GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO

FRAMEWORKS PARA GESTÃO DE RISCOS, ESTRATÉGIAS E CONSCIENTIZAÇÃO PARA AS ORGANIZAÇÕES

Autor: Esp. Priscila de Fátima Gonçalves
Revisor: Rafael Maltempe

INICIAR

introdução

Introdução

Nesta unidade serão identificadas as normas de segurança da informação, assim como descritos os benefícios existentes para uma organização em utilizá-las.

Serão apresentados os conceitos relacionados à Política de Segurança da Informação e os desafios para que sejam adotadas pelas empresas, desafios estes que serão analisados de forma consistente.

Veremos como são as estruturas de uma Política de Segurança da Informação, bem como são identificadas as estratégias para que ocorra a conscientização de sua importância para as organizações.

Abordaremos ainda, frameworks envolvidos com a Gestão de Riscos e estratégias de segurança da informação para os principais riscos envolvidos no ambiente de Tecnologia das organizações.

Política de Segurança da Informação e Desafios para a Adoção nas Organizações

Uma política de segurança da informação, pode ser definida como instruções que devem ser seguidas para que as organizações fiquem protegidas e para que haja uma gestão de segurança da informação correta.

De acordo com Sêmola (2014, p.105), “a política tem um papel fundamental e, guardada as devidas proporções, tem importância similar à Constituição Federal de um país”.

Para Trcek (2000), trata-se de um processo que ocorre de forma contínua, que estabelece, redefine e implementa objetivos relacionados à segurança de acordo com estrutura e missão da empresa e que possui relações com os níveis de recursos dos sistemas de informação.

Ainda, conforme consta na norma BNT NBR ISO/IEC 27002 (2013, p.2), o objetivo de uma política de segurança da informação é “Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentos relevantes”.

É de grande importância que as organizações tenham uma política de

segurança eficaz, porém além de tê-la, é necessário que todos os colaboradores a adotem corretamente. Certa empresa, que possuía uma política de segurança da informação que trabalhava com os dados de aproximadamente vinte e quatro mil clientes, teve uma grande falha cometida por um de seus colaboradores. Este colaborador foi enviar uma planilha para seus clientes, nessa planilha constavam os produtos que trabalhavam e quem eram os responsáveis pelas vendas e promoções deles. Para que ele obtivesse essas informações, foi realizada uma consulta no banco de dados, do qual mais informações, além dos nomes e setores, como por exemplo cargos e salários, foram extraídas para essa planilha. Ao realizar o envio, o colaborador não se deu conta de que as informações estavam em colunas ocultas no excel e, desta forma, divulgou informações confidenciais. Após o ocorrido, a empresa teve que arcar com custas de processos e pagamentos por danos que foram reivindicados na justiça. A empresa também teve que lidar com perda de credibilidade perante os clientes e colaboradores. Diante da exposição deste caso ocorrido, fica evidente que todos os colaboradores devem aderir à política de segurança da informação nas empresas, para que falhas graves como essa não ocorram.

A política de segurança da informação é de grande importância, assim como uma Constituição Federal para o país, pois ela garante que as informações serão preservadas contra qualquer ameaça que possa ocorrer, quando seguida de forma correta.

saiba mais

Saiba mais

Acesse o link e entenda mais a respeito do comportamento e das ações realizadas pelos usuários que colocam em risco ou protegem os sistemas de informação por eles utilizados. O artigo fala da importância dos usuários para manter os sistemas das empresas protegidos.

ACESSAR

Geralmente, sua definição ocorre por meio do setor estratégico da organização e, somente depois é levada para os outros funcionários e a quem quer mais que seja relevante sua apresentação. A política de segurança da informação normalmente vai ao encontro da dificuldade que cada organização tem em permanecer com as informações sensíveis protegidas.

Assim, a elaboração de uma política de segurança coerente deve ser criada de acordo com os pontos mais frágeis aos quais a organização esteja exposta, de acordo com o que cada uma delas carece e também deve ser analisada e aprovada pela equipe estratégica de cada empresa.

saiba mais

Saiba mais

Acesse o link e entenda mais a respeito da importância da política de segurança e as técnicas de proteção aos sistemas de informação. O artigo aborda a importância de uma política de segurança da informação em pequenas e médias empresas e apresenta de que maneira as empresas recebem essa

política.

Fonte: Elaborado pelo autor.

ACESSAR

Dentre as características da Política de Segurança da Informação, pode-se citar que ela está subdividida em diretrizes, normas e procedimentos.

A Figura 2.1 desta unidade, apresenta o diagrama de conceito dos componentes integrantes da política de segurança e as bases de sustentação e personalização.

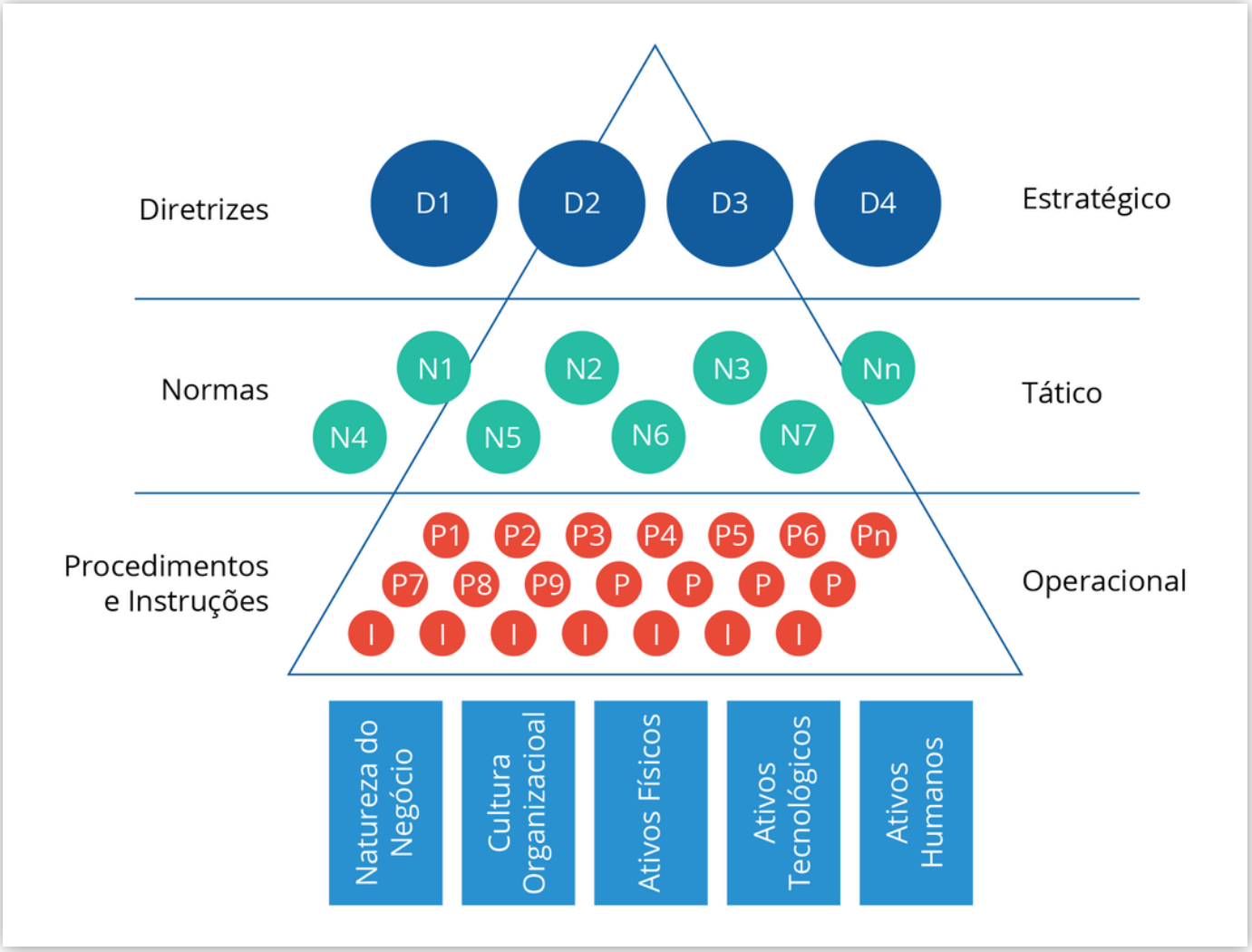


Figura 2.1 - Diagrama de componentes de política de segurança
Fonte: Sêmola (2014, p.106).

A partir do diagrama apresentado, pode-se verificar que o número de normas será de acordo com o nível de detalhes que uma empresa precisa e, que essas

normas, diretrizes e procedimentos devem ser utilizados para a manutenção da segurança da informação. Ainda pode-se dizer que as informações são os ativos de maior importância para a empresa e que é muito importante ter o apoio da área estratégica para descrever a segurança da informação. Também é necessário mostrar claramente que os funcionários são responsáveis, de maneira formal, por manter as informações protegidas e que deve ocorrer o estabelecimento de práticas que mantenham a segurança da informação.

Para que uma política de segurança da informação seja eficiente e eficaz, a organização deve envolver a equipe estratégica para seu concebimento e fazer com que os demais funcionários sejam responsáveis por manter as informações protegidas, estabelecendo práticas para que a manutenção da segurança ocorra sempre.

Desta forma, é necessário que a alta gerência das empresas dê seu apoio e, posteriormente, é necessária a criação de uma Comissão de Segurança da Informação, a qual deverá ter a participação de colaboradores de diferentes áreas do negócio dentro da empresa. Essa comissão será responsável por documentar todos os processos dentro da empresa que sejam relacionados às informações, colocando-as em ordem por categorias. No próximo item será descrita a estrutura de uma Política de Segurança da Informação.

praticar

Vamos Praticar

Segurança da Informação é definida pelo ISACA como algo que tem como objetivo garantir que a informação seja protegida da divulgação a pessoas não autorizadas (_____), de modificações inadequadas (_____) e de falta de acesso quando solicitado (_____) nas organizações.

Assinale a alternativa que contém as palavras que completam as lacunas corretamente.

- **a)** disponibilidade, confidencialidade e organização.
- **b)** confidencialidade, integridade e disponibilidade.
- **c)** integridade, disponibilidade e confidencialidade.
- **d)** organização, integridade e confidencialidade.
- **e)** disponibilidade, integridade e confidencialidade.

Estrutura de uma Política de Segurança da Informação

As políticas de segurança da informação possuem fatores comuns entre elas, mesmo que em diferentes organizações de diferentes segmentos. Como por exemplo, a descrição da política, a declaração de conformidade, especificação dos profissionais que desenvolverão a política, a referência aos regulamentos internos, a comunicação dos procedimentos de solicitações de exceções, o controle da atualização da política e a assinatura do principal executivo da organização que a autorizará na empresa.

Para que uma política de segurança da informação seja desenvolvida, é necessário que algumas etapas sejam seguidas. De acordo com Ribeiro (2016), abaixo serão explicadas as quatro etapas para o desenvolvimento.

Etapa I

A primeira etapa do desenvolvimento da política de segurança da informação é a elaboração de um questionário, no qual serão abordadas as informações sobre a empresa/organização. Nesse questionário, a meta é analisar se há ou houve uma política implementada, buscar informações sobre o ambiente de

negócio da empresa, verificar o ambiente tecnológico e concernir necessidades e utilização dos recursos tecnológicos nos processos existentes no negócio.

Nesta etapa, o questionário é aplicado a todos os colaboradores, desde os gestores até a menor camada hierárquica da organização. Assim, é possível analisar se existe uma política implementada e se é do conhecimento de todos na empresa.

Etapa II

A segunda etapa do desenvolvimento da política de segurança da informação é onde deve ser definido o gerenciamento da política, em que serão tratados temas como: definição de segurança, objetivo do gerenciamento, fatores críticos de sucesso de sua implementação e gerenciamento de versões bem como manutenções.

Ainda nesta etapa, serão realizadas as atribuições de normas e responsabilidades no que diz respeito à criação da Comissão de Segurança da Informação. Essas atribuições são direcionadas aos proprietários da informação, às áreas de segurança, aos usuários de informações, aos recursos humanos, bem como à auditoria interna.

As informações serão classificadas de acordo com o nível, reclassificações, armazenamento e descarte.

Fazem parte desta etapa os procedimentos de segurança tais como: classificação e tratamento da informação, notificação e gerenciamento de incidente, processos disciplinares, compra e utilização de hardwares e sistemas, proteção contra sistemas maliciosos, segurança e tratamento de mídias, uso da internet, utilização de e-mail, uso de recursos de TI, backup, manutenção de equipamentos e testes, coletas de falhas, controle de redes, monitoramento de acessos e utilização de sistemas, administração de criptografias e gestão de chaves, domínio de mudanças de operações, inventário de ativos de informações, controle de acesso físico em setores

sensíveis, segurança física, bem como a supervisão de visitantes e prestação de serviços de terceiros.

Etapa III

Na terceira etapa do desenvolvimento da política de segurança da informação devem ser elaborados os procedimentos de Segurança da Informação, contemplando os seguintes itens: pesquisa sobre melhores práticas a serem adotadas pela organização, a criação de regras bem como padrões para serem mostrados e discutidos com a alta gerência (verificando o que foi definido sobre as melhores práticas) e de acordo com a necessidade da empresa e, por fim, a apresentação dos procedimentos que deverão ser incorporados às políticas da empresa.

Etapa IV

A quarta e última etapa do desenvolvimento da política de segurança da informação é aquela na qual deve ocorrer a revisão, aprovação e a implementação da Política de Segurança da Informação na empresa e deve ser realizada da seguinte maneira: todas as regras, normas e procedimentos devem ser revisados e aprovados. Assim, ocorrerá a implementação em si, que deverá ser acompanhada pela equipe que fará a divulgação da nova política, nela constará as devidas responsabilidades dos funcionários.

praticar

Vamos Praticar

De acordo com a norma ABNT NBR ISO/IEC 27002 (2013, p.2), na Gestão da Segurança da Informação, implantar a segurança envolve a adoção de mecanismos para a segurança física. Uma das formas de prover a segurança física em uma empresa é:

- **a)** Estabelecer que os acessos aos computadores e estações de trabalho da organização sejam realizados com cartões inteligentes e biometria.
- **b)** Descriptografar mensagens transmitidas por meio de correio eletrônico entre todos os setores da organização.
- **c)** Implantar Firewall em todos os computadores e servidores da organização para monitorar e controlar os acessos, exceto para fornecedores terceiros.
- **d)** Usar protocolos de troca de informação seguros, como HTTPS, para a divulgação das informações comerciais e pessoais de funcionários da organização.
- **e)** Manter todas as portas corta-fogo dentro do perímetro de segurança tenham alarme, sejam monitoradas e testadas, bem como as paredes.

Estratégias de Implementação de Políticas de Segurança da Informação e a Importância de Conscientizar os Colaboradores

É importante que as organizações tenham estratégias para implantar as políticas de segurança da informação, pois as pessoas, ou seja, os recursos humanos são a parte mais frágil e têm uma maior probabilidade de serem manipulados perante a gestão de segurança.

De acordo com Fernandes e Abreu (2006), dentre os fatores que fazem empresas estudarem seus modelos de gestão de tecnologia da informação estão: a complexidade, que está cada vez maior entre todos os envolvidos e a dependência tecnológica utilizada pelo negócio, bem como a integração de sistemas e solução, necessidades conflitantes dos negócios, redução de custos, aumento de flexibilidade e agilidade, responsabilidade legal, transparência por parte de acionistas e do mercado, mudança de perfil de concorrentes e o aumento considerável de ameaças e vulnerabilidades em TI.

De acordo com Kruger & Kearney (2008), questões de segurança devem ser levadas aos usuários para que eles entendam a dimensão de sua importância

e os efeitos que causam as possíveis falhas.

De acordo com Sêmola (2014, p.128), “O ser humano é uma máquina complexa, dotada de iniciativa e criatividade, que sofre interferência de fatores externos, provocando comportamentos nunca antes experimentados".

Diante dessa afirmação, percebe-se quanto o ser humano é imprevisível e pode ser facilmente manipulado, tornando-se a porta de entrada para ameaças e ataques a uma organização. Assim, o desafio de conscientizar os funcionários da empresa é grande e faz-se necessária a criação de estratégia para que se alcance a todos da mesma forma.

saiba mais

Saiba mais

Os usuários fazem parte dos elementos que podem provocar vulnerabilidades e possíveis danos em sistemas de informação, por isso torna-se necessário verificar se estão conscientes da utilização de maneira correta e segura no desempenho das suas tarefas.

Leia no artigo mais a respeito da política de segurança da informação e a importância de conscientização dos usuários.

ACESSAR

Entre as estratégias utilizadas, pode-se afirmar que o treinamento e a disponibilização de materiais de apoio fazem com que os usuários estejam sempre atualizados no que diz respeito às políticas de segurança da informação da organização. Para que esse processo ocorra da melhor forma possível, é necessário que sejam realizados avisos através de e-mails, internet, cartazes, palestras e seminários, apresentando os riscos e os impactos a eles associados. São necessários também treinamentos e capacitações para funcionários, como, por exemplo, os administradores de redes devem ser

capazes de combater ataques e invasões. Poderá ser feita também uma carta pelo CEO da empresa relatando a importância da política e sua vontade de que a mesma seja seguida, além de um termo de responsabilidade cuja função é tornar oficial o ato de que o funcionário sabe quais são suas obrigações de proteção de informação sobre a qual tem acesso, bem como as penalidades a serem executadas caso ocorram desvios de conduta.

praticar

Vamos Praticar

A Política de Segurança da Informação trata-se de um documento que divulga as condutas de segurança da informação, estas devem estar de acordo com os objetivos da empresa, deve ser sabida e reconhecida por todos os colaboradores. Tem como objetivo promover:

- **a)** Regras de criação de processos pertinentes ao negócio e aos colaboradores.
- **b)** Controle sobre processos de TI.
- **c)** Orientações embasadas nos requisitos do negócio da organização, de acordo com as leis e regulamentações.
- **d)** Metodologia para renovar soluções de segurança da informação.
- **e)** Recursos financeiros para proteger as informações da organização contra ações perigosas.

Frameworks Envolvidos na Gestão de Riscos

Frameworks são considerados modelos que contêm ferramentas e regras ou normas que as organizações devem seguir para que os riscos sejam geridos de forma eficiente. Geralmente, esses modelos são vastos e não devem ser implementados em sua íntegra, pois devem ser adequados a cada tipo de negócio, verificando a necessidade de cada organização.

No mercado, hoje em dia, há vários modelos disponíveis, entre eles pode-se citar o IHI, utilizado para a gestão de riscos de organizações, direcionados para cuidados da saúde. Há também o Value at Risk, um modelo usado para avaliação de riscos de ativos financeiros; outro modelo é o Auditing Standard No.2 do PCAOB (Public Company Accounting Oversight Board, Conselho de Supervisão Contábil de Empresa Pública), trata-se de um modelo americano de auditoria que controla riscos relacionados a fraudes financeiras; já o COBIT é um modelo utilizado para gestão de riscos e governança; o ISO 31000 é utilizado para gestão de riscos e o Coso é utilizado para a gestão integrada de riscos.

Entre os frameworks citados acima, os dois últimos são os mais utilizados, e isso se deve ao fato de serem de mais fácil adaptação aos setores de negócios.

Coso tem por finalidade analisar fraudes em relatórios financeiros e da área de contabilidade, desenvolvendo recomendações a serem seguidas por empresas públicas e auditoria independente, desta forma, alinhando processos ao gerenciamento de riscos.

Independentemente do framework escolhido para ser utilizado na empresa, será necessário sempre realizar as atividades de identificação de riscos e definição de respostas àqueles encontrados

O COBIT (Control Objectives for Information and Related Technology), criado em 1994 pela Information Systems Audit and Control Foundation (ISACF), a partir de um conjunto de objetivos de controle, evolui por meio da incorporação de padrões internacionais técnicos, profissionais, regulatórios e específicos para processos de TI (ISACA, 2008).

Em 1998 foi publicada a segunda edição que contém uma revisão nos objetivos de controle de alto nível e seu detalhamento, assim como um conjunto de ferramentas e padrões para implementação (ISACA, 2008). Já, a terceira edição publicada em 2000 pelo IT Governance Institute (ITGI), órgão criado pela Information Systems Audit and Control Association (ISACA) tem como objetivo promover entendimento melhor e adotar princípios de governança de TI (FERNANDES e ABREU, 2006). O COBIT fornece um conjunto de procedimentos cheio de detalhes e diretrizes que devem ser aplicados na auditoria dos processos de TI, bem como uma avaliação dos riscos e probabilidades de ocorrência (ISACA, 2008).

A implementação do framework sempre terá como objetivo realizar a integração da gestão e do controle de segurança, bem como realizar a avaliação dos riscos e das políticas de segurança da informação, buscando manter a conformidade com as normas e padrões regulatórios existentes, como por exemplo, ABNT NBR ISO/IEC 27002 (2013), realizando a integração entre controle interno e planejamento estratégico.

praticar

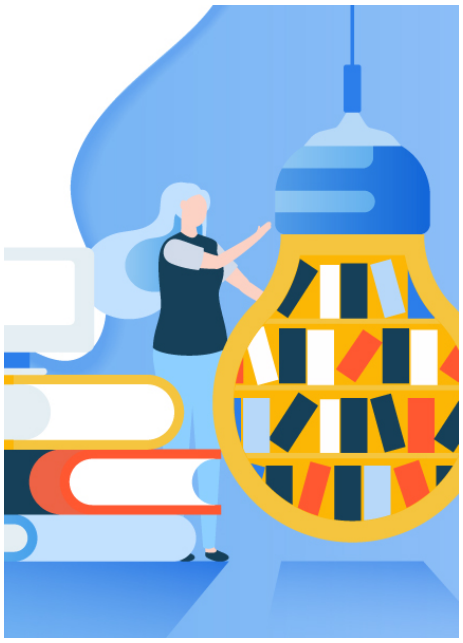
Vamos Praticar

O COBIT tem como objetivo a governança de TI. Porém, serve para dar atenção ao foco do negócio ao invés de simplesmente verificar os serviços de TI. Assinale a alternativa que apresenta seus benefícios.

- **a)** Otimiza os investimentos em Tecnologia da Informação, aumenta a produtividade e a satisfação dos usuários.
- **b)** Fortalece o combate à fraude, diminui a eficiência da TI e melhora desempenho da segurança da informação.
- **c)** Aumenta a eficiência da Tecnologia da Informação, melhora a segurança da informação e cria uma linguagem comum.
- **d)** Viabiliza investimentos em TI, diminui a produtividade e problemas e diminui a satisfação e motivação dos funcionários. D.
- **e)** Aumenta a eficiência da TI, diminui a produtividade e problemas e diminui a satisfação e motivação dos funcionários.

indicações

Material Complementar



LIVRO

Investigação Digital em Fontes Abertas

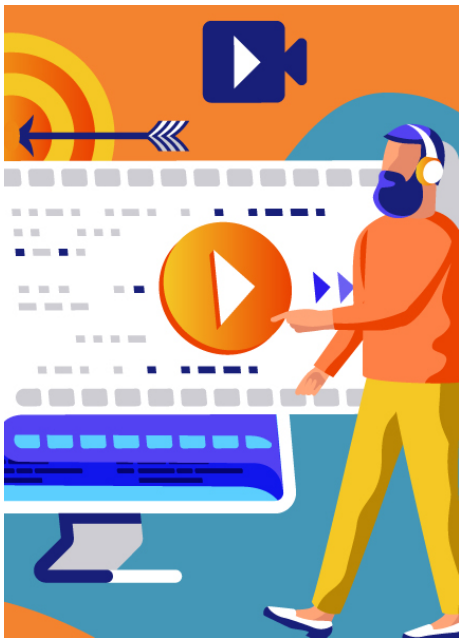
Alessandro Gonçalves Barreto

Editora: Editora Brasport

ISBN: 8574528145

Comentário: Tarefas relacionadas à inteligência de segurança pública e de investigação no âmbito policial têm maximizado a utilização de fontes abertas para produzir conhecimento ou provas. Muitos são os casos bem-sucedidos de prisão, localização de foragidos, identificação de testemunhas e produção de provas com informações disponíveis de forma livre na web. Este livro mostrará como auxiliar as pessoas em investigações modernas, em que ocorrem inclusive a

coleta de informações por meio do Facebook e na Deep Web.



FILME

O quinto poder

Ano: 2013

Comentário: Julian Assange conta com o apoio de Daniel Domscheit-Berg para fundar o site WikiLeaks. Esse site tem como objetivo apresentar uma plataforma para que as pessoas possam realizar denúncias anônimas, mostrando segredos de governo e crimes de empresas. No decorrer do tempo, eles passam a dar informações inéditas ao público, antes da mídia convencional.

Para conhecer mais sobre o filme, acesse o trailer disponível.

TRAILER

conclusão

Conclusão

No que tange a Políticas de Segurança da Informação, frameworks de gestão de riscos e estratégias para a implementação das políticas e normas, esta unidade deixa clara a importância e a necessidade de que as empresas as implementem. Sejam empresas de grande, médio ou de pequeno porte, cada uma com suas políticas adequadas ao seu modelo de negócio devem fazer com que todos os colaboradores entendam a real importância da utilização e implementação das políticas.

É notório que se os colaboradores não estiverem engajados com a causa, os riscos aumentam consideravelmente, pois, como vimos, os seres humanos são manipuláveis de fácil acesso.

referências

Referências Bibliográficas

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.

BARRETO, A. G. **Investigação digital em fontes abertas** . 2. ed. Rio de Janeiro: Brasport, 2017.

FERNANDES, A. A.; ABREU, V. F. **Implantando a governança de TI** : da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2006.

FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Políticas de Segurança da Informação** : Guia Prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2008.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). **COBIT 4.1** . Rolling Meadows: ISACA, 2008.

KRUGER, H. A.; KEARNEY, W. D. Consensus Ranking - An ICT security awareness case study. **Computers & Security** , Amsterdam, v.27, n.7, p.493-508, 2008.

LYRA, M. R. **Segurança e auditoria em sistemas de informação** . Rio de Janeiro: Ciência Moderna, 2008.

RIBEIRO, C. Segurança da Informação: o desenvolvimento de uma política de segurança da informação em conformidade com a norma **ABNT ISO/IEC 27002** . Ano 2016. 35 páginas. Trabalho de Conclusão de Curso de Sistema de Informação – FAIR Faculdades Integradas de Rondonópolis, 2016.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva** - 2 ed. São Paulo: Elsevier, 2014.

TAROUCO, H.; GRAEML, A. **Governança de tecnologia da informação** : um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. Disponível em: https://www.sciencedirect.com/science/article/pii/S0080210716302187 . Acesso em: 20 dez. 2019.

TRCEK, D. Security policy conceptual modeling and formalization for networked information systems. **Computer Communications** , v.23, n.17, p. 1716-1723, 2000.