic

3º Webinário de Segurança da Informação

Sites

Secretaria de Segurança da Informação e Cibernética

Legislação

Publicado em 24/11/2020 15h05 | Atualizado em 18/09/2023 16h31 Compartilhe:

K Portarias Instruções Normativas Normas Complementares Resoluções Publicações English Version

Lei

Nº da Lei	Ementa
Lei nº 12.737, de 30 de novembro de 2012.	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Lei nº 12.527, de 18 de novembro de 2011.	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; altera a Lei no 8.112, de 11 de dezembro de 1990; 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.

https://www.gov.br/gsi/dsic

3º Webinário de Segurança da Informação

Sites

Secretaria de Segurança da Informação e Cibernética

Legislação

Publicado em 24/11/2020 15h05 | Atualizado em 18/09/2023 16h31 Compartilhe:

K Portarias Instruções Normativas Normas Complementares Resoluções Publicações English Version

Lei

Nº da Lei	Ementa
Lei nº 12.737, de 30 de novembro de 2012.	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Lei nº 12.527, de 18 de novembro de 2011.	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; altera a Lei no 8.112, de 11 de dezembro de 1990; 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.

https://www.gov.br/gsi/dsic

3º Webinário de Segurança da Informação

Eventos

- Workshop voltado para desenvolvimento da nova Estratégia de Segurança Cibernética – GSI/LAC4
- Seminário de Segurança da Informação – GSI/LAC 4
- CMM – GSI/Reino Unido – Oxford University
- Curso de Open Source Inteligence – GSI/Reino Unido
- Webinário
- Seminário de Segurança da Informação para os Estados e o Distrito Federal
- CSIRT Training – GSI/LAC4

MUITO OBRIGADA!

MARINA CAMPOS LEÃO
Assistente Técnica
marina.leao@presidência.gov.br
Coordenação-Geral de Gestão de Segurança da Informação
Departamento de Segurança da Informação
SSIC/GSI/PR

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO