1

Conceitos de Integridade e Sigilo

Segurança da Informação

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

Violações de dados ressurgentes que podem estar associadas a uma falha em aderir aos princípios básicos da segurança da informação têm sido uma constante no mercado. Em um mundo em que as ameaças à segurança estão evoluindo continuamente, isso serve como um lembrete útil de que é preciso dominar o básico antes de investir em medidas mais ambiciosas.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

Senhas fracas e recicladas, atrasos na correção, ativos configurados incorretamente ou um inventário de ativos incompleto são todos exemplos de lapsos simples que podem levar à infiltração por hackers. Todas essas medidas fazem parte dos pilares básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

Esses três pilares são princípios básicos, mas fundamentais, para manter uma segurança robusta em um determinado ambiente. Entender cada um deles e saber como funcionam em conjunto é útil para criar resultados positivos para a segurança.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Confidencialidade: Os meus sistemas estão protegidos do acesso não autorizado?**

A confidencialidade envolve os esforços de uma organização para garantir que os dados sejam mantidos em segredo ou privados. Para conseguir isso, o acesso às informações deve ser controlado para evitar o compartilhamento não autorizado de dados — seja intencional ou acidental.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Confidencialidade: Os meus sistemas estão protegidos do acesso não autorizado?**

Um componente-chave para manter a confidencialidade é garantir que pessoas sem a devida autorização sejam impedidas de acessar ativos importantes para o seu negócio. Por outro lado, um sistema eficaz também garante que aqueles que precisam ter acesso tenham os privilégios necessários.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Confidencialidade: Os meus sistemas estão protegidos do acesso não autorizado?**

Existem várias maneiras pelas quais a confidencialidade pode ser comprometida. Isso pode envolver ataques diretos com o objetivo de obter acesso a sistemas que o invasor não tem direito de ver. Também pode envolver um invasor que faça uma tentativa direta de se infiltrar em um aplicativo ou banco de dados para obter dados ou alterá-los.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Confidencialidade: Os meus sistemas estão protegidos do acesso não autorizado?**

Esses ataques diretos podem usar técnicas como ataques man-in-the-middle (MITM), em que um invasor se posiciona no fluxo de informações para interceptar dados e, em seguida, roubá-los ou alterá-los. Alguns invasores se envolvem em outros tipos de espionagem de rede para obter acesso às credenciais. Em alguns casos, o invasor tentará obter mais privilégios de sistema para obter o próximo nível de liberação.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Confidencialidade: Os meus sistemas estão protegidos do acesso não autorizado?**

No entanto, nem todas as violações de confidencialidade são intencionais. Erro humano ou controles de segurança insuficientes também podem ser os culpados. Por exemplo, alguém pode deixar de proteger sua senha — seja para uma estação de trabalho ou para fazer login em uma área restrita. Os usuários podem compartilhar suas credenciais com outra pessoa ou permitir que alguém veja seu login ao inseri-lo.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Confidencialidade: Os meus sistemas estão protegidos do acesso não autorizado?**

Para lutar contra violações de confidencialidade, você pode classificar e rotular dados restritos, habilitar políticas de controle de acesso, criptografar dados e usar sistemas de autenticação multifator (MFA). Também é aconselhável garantir que todos na organização tenham o treinamento e o conhecimento de que precisam para reconhecer os perigos e evitá-los.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Integridade: meus dados são corrompidos, adulterados ou afetados por agentes externos de ameaças?**

A integridade garante que os dados sejam corretos, autênticos e confiáveis. Em outras palavras, ela garante que os dados não foram adulterados e, portanto, podem ser confiáveis. Os dados devem ser protegidos enquanto estão em uso, em trânsito e quando são armazenados, independentemente de residirem em um laptop, dispositivo de armazenamento, data center ou na nuvem.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Integridade: meus dados são corrompidos, adulterados ou afetados por agentes externos de ameaças?**

Você deve garantir que seus dados estejam protegidos contra exclusão e modificação por parte não autorizada, de tal forma que, mesmo quando um indivíduo autorizado fizer alterações por engano, essas alterações possam ser revertidas.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Integridade: meus dados são corrompidos, adulterados ou afetados por agentes externos de ameaças?**

A falta de integridade em um ambiente pode levar ao uso indevido de credenciais, o que significa que os invasores podem manipular dados para atingir vários objetivos sem fazer algo tão barulhento e perceptível como criptografar ou exfiltrar os dados.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Integridade: meus dados são corrompidos, adulterados ou afetados por agentes externos de ameaças?**

Os exemplos comuns incluem a manipulação de registros financeiros para remover rastros de transações e a manipulação de saldos de contas ou a alteração de projetos para sabotar intencionalmente um produto que a organização produz.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Integridade: meus dados são corrompidos, adulterados ou afetados por agentes externos de ameaças?**

A integridade dos dados pode ser preservada por meio de criptografia, hashing, assinatura digital, certificado digital, sistemas de detecção de intrusão, auditoria, controle de versão, autenticação e controles de acesso.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Disponibilidade: meus sistemas e dados estão prontamente acessíveis para uso diário e operações aprovadas?**

Mesmo que os dados sejam mantidos em sigilo e sua integridade seja mantida, eles geralmente são inúteis, a menos que estejam disponíveis para os membros da organização e os clientes que atendem. Isso significa que sistemas, redes e aplicativos devem estar funcionando como deveriam e quando deveriam.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Disponibilidade: meus sistemas e dados estão prontamente acessíveis para uso diário e operações aprovadas?**

A disponibilidade garante que sistemas, aplicativos e dados estejam disponíveis e acessíveis para usuários autorizados quando eles precisarem. Redes, sistemas e aplicativos devem estar constantemente ativos e funcionando para garantir que processos críticos de negócios não sejam interrompidos.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Disponibilidade: meus sistemas e dados estão prontamente acessíveis para uso diário e operações aprovadas?**

A disponibilidade de seus sistemas de dados pode ser afetada por erro humano, falha de hardware, falha de software, falha de rede, falta de energia, desastres naturais e ataques cibernéticos.

Segurança da Informação

Conceitos de Integridade e Sigilo

Confidencialidade, integridade e Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação

- **Disponibilidade: meus sistemas e dados estão prontamente acessíveis para uso diário e operações aprovadas?**

Alguns dos métodos usados para garantir a disponibilidade de dados e aplicativos incluem redundância (servidores, redes, aplicativos e serviços), tolerância a falhas (hardware), patching de software regular e atualizações de sistema, manutenção de backups e cópias de backup e recuperação de desastres.

Segurança da Informação

Conceitos de Integridade e Sigilo

Compreendendo os pilares da segurança

É importante entender o que são cada um dos pilares e como eles são usados para planejar e também implementar uma política de segurança de qualidade, ao mesmo tempo em que compreende os vários princípios por trás deles. Também é importante entender as limitações que eles apresentam.

Uma estratégia abrangente incorpora a consciência de segurança em toda a estrutura de sua organização, minimiza a superfície de ataque de sua rede e prepara seu pessoal e infraestrutura para requisitos regulamentares futuros.

Segurança da Informação

Conceitos de Integridade e Sigilo

Qual é a relação entre a propriedade intelectual da empresa e os dados sigilosos?

A propriedade intelectual de uma empresa é o conjunto de conhecimentos, práticas, processos, técnicas, procedimentos, tecnologias e informações (entre outras coisas) que lhe conferem diferencial competitivo no mercado. Dessa forma, trata-se de dados que, de alguma forma, têm valor econômico por sua confidencialidade, o que leva à necessidade de proteção constante.

Segurança da Informação

Conceitos de Integridade e Sigilo

Qual é a relação entre a propriedade intelectual da empresa e os dados sigilosos?

Não é difícil compreender a importância de atribuir proteção e sigilo aos dados de uma empresa. Pense no Google: por que ele não divulga com detalhes como os sites são organizados em seu buscador? Porque é isso o que dá à empresa o seu diferencial de mercado, que gera receita. O que torna a Coca-Cola um produto único no mercado? A sua fórmula exclusiva.

Segurança da Informação

Conceitos de Integridade e Sigilo

Qual é a relação entre a propriedade intelectual da empresa e os dados sigilosos?

São esses itens que garantem maior competitividade a um negócio e mesmo a sua liderança em um determinado segmento mercadológico. Portanto, merecem toda atenção quando se trata de manter sigilo absoluto sobre as informações envolvidas. Caso dados como esses não sejam protegidos, uma empresa pode facilmente perder o seu diferencial no mercado e, consequentemente, deixar de faturar.

Se o objetivo de uma companhia — seja qual for a sua natureza comercial — é se manter cada vez mais competitiva, de modo a alcançar solidez em um ramo de negócio, ela deve investir em estratégias de segurança da informação.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

Elabore uma Política de Segurança da Informação (PSI)

Vale lembrar que toda melhor prática começa com a gestão da organização. Nessa perspectiva, é essencial que seja criada uma Política de Segurança da Informação (PSI). Esse documento deve conter todas as diretrizes a serem seguidas pela totalidade de profissionais envolvidos com as atividades da empresa, o que inclui funcionários, fornecedores, sócios e acionistas.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Elabore uma Política de Segurança da Informação (PSI)**

Vale lembrar que toda melhor prática começa com a gestão da organização. Nessa perspectiva, é essencial que seja criada uma **Política de Segurança da Informação (PSI)**. Esse documento deve conter todas as diretrizes a serem seguidas pela totalidade de profissionais envolvidos com as atividades da empresa, o que inclui funcionários, fornecedores, sócios e acionistas.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Elabore uma Política de Segurança da Informação (PSI)**

A PSI é essencial, uma vez que abrange os procedimentos que os profissionais precisam adotar no cotidiano da empresa. Ela contempla as tecnologias que devem ser utilizadas, os processos a serem conduzidos, as sanções aplicadas a quem desobedecer às diretrizes, assim como quais dados são sigilosos e devem ser mantidos sob total segurança.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Elabore uma Política de Segurança da Informação (PSI)**

A política funciona como uma esfera reguladora da manipulação dos dados empresariais. Dessa maneira, algumas ações são necessárias. Identifique as melhores práticas a serem tomadas em cada setor, quem são as pessoas responsáveis e os níveis de acesso de cada usuário de sistemas dentro da empresa. Também atente a outras informações que julgue necessárias para orientar o seu time a agir corretamente no tratamento das informações, para dar a elas a proteção adequada.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Elabore uma Política de Segurança da Informação (PSI)**

A elaboração de uma PSI, com o seu devido cumprimento, funciona como um pré-requisito para que ocorra a proteção dos dados de uma empresa. Isso porque de nada adianta a implementação de ferramentas tecnológicas, como as que mostraremos a seguir, se não houver o cultivo cotidiano de uma cultura empresarial em prol da segurança da informação.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Elabore uma Política de Segurança da Informação (PSI)**

Uma PSI, na qual estejam estabelecidas as diretrizes de proteção de dados, em conjunto ao uso de instrumentos tecnológicos adequados, ajuda a garantir a efetivação de práticas eficientes de segurança da informação. Levando em conta a importância da conjugação desses dois elementos, na seção seguinte, indicaremos algumas tecnologias cuja implementação é fundamental para cuidar dos segredos informacionais de uma empresa.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Implemente as tecnologias necessárias**

Com o atual desenvolvimento tecnológico, não existe empresa que trabalhe 100% manual na hora de manipular dados. Tanto aquelas que foram criadas recentemente quanto as mais conservadoras utilizam algum tipo de tecnologia para coletar, armazenar, processar e analisar informações.

Para manter o sigilo desses dados, você precisa de tecnologias auxiliares que promovam a cibersegurança. Existem diversos recursos tecnológicos que atuam, em conjunto ou de modo isolado, na proteção dos dados de uma empresa:

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Implemente as tecnologias necessárias**
- conexões seguras;
- criptografia de dados;
- assinatura eletrônica;
- armazenamento em nuvem;
- antivírus;
- antispywares.

Cada empresa deve analisar o nível de segurança necessário e aplicar as tecnologias mais adequadas ao seu perfil e condições. Estas que listamos acima são bastante acessíveis e conferem uma excelente proteção aos dados do seu negócio.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Proteja suas redes de Wi-Fi**

Quando falamos em conexão, é bom lembrar que operar com uma rede sem fio de internet é muito importante para o ganho de eficiência nos mais diversos tipos de atividades desenvolvidas no interior de uma empresa. E não poderia ser diferente. Isso ocorre em razão da facilidade, rapidez e comodidade de acesso, navegação e troca de informação próprios dos dispositivos de conexão Wi-Fi.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Proteja suas redes de Wi-Fi**

No entanto, se não for manipulada de modo adequado, uma rede sem fios pode trazer riscos para a segurança dos negócios. Sem a devida proteção, usuários não autorizados facilmente obtêm acesso à rede Wi-Fi, podendo invadir o banco de dados da empresa, roubar as informações e até mesmo praticar ações que danificam, destroem ou copiem periodicamente as informações registradas.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Proteja suas redes de Wi-Fi**

Por isso, é fundamental que sejam implementados mecanismos que protejam a rede sem fio de um negócio. Uma solução viável, tendo em vista a sua simplicidade e agilidade, é a criação de senha de acesso, a qual deve ser forte, isto é, ser composta por letras, números e caracteres especiais, que, em conjunto, dificultam a descoberta da chave por usuários indesejados.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Proteja suas redes de Wi-Fi**

Outra ação eficiente é efetuar o cadastro dos equipamentos autorizados a acessarem a rede Wi-Fi da corporação, o que bloqueia o acesso de pessoas não autorizadas. Essa medida é ainda vantajosa porque ajuda a ter um maior controle no que se refere a quem exatamente acessa o banco de dados da empresa ou mesmo faz alguma alteração nele.

Ambas as alternativas permitem a navegação de usuários temporários, como colaboradores eventuais, clientes e fornecedores. Isso pode ser feito por meio da criação de logins para visitantes e do registro de equipamentos por tempo determinado, com a predeterminação do período de acesso do dispositivo.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Faça backups**

Bastante comum no universo tecnológico, backup é uma expressão em língua inglesa que significa cópia de segurança. Trata-se de um conjunto de procedimentos relativos a outra vertente crucial da segurança da informação: proteção contra a perda de dados, ação que é tão necessária quanto protegê-los do acesso feito por usuários não autorizados.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Faça backups**

Com a realização de backups periódicos, a empresa garante que dispõe de todas as informações de que pode precisar, evitando as consequências trazidas por imprevistos. E isso é fundamental, uma vez que, embora os recursos tecnológicos sejam cada vez mais sofisticados e desenvolvidos, ainda é comum haver perdas de dados, por falha computacional ou erro humano.

Além disso, o backup, principalmente os que são feitos em nuvem, protege as informações de potenciais roubos aos equipamentos em que estão armazenadas. Como não podemos prever o futuro ou apenas contar com a sorte, essa é uma ação essencial para promover a segurança das informações empresariais.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Armazene seus documentos na nuvem**

Como mostramos no tópico anterior, guardar adequadamente as informações relativas a um negócio é muito importante para o seu funcionamento. Por isso, o local de armazenamento desses dados deve ser o mais seguro possível, tanto no que se refere ao acesso de usuários quanto no que diz respeito ao backup feito para manter cópias extras das informações.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Armazene seus documentos na nuvem**

Nessa perspectiva, o armazenamento em nuvem figura como uma excelente solução. Isso porque, ao consistir em uma tecnologia que permite o armazenamento de dados de forma remota, por meio da internet e sem a necessidade de um local físico para a guarda dos arquivos, o sistema em nuvem confere, ao mesmo tempo, praticidade e segurança no processo de arquivamento e acesso informacional.

Esse tipo de serviço de armazenamento permite que a empresa proteja suas informações de modo a compartilhá-las somente com os usuários autorizados. Tal compartilhamento seguro é possível uma vez que uma nuvem privada, modelo comumente usado no mundo comercial, tem sua proteção feita por meio do firewall da empresa, o que confere maior controle dos dados.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Firme um contrato de confidencialidade**

Cada pessoa que se relaciona direta ou indiretamente com dados sigilosos deve assinar um documento destes comprometendo-se a manter a confidencialidade dos dados trocados com a sua organização.

Empresas de tecnologia já têm bastante familiaridade com contratos de confidencialidade, já que desenvolvem inovações que estão na dianteira do mercado. Já pensou se o protótipo do novo iPhone vaza e os concorrentes lançam produtos semelhantes antes da Apple? Seria um desastre comercial.

O contrato de confidencialidade não pode impedir que alguém roube as informações da sua empresa e transmita a terceiros, no entanto, é a garantia de que você poderá ser indenizado por isso. Portanto, trata-se de um documento com validade jurídica, que deve ser assinado e guardado com todo o rigor.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Gerencie os riscos**

A perda de dados sigilosos pode se dar de muitas maneiras: um vírus que rouba a informação de um computador, um hacker que invade o sistema da empresa, uma inundação que coloca a perder seu servidor e um pendrive perdido. Estes são só alguns exemplos de situações que podem ocorrer.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Gerencie os riscos**

Antes que elas aconteçam, o ideal é que você mapeie todos esses riscos, por mais absurdos que possam ser, e crie um plano de ação para reduzir ao máximo as possibilidades de que eles venham a se tornar realidade. Por exemplo: em vez de manter seus funcionários levando informações sigilosas em pendrives, opte pelo armazenamento na nuvem. Essa solução traz mobilidade sem afetar a segurança da informação.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Gerencie os riscos**

Evite também enviar contratos impressos para assinatura, o que abre brechas para fraudes e vazamento de informações. Prefira a assinatura eletrônica e tramite seus documentos completamente pela via digital. Quanto menos pessoas tiverem contato com os dados da empresa, menor a chance de ver seu segredo comercial divulgado por aí.

Segurança da Informação

Conceitos de Integridade e Sigilo

O que levar em consideração para a segurança da informação da empresa?

- **Tenha um plano de contingência**

O plano de contingência é executado quando a companhia sofre com desastres e precisa prosseguir com as atividades operacionais da melhor forma possível. Logo, essa estratégia preventiva precisa considerar um conjunto de situações possíveis e quais as principais reações para assegurar a disponibilidade do sistema e dos dados, a fim de garantir a continuidade do negócio.

É necessário que todos os setores tenham prévio sobre como precisam agir caso uma ocorrência desagradável (invasão, vazamento etc.) surja de forma repentina — para evitar que nenhuma das informações críticas se percam e a companhia fique inativa por muito tempo.

Segurança da Informação

Conceitos de Integridade e Sigilo

Como proteger dados sigilosos?

Existem dois tipos de registros sigilosos: os da própria empresa (planos de negócio, informações de processos, dados de funcionários etc.) e os dos clientes (cadastros, contas bancárias, histórico de transações etc.). Por isso, ambos devem ser devidamente protegidos com eficiência. Veja as dicas a seguir.

Segurança da Informação

Conceitos de Integridade e Sigilo

Como proteger dados sigilosos?

- **Escolha bons aplicativos de segurança**

Nada mais eficiente para a segurança de dados do que contar com a tecnologia. Para isso, escolha ferramentas de qualidade, como um bom software de gestão, antivírus e firewall para evitar a infecção de dados por vírus e outros riscos presentes no ambiente digital.

Esse tipo de investimento vale muito a pena, pois previne prejuízos em arquivos, equipamentos e sistemas. Sem falar que garante a produtividade e a eficiência da equipe, graças à agilidade e a precisão das tarefas, reduzindo a probabilidade de erros.

Segurança da Informação

Conceitos de Integridade e Sigilo

Como proteger dados sigilosos?

- **Estabeleça níveis de acesso à informação**

Essa é uma das melhores atitudes que sua empresa pode tomar em questão de segurança da informação: deixar as informações estratégicas no âmbito estratégico, sem socializar os dados com quem não participa do processo.

Se sua equipe de desenvolvimento está trabalhando em um sistema que vai revolucionar o atendimento bancário, por exemplo, limite o acesso de pessoas não autorizadas ao setor. Mantenha os computadores conectados ao servidor da empresa, mas separados dos demais usuários, para evitar invasões.

Servidores virtuais são ótimos para isso. Crie protocolos de segurança, instale biometria para controle de acesso a computadores e mantenha monitoramento constante em locais onde soluções são desenvolvidas.

Segurança da Informação

Conceitos de Integridade e Sigilo

Como proteger dados sigilosos?

- **Não ignore as atualizações**

Quem está atento aos relatórios de atualização dos programas que utiliza, sempre vai identificar registros relacionados à correção de segurança. Ou seja, existia alguma etapa vulnerável que passou por ajustes para potencializar a proteção do sistema.

Cibercriminosos estão de olho nessas brechas, porque é por meio delas que realizam acesso não autorizado aos programas para roubar dados sigilosos.

Em resumo, as atualizações não modificam somente a interface da aplicação e trazem mais recursos, mas também elevam sua segurança. Embora os updates sejam frequentes, porque os ataques também são, deixe sempre seu sistema na última versão para garantir a proteção mais adequada.

Segurança da Informação

Conceitos de Integridade e Sigilo

Como proteger dados sigilosos?

- **Digitalize os documentos**

É muito mais prático e seguro trabalhar com documentos digitais. Além de preservar papéis da ação do tempo e de acidentes, a empresa que opta por digitalizar seus registros otimiza esse tipo de gestão.

Com um software específico é possível armazenar documentações sem correr o risco de extravio. As funcionalidades presentes na ferramenta facilitam a organização e a atualização de registros sem comprometer a segurança do processo. Além disso, qualquer documento pode ser facilmente encontrado pelo mecanismo de busca.

Referências

- **Docusign**

  https://www.docusign.com/pt-br/blog/seguranca-da-informacao

- **IBM**

  https://www.docusign.com/pt-br/blog/seguranca-da-informacao