



GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO

GESTÃO DE SEGURANÇA DA INFORMAÇÃO: NORMAS E PADRÕES A SEREM APLICADOS NAS EMPRESAS

Autor: Me. Priscila de Fátima Gonçalves

Revisor: Rafael Maltempe

INICIAR



introdução

Introdução

A Segurança da Informação tem se tornado uma das ações mais importantes dentro de uma organização, pois a enorme circulação de informações no mundo digital faz com que esses dados fiquem expostos de maneira preocupante.

Nesta unidade, estudaremos a respeito de Segurança da Informação e sobre a importância frente às organizações. Serão apresentadas características de ambientes seguros que podem ser utilizadas em empresas de qualquer tamanho.

Veremos os princípios teóricos que são relacionados à Segurança da Informação nas atividades das empresas, bem como a comparação das estratégias de segurança utilizadas por elas.

Serão identificados e apresentados os benefícios existentes para organizações que tenham um Sistema de Gestão de Segurança da Informação certificado através de uma norma, como por exemplo, a ISO 27002.

Governança: Gestão da Segurança da Informação

As informações são evidentemente consideradas muitas vezes um dos principais patrimônios das organizações e, frequentemente, estão sob fortes riscos e ameaças. Pode-se dizer que o roubo ou a perda dessas informações ocasionaria um prejuízo sem tamanho para as empresas e, muitas vezes, pode fazer com que uma empresa deixe de existir caso isso ocorra.

As informações são consideradas úteis e reutilizáveis e possuem um enorme valor para o usuário; por isso, é primordial que estejam sob proteção, que estejam sempre disponíveis, que possuam controle de acesso, que sejam confiáveis e corretas. As informações têm como propósito habilitar a empresa e alavancar os objetivos através do uso eficiente dos recursos disponíveis. A perda das informações pode trazer prejuízos financeiros e até a descontinuidade do negócio, conforme citado no trecho anterior.

Segundo Stallings (2014), segurança de computadores refere-se à proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, disponibilidade e confidencialidade dos recursos do sistema de informação, onde são incluídos: hardware, software, firmware, informações/dados e telecomunicações.

A confidencialidade está ligada à confidencialidade de dados e à privacidade, onde é seguro que informações privadas e confidenciais fiquem indisponíveis para indivíduos sem autorização. Em relação à privacidade, parte-se do pressuposto que é assegurado que os indivíduos façam o controle ou influenciem informações relacionadas e como podem ser obtidas e armazenadas, assim como a quem serão reveladas as informações.

No que diz respeito à integridade, são tratados integridade de dados e do sistema e é assegurado que informações e programas sejam alterados somente da forma especificada e autorizada. Já a integridade do sistema permite que um sistema realize funcionalidades de forma ilesa e que seja livre de manipulações.

Sobre a disponibilidade, pode-se assegurar que os sistemas funcionem sempre e que os serviços estejam sempre disponíveis.

Para que se tenham garantias em relação às informações, as normas e procedimentos devem ser seguidos por todos dentro das organizações. Esta é uma dificuldade clara existente, ou seja, garantir que todos os funcionários conheçam e adotem normas e políticas de segurança, entendendo a importância e o quanto é relevante.

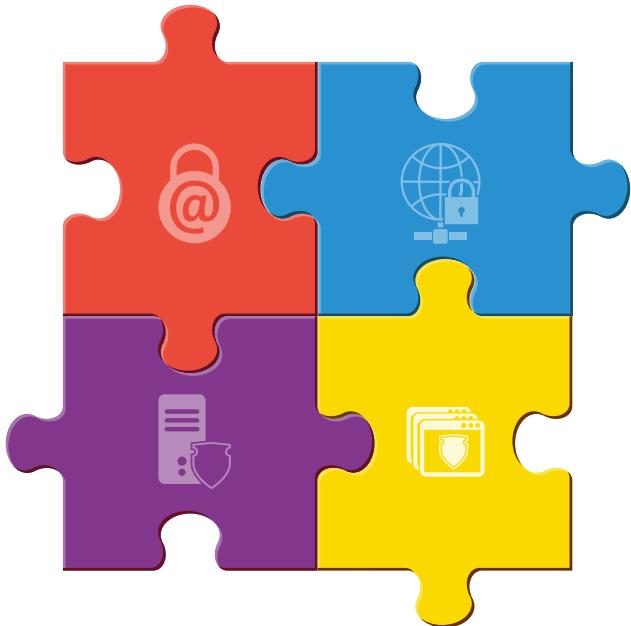
Na era do conhecimento o controle das informações também é fundamental, pois através dele os acessos aos programas, aos arquivos de dados, aplicações ou sistemas de software, acesso à rede, inovação tecnológica e projetos de grande valor são tratados de forma regrada pelos gestores de todas as áreas.

O que se pode ver no mercado é que as organizações passaram a considerar ambientes externos (enxergando as oportunidades e ameaças) e os ambientes internos (verificando as forças e fraquezas) e, através dessa visão, realizar o planejamento estratégico de segurança, minimizando riscos e impactos. As estratégias são em longo prazo, fragmentadas em objetivos de curto prazo e compartilhadas em linhas de processos, que são respectivamente: desenvolvimento de sistemas e softwares, coordenação de operações e comunicações, segurança ambiente, segurança física e

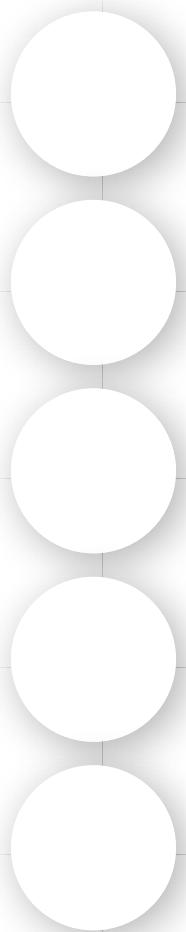
continuidade de negócios, de acordo com a ISO/IEC 27002.

Dentre as ações que podem ser tomadas para que as informações estejam fora de risco, encontram-se mapear e identificar a situação atual, sendo em empresa pública ou privada, detectando as ameaças, vulnerabilidades, riscos, sensibilidade e impactos, o que garantirá um correto dimensionamento e formação da solução.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



Uma **política de Segurança da Informação** garante a proteção sobre as informações das **organizações**, mas quando falamos em segurança, devemos lembrar que esta é subdividida em quatro partes:



No próximo item, abordaremos a importância e relevância da segurança da informação para empresas e organizações, e os principais quesitos de segurança que devem ser seguidos para que as informações sejam geridas e protegidas da melhor maneira.

Vamos Praticar

As informações são evidentemente consideradas muitas vezes como um dos principais patrimônios das organizações e, frequentemente, estão sob fortes riscos e ameaças. Diante dessa afirmativa, assinale a alternativa que corresponde aos objetivos da segurança da informação:

- a)** Informações são acessadas por qualquer colaborador da empresa.
- b)** O vazamento de informações deixa de ser um problema à organização.
- c)** Utiliza-se para implementar ações somente em uma categoria independente.
- d)** Utilizada para obter a rastreabilidade das alterações desde a solicitação até a implantação.
- e)** Asseguram que os sistemas funcionem sempre e que os serviços estejam sempre indisponíveis.

A Importância da Segurança da Informação para as Organizações

É inegável que estamos vivendo na era do conhecimento em um mundo cada vez mais digital, o que aumenta consideravelmente o grau de importância das informações geradas pelas corporações, informações estas que são cada vez mais sensíveis a ataques cibernéticos em tempo real. Por estes e outros motivos, é de extrema importância para empresas e organizações que essas informações sejam geridas e protegidas da melhor forma.

A importância da segurança da informação dá-se ao fato de que, como as informações são um dos maiores bens para a organização, elas devem ser “cuidadas” com todo o empenho. A grande motivação para que as organizações fiquem cada vez mais atentas à segurança da informação é que, cada vez mais o número de incidentes relacionados à segurança aumenta, causando transtornos muitas vezes irreversíveis para as empresas, principalmente na ordem financeira.

Saiba mais

Diante do que foi apresentado no capítulo, a segurança da informação tem três principais objetivos. Qual a importância da disponibilidade, integridade e confidencialidade da segurança da informação? Leia no livro: Criptografia e segurança de redes - princípios e práticas.

Fonte: Elaborado pelo autor.

[ACESSAR](#)

De acordo com Beal (2005), segurança da informação é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. Conforme Sêmola (2013), é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Logo, podemos definir a segurança da informação como uma área cujo objetivo é proteger a informação das ameaças mantendo a sua integridade, disponibilidade, confidencialidade, autenticidade e confiabilidade, para que seja garantida a continuidade do negócio e torne os riscos menores.

Serão apresentados os cinco objetivos da segurança da informação:

- Confidencialidade



Figura 1.1 - Confidencialidade

Fonte: Tashka2000 / 123RF.

A confidencialidade garante que as informações sejam acessadas somente por pessoas autorizadas, evitando assim que ocorra disseminação de informação sem autorização.

Segundo Stallings (2014), outros dois conceitos estão relacionados à confidencialidade, à confidencialidade de dados e à privacidade. A confidencialidade de dados garante que as informações privadas e confidenciais fiquem indisponíveis para pessoas não autorizadas. Já a privacidade garante que pessoas controlem quais informações sejam relacionadas a elas, possam ser obtidas e guardadas e, por quem podem ser reveladas.

- Integridade



Figura 1. 2 - Integridade

Fonte: Kchung / 123RF.

A integridade garante que conteúdos sejam mantidos de maneira segura e sempre protegidos, como por exemplo quando um arquivo não sofre nenhum tipo de dano. Os dados relevantes estão sempre protegidos contra falhas técnicas, com a utilização por exemplo do backup.

Segundo Stallings (2014), ao termo integridade estão relacionados dois conceitos, integridade de dados e integridade do sistema. A integridade de dados garante que informações e programas sejam modificados unicamente da forma especificada, assim como previamente autorizada. A integridade do sistema garante que este execute as funcionalidades pertencentes a ele de forma íntegra, livre de manipulações determinadas do sistema.

- Disponibilidade



Figura 1.3 - Disponibilidade

Fonte: Canjoena / 123RF.

Garante que os dados sejam acessados pelos usuários em qualquer momento. Está ligada à utilização de tecnologias móveis e cloud computing.

Segundo Stallings (2014, p.7), “a disponibilidade assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados”. Além disso, a disponibilidade deve garantir que o acesso seja rápido e confiável à informação.

- Autenticidade

Dados só podem ser acessados de acordo com permissões, como por exemplo a folha de pagamento de uma empresa.

De acordo com Stallings (2014, p. 7), “autenticidade é a propriedade de ser genuíno e capaz de ser verificado e confiável; confiança na validação de uma transmissão, em uma mensagem”. Assim, ocorre a verificação onde são validados se os usuários do sistema são quem dizem ser e se as fontes de acesso são confiáveis.

- Confiabilidade

Garante que os dados são e continuarão sendo relevantes e corretos. Como por exemplo, um software de gestão onde é possível delegar a aquisição e análise de dados para esses programas, permitindo mais rapidez em todo o processo.



Figura 1.4 - Confiabilidade
Fonte: Wrightstudio / 123RF.

Diante do que foi apresentado, pode-se afirmar que a segurança da informação não somente garante a proteção contra invasores externos, mas também previne que elas sejam comprometidas internamente, como no exemplo da folha de pagamento, onde qualquer funcionário que não tenha a autorização para alterá-la poderia causar um enorme prejuízo.

O Valor da Segurança da Informação

Um levantamento da National Retail Federation (2018) apresentou que cerca de 90% das invasões são dirigidas aos sistemas de pequenas e médias empresas, onde o custo que essas vulnerabilidades trouxeram foi de aproximadamente U\$D 36.000 anuais. Verificou-se ainda que além dos custos monetários, existem ainda os custos relacionados à perda de confiança de

clientes e parceiros, que pode fazer com que essas empresas sejam extintas do mercado.

Dentre as ameaças existentes, as mais comuns são ataques internos, que ocorrem quando alguém que possui acessos privilegiados os utiliza de má-fé, geralmente ocorre com ex-funcionários. Por esse motivo, assim que funcionários são desligados das empresas, faz-se necessária a retirada dos acessos e contas.

Há também os ataques relacionados a malwares, que são vírus, trojans e softwares mal-intencionados que fazem a exploração de vulnerabilidades em sistemas e vazam as informações para hackers.

Os ataques de senha são conhecidos na segurança da informação como uma ameaça também, onde através de algumas ferramentas específicas, força bruta ou engenharia social, os sistemas são afetados e colocados em risco.

O ataque DDoS ocorre quando um servidor é sobre carregado de forma intencional com muitas solicitações para que fique inacessível, um exemplo comum são sites do governo, que muitas vezes recebem esse tipo de ataque e ficam inacessíveis para os usuários.

Existem também as tentativas de phishing, consideradas uma das mais antigas estratégias de ataque explorada por cibercriminosos, onde ocorre a coleta de credenciais de acessos por meio de sites falsos que simulam com perfeição os verdadeiros existentes, como por exemplo sites de bancos.

reflita
Reflita

A segurança da informação é de uma importância muito grande nos dias de hoje, pois estamos vivendo uma era digital, onde informações sensíveis circulam a cada milionésimo de segundo na rede e, estamos vulneráveis a qualquer tipo de ataque, uma vez que utilizamos nossos dispositivos móveis

para realizarmos tarefas que exigem maiores cuidados, por exemplo, acesso a bancos e documentos oficiais.

Fonte: Elaborado pela autora.

Mas como garantir a segurança da informação diante de tantas possibilidades de ataques? A principal maneira é admitir que as ameaças existem e, utilizar firewalls, antivírus e backups para trabalhar com as aplicações virtuais. Uma outra forma de atuar é utilizar conexões seguras via https e criptografia, isso tanto para sistemas internos quanto em envios de formulários, pois será assegurada a inviolabilidade da informação. E, não podem faltar práticas de governança de TI, normas de segurança e planos de contingência (caso ocorra algum problema de segurança).

Saiba mais

Saiba mais

Existem controles que podem ser utilizados por gestores de segurança da informação para que as decisões sejam tomadas de forma mais assertiva na elaboração da política de segurança.

Leia no artigo a seguir mais a respeito da política de segurança da informação e os controles existentes para subsidiar tomadas de decisões por gestores.

Fonte: GALEGAL; FONTES; GALEGAL (2017).

[ACESSAR](#)

praticar

Vamos Praticar

Os programas existentes para a segurança da informação trazem, se executados corretamente, uma série de benefícios para as organizações. Entre eles, assinale a alternativa correta que apresenta quais são eles:

- a)** A identificação e correção das falhas e vulnerabilidades.
- b)** Deixa de atrair novos investidores aumentando o grau de satisfação dos atuais.
- c)** Ajuda a ajustar o fluxo operacional e gerar menos visibilidade sobre as atividades diárias.
- d)** Consegue recuperar o que investiu em forma de menos gastos.
- e)** Assegurar a continuidade da companhia, sem credibilidade e boa reputação no mercado.



Norma de Segurança



Norma técnica trata-se de um documento que deve ser desenvolvido por órgão oficial, ou seja, que tenha acreditação para realizar essa produção, assegura que produtos e serviços tenham características, como por exemplo, qualidade, segurança, confiabilidade e torna o desenvolvimento desses produtos e serviços mais seguros, eficientes e limpos, protegendo consumidores e usuários.

Em razão de interesse internacional em uma norma de segurança da informação, em dezembro de 2000, foi publicada a norma internacional ISO 17799:2000. Em 2001, a Associação Brasileira de Normas Técnicas (ABNT) publicou a versão brasileira, NBR/ISO 17799 - Código de Prática para a Gestão da Segurança da Informação (OLIVA; OLIVEIRA, 2003). Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. Segundo Holanda (2006), o comitê que trata da segurança da informação na ISO aprovou a criação de uma família de normas sobre gestão da segurança da informação, batizada pela série 27000, onde a então ISO IEC 17799:2005 foi rebatizada por ISO IEC 27002:2005. A norma ABNT ISO/IEC 27002:2005 tem por objetivo estabelecer diretrizes sobre as metas geralmente aceitas para a

gestão da segurança da informação e apresenta 133 controles (ABNT, 2005).

De acordo com Silva Netto e Silveira (2007), a norma NBR ISO/IEC 27002:2005 (ABNT, 2005) está dividida em 11 seções que possuem controles de segurança da informação, que englobam categorias principais de segurança. Cada uma das categorias principais contém: objetivo de controle que deve ser alcançado e, um ou mais controles que podem ser utilizados para alcançar o objetivo de controle em questão. As 11 seções e respectivas quantidades de categorias principais com a correspondente quantidade de controles são (ABNT, 2005):

- a) Política de Segurança da Informação: 1 categoria e 2 controles;
- b) Organizando a Segurança da Informação: 2 categorias e 11 controles;
- c) Gestão de Ativos: 2 categorias e 5 controles;
- d) Segurança em Recursos Humanos: 3 categorias e 9 controles;
- e) Segurança Física e do Ambiente: 2 categorias e 13 controles;
- f) Gestão das Operações e Comunicações: 10 categorias e 32 controles;
- g) Controle de Acesso: 7 categorias e 25 controles;
- h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: 6 categorias e 16 controles;
- i) Gestão de Incidentes de Segurança da Informação: 2 categorias e 5 controles;
- j) Gestão da Continuidade do Negócio: 1 categoria e 5 controles;
- k) Conformidade: 3 categorias e 10 controles.

A conformidade de qualquer organização à norma ISO IEC 27002:2005 certifica conformidade com melhores práticas em gestão da segurança da informação. De acordo com Holanda (2006), normas são criadas para que sejam determinadas diretrizes e princípios com a finalidade de tornar a gestão de segurança nas empresas e organizações melhores.

praticar

Vamos Praticar

A norma ISO IEC 27002 define 127 controles que compõem o escopo do Sistema de Gestão de Segurança da Informação (Information Security Management System - ISMS), agrupados em 11 seções de controle. Assinale a alternativa que contém ao menos 3 delas.

- a)** Desenvolvimento e Manutenção dos Sistemas de Informação; Gestão de Incidentes da Segurança da Informação e criptografia de dados e senhas.
- b)** Gestão de Incidentes da Segurança da Informação, criptografia de dados e senhas e Comunicações e falhas vindas da criptografia.
- c)** Desenvolvimento e Manutenção dos Sistemas de Informação, Gestão das Operações e Comunicações e falhas vindas da criptografia.
- d)** Gestão das Operações e Comunicações; Controle de Acesso e Aquisição.
- e)** Comunicações e falhas vindas da criptografia, Gestão das Operações e Comunicações, realizar ações que mapeiem e identifiquem a situação atual na instituição.

Aplicação dos Princípios Básicos de Segurança da Informação em Empresas, de Acordo com o Mercado em que Atua

As atuações de segurança da informação têm como objetivo dificultar ao extremo o trabalho de um hacker que pretende invadir as informações da empresa. Assim, quando uma organização se resguarda, o possível invasor encontrará mais dificuldades ao tentar entrar no sistema. Logo, achará mais viável tentar invadir um sistema mais vulnerável.

Pode-se citar como exemplo a utilização de aplicativos bancários para dispositivos móveis, algo que vem crescendo desde a sua implantação. Segundo a Trend Micro, empresa considerada líder em consultoria e produtos utilizados em estratégias de segurança pelo The Forrester Wave™: Cloud Workload Security em 2019, os invasores estão utilizando métodos diferentes para comprometer serviços disponibilizados aos usuários, como por exemplo aplicativos falsos, ataques através de redes maliciosas e roubos de credenciais. Outra preocupação são os trojans, como por exemplo o malware Aunbis, que em 2019 adotou sensores baseados em movimento para evitar a análise de sandbox e sobreposições para roubar informações de identificação pessoal ou ainda, aplicativos falsificados como por exemplo o Trojan Ginp, que rouba as informações de login e cartão de crédito dos usuários.

Para evitar esses tipos de ataques, a Trend Micro oferece algumas dicas de segurança, como por exemplo, baixar os aplicativos bancários somente de fontes confiáveis, atualizar sempre que houver uma versão nova (desta forma as vulnerabilidades serão corrigidas mais rapidamente), habilitar recursos de segurança internos, utilizar somente conexões em redes seguras e sempre com a wi-fi e bluetooth desligados. Também é interessante que seja habilitada a autenticação em dois fatores, senhas fortes e exclusivas para cada um dos aplicativos (caso o usuário trabalhe com mais de um banco) e, sempre monitorar atividades em suas contas bancárias.

Na execução de algumas medidas realizadas por organizações, são recomendadas soluções mais potentes e complexas e não apenas a instalação de antivírus e atualizações de softwares e sistemas e de senhas.

Uma proteção mais competente é realizada através de políticas de segurança, geralmente implementadas por meio de consultoria de segurança da informação por especialistas, que trabalham com normas e procedimentos testados e aprovados.

praticar

Vamos Praticar

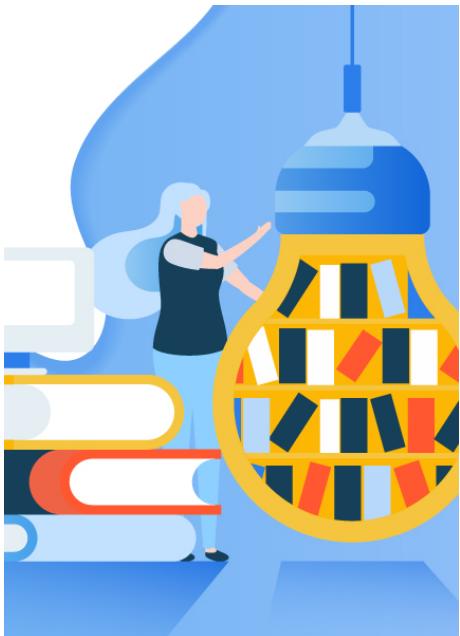
A fim de obtermos uma segurança da informação adequada, o que é uma necessidade nos dias atuais, devido ao aumento de incidentes a segurança, e a grande necessidade de proteger as informações das organizações, deve-se criar uma política de segurança da informação que garanta essa proteção, isso é fundamental dentro do ambiente corporativo. A segurança pode ser subdividida em:

- a) Computacional, física e lógica.

- b)** Pessoal, interpessoal e hardware.
 - c)** Software, hardware e computacional.
 - d)** Lógica, pessoal e funcional.
 - e)** Pessoal, software e funcional.
-

indicações

Material Complementar



LIVRO

Fundamentos de Segurança da Informação. Com Base na ISO 27001 e na ISO 27002

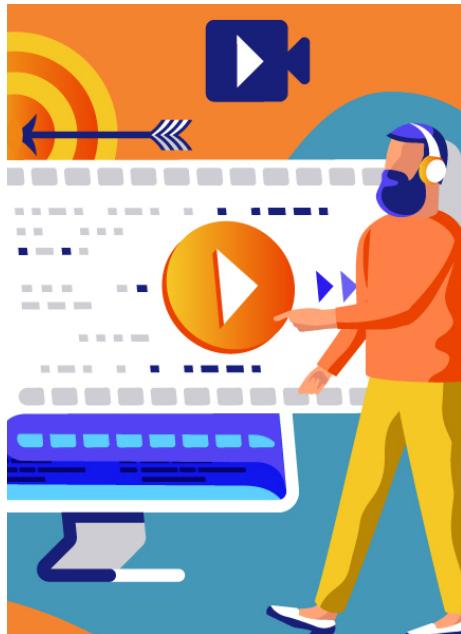
Hans Baars, Kees Hintzbergen, Jule Hintzbergen, André Smulders

Editora: Brasport Livros e Multimídia Ltda.

ISBN: 978-85-845-2867-0

Comentário: Este livro é indicado para que vocês possam entender de forma clara as abordagens e políticas de gerenciamento de segurança da informação, pois colabora com a análise e implementação da mesma nos negócios. Tem base nas normas ISO/IEC 27001 e ISO/IEC 27002, e traz referências de padrões internacionais de segurança da

informação.



FILME

A senha: Swordfish

Ano: 2001

Comentário: Em sua sinopse, o filme mostra que há um mundo disfarçado sob o que chamamos de ciberespaço, que é protegido por firewalls, senhas e os mais evoluídos sistemas de segurança. E, neste local estão guardados os maiores segredos, as informações mais incriminadoras e, muito dinheiro. É apresentado um hacker super conceituado que tem conhecimento e talento para quebrar os sistemas de segurança mais fechados do mundo. Através deste filme será possível dimensionar o quanto é importante a proteção das informações sensíveis.

TRAILER

conclusão

Conclusão

Diante do tema abordado nesta unidade, pode-se ressaltar a importância da segurança da informação para empresas de qualquer porte, pois uma falha pode ocasionar a extinção da empresa, por motivos financeiros ou por falta de confiança do mercado em que atua junto aos clientes e parceiros. Pode-se verificar diante do exposto que, diante da digitalização, é de extrema importância o controle de acessos aos programas, dados, aplicações e acesso à rede. É grande a importância de conscientização dos funcionários em relação à segurança da informação, por isso, a questão de treinamentos deve estar sempre presente. É notável também que um plano de continuidade de negócio é de extrema importância, pois é a única forma de responder a respeito dos problemas encontrados referentes à segurança da informação.

referências

Referências Bibliográficas

2018 NATIONAL RETAIL SECURITY SURVEY. [2018]. Disponível em: <https://nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf>. Acesso em: 11 dez. 2019.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005** : Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013** : Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

BEAL, A. **Segurança da Informação** : princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política da Segurança da Informação** : Guia Prático para Elaboração e Implementação. 1. ed. Rio de Janeiro: Ciência Moderna, 2006.

GALEGAL, N. V.; FONTES, E. L. G.; GALEGAL, B. P. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. **Perspect. ciênc. inf.**, Belo Horizonte, v. 22, n. 3, p. 75-97, set. 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362017000300075&lng=pt&nrm=iso. Acesso em: 11 dez. 2019.

HOLANDA, R. de. **O estado da arte em sistemas de gestão da segurança da Informação** : Norma ISO/IEC 27001:2005. São Paulo: Módulo Security Magazine, 19 jan. 2006. Disponível em: <https://pt.scribd.com/document/353991140/norma-ISO-IEC-27001-2005-pdf>. Acesso em: 14 jan. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 17799:2000 Information technology** - Code of practice for information security management. Geneva: ISO/IEC, 2000.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001:2006 Information technology** - Security techniques - Information security management systems - Requirements. Geneva: ISO/IEC, 2006.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL

ELECTROTECHNICAL COMMISSION. **ISO/IEC 27002:2005 Information technology** - Code of practice for information security management. Geneva: ISO/IEC, 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27002:2013 Information technology** - Code of practice for information security management. Geneva: ISO/IEC, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO Survey 2014**. 2014. Disponível em: <http://www.iso.org/iso/iso-survey>. Acesso em: 2 fev. 2016.

MOBILE money: how to secure banking applications. 27 dez. 2019. Disponível em: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mobile-money-how-to-secure-banking-applications>. Acesso em: 4 jan. 2020.

OLIVA, R. P.; OLIVEIRA, M. Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799. In: ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO (ENANPAD), XXVII, 2003, Atibaia. **Anais[...]**. Atibaia: ANPAD, 2003.

SÊMOLA, M. **Gestão da Segurança da Informação** : uma visão executiva. Rio de Janeiro: Campus, 2013.

SILVA NETTO, A. da; SILVEIRA, M. A. P. da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM J. Inf. Syst. Technol. Manag.** (Online), São Paulo, v. 4, n. 3, p. 375-397, 2007. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752007000300007. Acesso em: 28 nov. 2019.

STALLINGS, W. **Criptografia e Segurança de Redes** : princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2014.