

GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO

COMPLIANCE : AUDITORIA DE SISTEMAS E PERÍCIA FORENSE

Autor: Me. Priscila de Fátima Gonçalves

Revisor: Rafael Maltempe

INICIAR

introdução

Introdução

Compliance é um termo bastante utilizado por organizações nos dias atuais. Mas, afinal, o que é *compliance*? Para que serve? Quais os benefícios? Essas e outras perguntas serão respondidas no decorrer desta unidade.

Compliance significa estar em conformidade com as obrigações legais, situação em que a

organização tem responsabilidades em relação a proteção à saúde, bem-estar e segurança para com os colaboradores, principalmente no que diz respeito a contratações, demissões, assédio, segurança, benefícios, folha de pagamento, salários e discriminação. Essa conformidade estende-se a normas, regulamentos e leis que norteiam as atividades das organizações, para que se evitem problemas, como, por exemplo, corrupção e falta de ética.

Nesta unidade, serão apresentados conceitos envolvidos com auditoria de sistemas, aplicação de melhores práticas de *compliance*, bem como a avaliação delas e conhecimentos relativos à perícia forense.

Compliance



Figura 4.1 - Compliance

Fonte: Rawpixel / 123RF.

Compliance tem como objetivo dar garantia de que processos e pessoas em organizações cumpram normas reguladoras, regulamentos e leis interna e externamente, por meio de boas práticas.

Quando uma empresa é gerida por meio de *compliance*, multas, paralisações, ações judiciais e sanções podem ser evitadas. No que refere-se a empresas de TI, é importante dar atenção a alguns pontos, como a utilização de novas tecnologias, segurança de dados, políticas de acesso e utilização de tecnologias e ferramentas que ajudem a evitar fraudes. Trata-se do cumprimento de normas, tais como leis, decretos, regulamentos e instruções normativas.

O *compliance* tem similaridade com a segurança da informação no que se refere à proteção de seus ativos. Porém, a razão que existe em *compliance* se difere por ser centrada em requisitos de terceiros, em termos existentes em contratos de cliente, estrutura, entre outros. Ou seja, o *compliance* em TI atende a requisitos de terceiros em relação à segurança digital, viabilizando operações comerciais em mercados ou com clientes específicos.

Compliance potencializa a necessidade de existir um programa de segurança da informação eficiente, pois faz com que a empresa trabalhe com práticas que protegem seus ativos mais importantes. Assim, são realizados treinamentos de conscientização para colaboradores, sistemas

de segurança em camadas e testes feitos por terceiros que garantem que os controles sejam efetivos.

Utilizar *compliance* é uma vantagem, pois, quando a empresa passa a trabalhar em conformidade com a norma ISO: 27001, esta reforça sua imagem e pode gerar mais negócios com clientes preocupados com segurança. Outra vantagem é que permite o funcionamento correto da TI, aumentando a segurança acerca de ataques cibernéticos.

Diante de tudo o que foi exposto neste tópico, pode-se observar que utilizar *compliance* em organizações traz inúmeros benefícios não somente para a empresa como para funcionários, fornecedores e clientes.

Vamos Praticar

Compliance significa estar em conformidade com as obrigações legais, situação em que a organização tem responsabilidades em relação a proteção à saúde, bem-estar e segurança para com os colaboradores.

Assinale a alternativa que diz respeito ao objetivo do *compliance*.

- a)** Garantir que processos e pessoas em organizações cumpram normas reguladoras, regulamentos e leis internamente por meio de boas práticas.
- b)** Garantir que processos e pessoas em organizações cumpram normas reguladoras, regulamentos e leis externamente por meio de boas práticas.
- c)** Garantir que as pessoas em organizações cumpram normas reguladoras, regulamentos e leis externamente por meio de boas práticas.
- d)** Garantir que processos e pessoas em organizações cumpram normas reguladoras, regulamentos e leis interna e externamente por meio de boas práticas.
- e)** Garantir que processos em organizações cumpram normas reguladoras, regulamentos e leis interna e externamente por meio de boas práticas.

Melhores Práticas de Compliance em TI

Não são poucas as práticas de compliance em TI. Entre elas, podem-se citar *cloud computing*, utilização de *software as a service*, cuidados com BYOD (*bring your own device*), ferramentas para monitorar a TI e programas voltados para governança corporativa.

Em TI, o *compliance* viabiliza a realização de tarefas estratégicas que fornecem suporte para outras atividades e outros departamentos, facilitando o trabalho a ser executado, reduzindo custos e retrabalho e garantindo que a organização tenha maior sucesso nas atividades que realiza, bem como gera aumento de produtividade. A seguir, serão explicadas as melhores práticas em *compliance*.

Cloud Computing



Figura 4.2 - Cloud computing

Fonte: Daniil Peshkov / 123RF.

A utilização de *cloud computing* (computação em nuvem) faz com que o trabalho em equipe seja reduzido, assim como ocorre com os custos para cada atividade realizada. Como as regras tendem a mudar com uma certa frequência, essa técnica facilita a implantação de *compliance*, pois garante a aceitação da empresa às normas e fazem com que os riscos e custos sejam menores.

SAAS (*Software as a service*)



Figura 4.3 - SAAS (*Software as a service*)

Fonte: Tatyana Merkusheva / 123RF.

Trata-se de ferramentas que geram um repositório de dados que podem ser vistos e acessados sempre que necessário e desejado, a partir de qualquer dispositivo (computador, *tablet*, *smartphone* e *notebook*) para que sejam realizadas consultas sobre requisitos referentes a regulamentações, monitoramento de sistemas, política de segurança das organizações e índices que mostram o cumprimento das medidas, desde que estes possuam acesso via internet.

BYOD (*Bring your own device*)

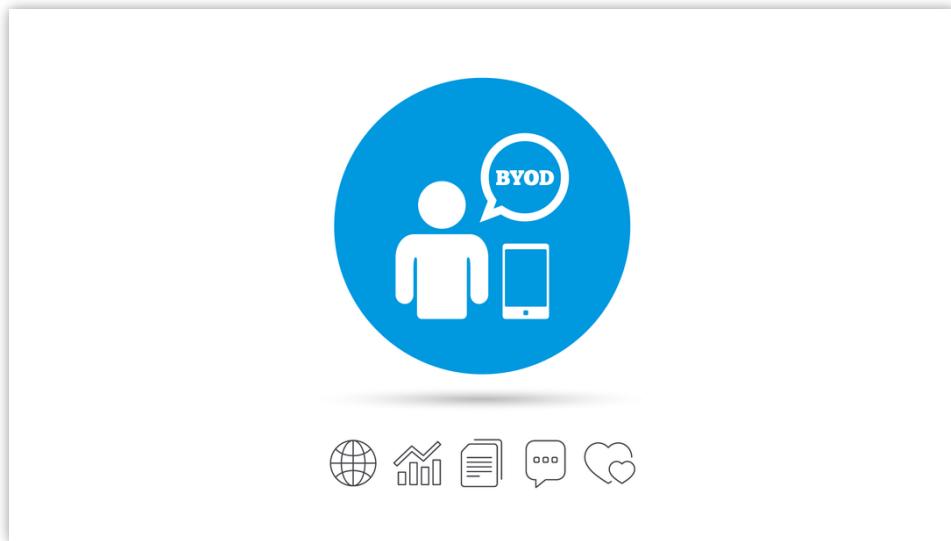


Figura 4.4 - BYOD (*Bring your own device*)

Fonte: blankstock / 123RF.

Trata-se da utilização de dispositivos próprios dos funcionários, como, por exemplo, a utilização de *notebooks* ou *smartphones* próprios. As empresas estão aderindo a essa prática, porém, ainda com ressalvas, pois funcionários podem utilizar de maneira errada e, dessa forma, ocasionar problemas para sistemas e redes das organizações.

Para que esses tipos de problemas não ocorram ou, ainda, que os riscos sejam minimizados em relação a ataques ou ações maliciosas, as organizações estão adotando termos de responsabilidade,

senhas que possuam bloqueio automático e instalações de antivírus nos dispositivos.

Ferramentas para Monitoramento

Por meio da utilização de ferramentas de monitoramento, a infraestrutura pode ser controlada e é possível extinguir a falta de eficiência operacional, bem como facilitar para que sejam encontradas falhas e se aumente a produtividade.



Figura 4.5 - Ferramentas de monitoramento TI

Fonte: alexandersikov / 123RF

Dessa forma, é possível dar atenção às tarefas estratégicas e verificar realmente o que tem maior importância para o negócio.

Programas para Governança Corporativa



Figura 4.6 - Governança corporativa

Fonte: emevil / 123RF.

O *compliance* é um dos principais itens para que a governança corporativa seja alcançada da forma mais eficiente, pois assegura que as atividades ou tarefas realizadas tenham menos interrupções, deixem os usuários mais satisfeitos e resolvem-se os problemas mais rapidamente, trazendo, inclusive, transparência para relação com fornecedores.

praticar

Vamos Praticar

SAAS são ferramentas que geram um repositório de dados que podem ser vistos e acessados sempre que necessário e desejado, a partir de qualquer dispositivo (computador, *tablet*, *smartphone* e *notebook*) para que sejam realizadas consultas sobre requisitos referentes a regulamentações, monitoramento de sistemas, política de segurança das organizações e índices que mostram o cumprimento das medidas, desde que estes possuam acesso via internet.

Assinale a alternativa que diz respeito às vantagens em sua utilização.

- a)** Redução de custos, despreocupar-se com infraestrutura, investimento na atividade-fim, acesso remoto e facilidade em realizar melhorias.
- b)** Redução de custos, atentar-se para infraestrutura, investir na atividade-fim, acesso remoto e facilidade em realizar melhorias.
- c)** Aumento de custos para infraestrutura, investimento maior na atividade-fim, acesso remoto e facilidade em realizar melhorias.
- d)** Custos variáveis, despreocupar-se com infraestrutura, investimento na atividade-fim, acesso remoto e facilidade em realizar melhorias.
- e)** Redução de custos, despreocupar-se com infraestrutura, investimento na atividade-fim, acesso remoto e menor possibilidade de customização.

Auditoria Interna x Compliance

De acordo com a PricewaterhouseCoopers Brasil (FÓRUM ABBC, 2011), a auditoria interna e o *compliance* se complementam, pois *compliance* define e estabelece regras, treinamentos, procedimentos, conscientiza os colaboradores, bem como os fornecedores a respeito das normas. A auditoria interna, por sua vez, identifica oportunidades de aperfeiçoar, fazer com que os controles sejam mais eficazes, verificar e apontar desde indícios até a existência propriamente dita de irregularidades nas empresas.

Para que o programa de *compliance* seja eficaz e implantado corretamente, ele deve conter elementos essenciais, tais como política e procedimentos formalizados; padrões de conduta; a designação de um comitê ou um responsável; uma comunicação efetiva e preventiva; treinamento para que o conhecimento seja disseminado de forma efetiva; um canal de comunicação que os colaboradores possam utilizar sem preocupar-se em se identificar; monitoramento de não conformidades; e ações disciplinares que façam a correção de possíveis inconformidades.

São exemplos de empresas que trabalham com gestão por *compliance* : Nestlé, Coca-Cola, Renault do Brasil, 3M, entre outras. A 3M, por exemplo, multinacional americana, tem envolvimento com *compliance* desde 1988 e foi uma empresa que se autodenunciou, em 2009, por suspeita de violação à Lei Anticorrupção dos Estados Unidos da América. O processo, nesse caso, não seguiu adiante, pois os reguladores entenderam que, diante da colaboração e denúncia da própria empresa, não se fazia necessário e não seria a melhor maneira de conquistar novos negócios. Ainda nos dias de hoje, a 3M mantém o canal de denúncias aberto para que qualquer pessoa possa fazer denúncias, tanto internamente quanto externamente.

Já a auditoria interna ajuda a organização atingir os objetivos estratégicos a partir de abordagens metodológicas, com muita disciplina para realizar a avaliação, bem como melhorias nos processos de gestão de riscos, governança corporativa e controles internos.

Dessa forma, a auditoria interna ajuda a empresa a concluir seus objetivos por meio da disciplina e busca constantes melhorias em processos referentes à gerência de riscos, *compliance* , governança e melhor controle.

Vamos Praticar

Compliance define e estabelece regras, treinamentos, procedimentos, a conscientização dos colaboradores, bem como os fornecedores a respeito das normas. Para que o programa seja eficaz, ele deve conter:

Analise as afirmativas a seguir e assinale V para a(s) verdadeira(s) e F para a(s) falsa(s).

() Política e procedimentos formalizados, padrões de conduta, designação de um comitê ou um responsável, comunicação efetiva e preventiva, treinamento, canal de comunicação que os colaboradores possam utilizar de forma anônima, monitoramento de não conformidades, ações disciplinares.

() Política e procedimentos informais, padrões de conduta, designação de um responsável, comunicação efetiva e preventiva, treinamento, canal de comunicação que os colaboradores possam utilizar de forma anônima, monitoramento de não conformidades, ações disciplinares.

() Política e procedimentos formalizados, padrões de conduta, designação de um comitê, comunicação paliativa e utópica, treinamento, canal de comunicação que os colaboradores possam utilizar de forma anônima, monitoramento de não conformidades, ações disciplinares.

A seguir, assinale a alternativa correta.

- a)** F, V, F.
- b)** F, V, V.
- c)** V, F, F.
- d)** V, V, F.
- e)** V, F, V.



Perícia Forense Digital



A perícia forense digital dá apoio a clientes e assessores jurídicos em relação a sistemas de informação e recursos computacionais, no que diz respeito a ações que precisam de provas para acompanhamento em ações. Esses serviços podem ser solicitados também por diferentes esferas do Poder Judiciário.

Geralmente, para realizar investigação em ocorrências em ambientes de tecnologia da informação (TI), é importante que as evidências sejam apresentadas e isso se dá por meio de procedimento aprimorado, a fim de evitar que informações de grande importância sejam perdidas, podendo-se, assim, reconstruir as cenas dos eventos ocorridos.

Entre as tarefas da perícia forense digital, estão a procura e preservação das provas para que deem suporte aos processos, a verificação de roubo ou furto de informações, a análise de invasões a sistemas computacionais, a verificação de propriedades intelectuais que tenham sido violadas, a verificação se o controle de normas e políticas de segurança estão sendo cumpridas e o estabelecimento de ocorrências na ordem em que ocorreram em computadores e dispositivos.

Saiba mais

A Lei Anticorrupção Empresarial fala sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos realizados contra a administração pública, nacional ou estrangeira.

Fonte: Ribeiro e Diniz (2015, p. 87).

[ACESSAR](#)

Pode-se citar como exemplo de atuação da perícia forense computacional a investigação de crimes de pedofilia, na qual são apreendidos os dispositivos do acusado, tais como computadores, notebooks e celulares, pois, por meio deles, realiza-se a investigação de vestígios ou evidências

digitais que qualifiquem o crime. Outro exemplo é o de crimes financeiros. Um usuário, ao tentar realizar um pagamento por meio digital, pode ser redirecionado a uma página idêntica à de seu banco, porém, trata-se de uma página falsa, que será utilizada para realizar furto de dados e estes serão usados para que seja furtado dinheiro da conta do usuário sem que ele saiba. Dessa forma, pode ocorrer a investigação a partir do dispositivo utilizado pelo usuário ou, ainda, a busca pelo endereço de onde surgiu a página.

A perícia forense computacional é realizada em quatro etapas na prática, são elas: coleta, exame, análise e resultados. Abaixo, serão apresentadas cada uma delas.

1. Coleta

Nesta etapa, deve-se ter muito cuidado em relação à integridade do material que será coletado, pois as informações não podem sofrer alterações durante o processo investigatório.

2. Exame

Nesta etapa, deve ser executada uma série de procedimentos para que sejam recuperados e catalogados os dados existentes em dispositivos. Esses procedimentos devem ser embasados científicamente. É importante realizá-los em cópias para que o material original seja mantido intacto.

3. Análise

Nesta etapa, peritos examinarão informações e serão realizadas buscas por evidências referentes ao crime. É importante que se tenha uma definição clara e detalhada sobre o que é preciso investigar e seguramente pode ser uma das mais demoradas etapas da perícia. Assim, ao final do processo, será possível formular a conclusão sobre o crime que originou a investigação.

4. Resultado

Após a análise criteriosa de todas as informações, nesta etapa é apresentado o laudo pericial que contém as evidências que foram encontradas e que servirão de provas que deverão ser apresentadas no processo.

Muitas vezes, não nos damos conta de que as informações que estamos coletando e armazenando por meio de ferramentas de dispositivos, como, por exemplo, filmagens, batimentos cardíacos, qualidade de sono, entre outras, podem ser roubadas em crimes cibernéticos e é mediante a computação forense que se pode analisar e investigar esses tipos de crimes.

reflita

Reflita

De acordo com Bowen et al. (2007), a gestão de recursos de tecnologia de informação facilita para que ocorra sucesso da organização. Esse sucesso acontece porque a governança de TI, realizada de forma eficiente, gera benefícios como credibilidade, prestação de serviços de qualidade, diminuição de custos, entre outros.

Fonte: Bowen et al. (2007, p. 191-221).

A partir da perícia forense digital, é possível descobrir transgressões, tais como roubos de identidade e alguns crimes financeiros, fazendo o uso de técnicas para realizar essa busca. As ameaças são reais e cada vez mais frequentes. Por isso, é muito importante que as pessoas e as organizações estejam atentas às suas informações e, no caso das empresas, é de extrema importância que sejam desenvolvidas políticas de segurança e treinamentos para funcionários a fim de evitar que ocorram transtornos.

praticar

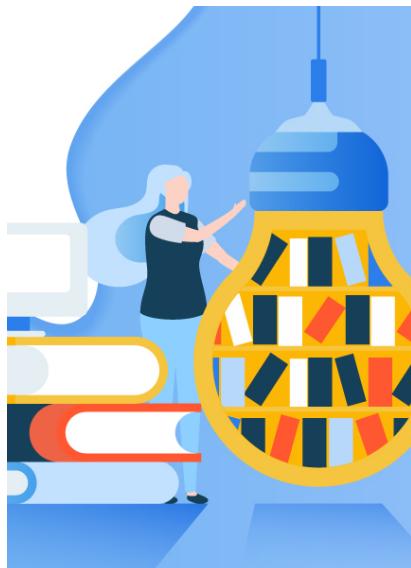
Vamos Praticar

A perícia forense digital dá apoio a clientes e assessores jurídicos em relação a sistemas de informação e recursos computacionais no que diz respeito a ações que precisam de provas para acompanhamento em ações.

Assinale a alternativa que corresponde às tarefas realizadas pela perícia forense digital.

- a)** Procurar e preservar as provas para que deem suporte aos processos, analisar invasões a sistemas computacionais, automatizar o controle de normas e políticas de segurança.
- b)** Procurar e preservar as provas para que deem suporte aos processos, analisar invasões a sistemas computacionais, estabelecer ocorrências na ordem aleatória em que ocorreram em computadores.
- c)** Procurar e preservar as provas para que deem suporte aos processos, analisar invasões a sistemas computacionais, criar controle de normas e políticas de segurança.
- d)** Verificar roubo ou furto de informações, analisar invasões a sistemas computacionais, criar controle de normas e políticas de segurança.
- e)** Verificar roubo ou furto de informações, bem como propriedades intelectuais que tenham sido violadas, analisar invasões a sistemas computacionais.

indicações Material Complementar



LIVRO

Surviving as a "Software as a Service" (SaaS) Startup

Editora : GRIN Publishing; Edição: 1. (28 de janeiro de 2015)

Autor : Nick Birch

ISBN : 3656882290

Comentário : Software como Serviço (SaaS) não é apenas uma tendência, mas uma forma comprovada para que os proprietários de pequenas empresas economizem tempo e dinheiro. Pequenas empresas e startups podem ter e-mail, armazenamento de arquivos, despesas, compras, recursos humanos, colaboração e gerenciamento de tarefas a um custo menor para TI e software . Com acesso a serviços e softwares que antes só estavam disponíveis para grandes empresas por causa do alto custo de infraestruturas e manutenção, os serviços de software permitem que uma empresa reduza custos e se concentre em seus produtos e serviços, em vez de configurar software ou delegar entre departamentos. Leia o livro indicado e aprenda um pouco mais sobre a utilização do SaaS.

conclusão

Conclusão

Conforme apresentado nesta unidade, o termo *compliance* vem sendo cada vez mais utilizado em empresas. No que diz respeito a empresas de TI, trata sobre a utilização de tecnologias novas, segurança de dados, políticas de acesso e utilização de tecnologias e ferramentas que ajudem a evitar fraudes. Governar a partir de *compliance* significa estar em conformidade com as obrigações legais, situação em que a organização tem responsabilidades em relação a proteção à saúde, bem-estar e segurança para com os colaboradores, principalmente no que se refere a contratações, demissões, assédio, segurança, benefícios, folha de pagamento, salários e discriminação. Essa conformidade estende-se a normas, regulamentos e leis que norteiam as atividades das organizações, para que se evitem problemas como a corrupção e a falta de ética.

Foram abordadas as melhores práticas em *compliance*, cujo objetivo é viabilizar a realização de tarefas estratégicas que forneçam suporte para outras atividades e outros departamentos, facilitando o trabalho a ser executado, reduzindo custos e retrabalho e garantindo que a organização tenha maior sucesso nas atividades que realiza, bem como gere aumento de produtividade.

A PricewaterhouseCoopers Brasil (FÓRUM ABBC, 2011) nos mostra que a auditoria interna e o *compliance* se complementam, pois *compliance* define e estabelece regras, treinamentos, procedimentos, conscientiza os colaboradores, bem como os fornecedores a respeito das normas; e a auditoria interna, por sua vez, identifica oportunidades de aperfeiçoar, faz com que os controles sejam mais eficazes, verifica e aponta desde indícios até a existência propriamente dita de irregularidades nas empresas.

Por fim, foi abordado o tema de perícia forense digital, que pôde mostrar que, a partir desta, é possível descobrir transgressões como roubos de identidade e alguns crimes financeiros, fazendo o uso de técnicas para realizar essa busca.

referências

Referências Bibliográficas

BOWEN, P. L.; CHEUNG, M. Y. D.; ROHDE, F. H. Enhancing IT governance practices: A model and case study of an organization's efforts. **International Journal of Accounting Information Systems**, 8(3), 191–221. doi, 2007. Disponível em: <http://dx.doi.org/10.1016/j.accinf.2007.07.002>. Acesso em: 03 jan. 2020.

CONHEÇA PRÁTICAS DE **COMPLIANCE** ADOTADAS POR EMPRESAS DO SELO PRÓ-ÉTICA. Disponível em: <https://blueprintt.co/blog/praticas-de-compliance/>. Acesso em: 14 jan. 2020.

CREESE, G. **SaaS vs. Software** : The Release Cycle for SaaS Is Usually (Not Always) Faster. Disponível em: <http://blogs.gartner.com/guycreese/2010/05/18/saas-vs-software-the-development-cycle-for-saas-is-usuallynot-always-faster/>. Acesso em: 25 dez. 2019.

FÓRUM ABBC, 2011. **Como a atuação integrada do compliance e da auditoria interna pode se tornar estratégica na governança corporativa** . Disponível em: http://www.abbc.org.br/arquivos/compliance_auditoria_e_governanca_corporativa.pdf . Acesso em: 28 dez. 2019.

GIL, P. What Is 'SaaS' (Software as a Service)? **Lifewire** . Disponível em: <https://www.lifewire.com/what-is-saas-software-2483600> . Acesso em: 24 dez. 2019.

KHURANA, S.; VERMA, A. **Comparison of Cloud Computing Service Models** : SaaS, PaaS, IaaS. Disponível em: https://pdfs.semanticscholar.org/fabe/9beaff63b625b47c269e861981b5654e7c18.pdf?_ga=2.240668619.914894973.1578153396-1085619846.1578 . Acesso em: 02 dez. 2020.

RIBEIRO, M. K. P.; DINIZ, P. D. F. Compliance e Lei Anticorrupção nas empresas. **Revista de Informação Legislativa** . Ano 52, n. 205 jan./mar. 2015. Disponível em: https://www12.senado.leg.br/ril/edicoes/52/205/ril_v52_n205_p87.pdf . Acesso em: 17 fev. 2020.

VERDE GHAIA. **Compliance na prática** : exemplos brasileiros para você se inspirar. Disponível em: <https://www.verdeghaia.com.br/blog/principais-nomes-do-compliance-no-brasil/> . Acesso em: 14 jan. 2020.