

# INTRODUÇÃO À PROTEÇÃO DE DADOS



CYBERSECURITY  
EXPERTS ON YOUR SIDE

## Entendendo o básico de proteção de dados

Proteger a segurança e privacidade das informações sensíveis do cliente é uma obrigação fundamental de toda empresa, incluindo SMEs.

A proteção de dados (e mais amplamente, segurança da informação), abrange todos os controles técnicos, administrativos, lógicos e técnicos necessários para proteger informações. A tríade C-I-A (consulte a Figura 2-1) é geralmente usada para guiar o desenvolvimento e implementação de uma estrutura para gerenciar segurança da informação dentro de uma organização. A tríade C-I-A consiste de três conceitos fundamentais de segurança da informação:

### Confidencialidade e privacidade

Previne o acesso, uso, revelação, leitura, inspeção ou registro não autorizado de dados.

### Integridade

Previne a modificação inadequada ou não autorizada de dados.

### Disponibilidade

Garante que usuários autorizados tenham acesso confiável e pontual aos dados, e previne a interrupção ou destruição de dados não autorizados.



Figura 2-1: A tríade C-I-D.

Para **proteger a confidencialidade de dados** sensíveis, várias políticas de empregabilidade, segurança e privacidade geralmente definem **quem tem acesso a certos dados dentro de uma organização, por quais propósitos e o que são autorizados a fazer com esses dados**. Os controles técnicos para garantir confidencialidade podem incluir criptografia de gestão de acesso e identidade (IAM) e soluções de prevenção de perda de dados.

Para **proteger a integridade de dados**, várias soluções técnicas como **checksums e validação de inserção de dados em formulários e bases de dados podem ser implementados**. Assinaturas digitais e tecnologias de criptografia com uso de *hash* para provar a autenticidade dos dados ou para **verificar que os dados não foram alterados**. Finalmente, soluções anti-malware protegem a integridade dos dados (e potencialmente a confidencialidade e disponibilidade dos dados).

Para **proteger a disponibilidade dos dados** de destruição acidental (por exemplo, exclusão) ou intencional (por exemplo, um ataque de *ransomware*), **sistemas de recuperação e backup, além de políticas de retenção e de backup, são implementados**.

A segurança de informação efetiva requer uma empresa para **abordar a confidencialidade, integridade e disponibilidade de todos seus dados sensíveis**, incluindo os sistemas e aplicações que processam e armazenam aqueles dados.

Usando uma abordagem baseada em risco, as organizações podem implementar controles apropriados para abordar vulnerabilidades e atingir um nível aceitável de risco aos dados contra ameaças específicas. Quanto maior o risco para os dados, maior devem ser as medidas que devem ser implementadas.

A gestão de risco de segurança consiste de quatro fases-chave:



Figura 2-2: Processo básico de gerenciamento de risco.

## Avaliação de riscos

Há muitas metodologias de avaliação de riscos com muitos níveis de custo e complexidade. O processo básico consiste em:

- **Identificação dos ativos**

Identificar todos os ativos da organização (tangíveis e intangíveis) que precisam de proteção, incluindo o valor quantitativo (como custo ou contribuição para a receita) e/ou qualitativo (como importância relativa) do ativo.

- **Análise da ameaça**

Definir circunstâncias ou eventos adversos naturais e/ou de origem humana, o impacto potencial ou consequências e a probabilidade e frequência de ocorrência.

- **Avaliação de vulnerabilidades**

Determinar quais proteções e/ou controles estão ausentes ou fracos em um ativo, tornando, portanto uma ameaça potencialmente mais prejudicial, cara, provável ou frequente.

## Tratamento de riscos

A avaliação de risco fornece a base para decisões de gestão relacionadas ao que fazer sobre riscos específicos. As opções incluem:

- **Atenuação de riscos**

Implementar políticas, controles e/ou outras medidas para reduzir o impacto ou probabilidade de uma ameaça específica contra um ativo específico.

- **Avaliação de risco (ou transferência)**

Transferir o risco potencial para terceiros, como uma seguradora, um provedor de serviços ou outro agente que concorde explicitamente em aceitar o risco.

- **Evasão de risco**

Eliminar o risco completamente, por exemplo, atualizando ou eliminando o ativo ou parando a atividade que introduz o risco.

## Aceitação do risco

Essa é a aprovação de gestão formal das medidas de tratamento de risco que são implementadas, e a aceitação de quaisquer riscos residuais (ou remanescentes) que não possam ser mais ou viavelmente atenuados, atribuídos ou evitados.

## Comunicação de risco

Os stakeholders apropriados precisam estar cientes de quaisquer tratamentos de riscos e/ou decisões de aceitação de riscos que tenham sido feitas, incluindo seus papéis e responsabilidades individuais com relação a riscos específicos.

## Comparando opções de implementação presencial, na Nuvem e híbrida

As empresas hoje têm muitas opções para implementar tecnologia, incluindo implementação presencial, na Nuvem e híbrida, com alguns recursos localizados nas instalações e outros, na Nuvem.

Em um passado não muito distante, a única opção de implantação para empresas era presencial. Mesmo a menor das empresas frequentemente se encontra na necessidade de adquirir vários servidores caros, frequentemente instalados precariamente em um armário lotado e escuro em algum lugar do edifício (talvez com um extintor de incêndio no teto – para que um incêndio não destruía seus caros investimentos em TI). Esses servidores precisavam de manutenção e administração contínua, o que frequentemente significava equipe ou prestadores de TI adicionais. Não apenas servidores, mas também equipamentos de rede como roteadores, switches e cabeamento de rede tinham que ser instalados e gerenciados. No mínimo, um firewall protegia a rede interna “confiável” da “inconfiável” internet.

Gerenciar uma sala de servidores ou datacenter presencialmente ainda é uma opção viável para muitas empresas. Mas como as tecnologias computacionais de virtualização, conectividade de rede e computação em Nuvem tornaram-se mais robustas e estáveis na última década, muitas empresas estão agora movendo alguns ou todos os seus recursos de TI para a Nuvem.

Mas o que é exatamente a Nuvem? Praticamente todo fornecedor de tecnologia no mercado tem uma oferta “na Nuvem” de algum tipo e, infelizmente, a definição de Nuvem pode ser algumas vezes um pouco... bem, nebulosa. Então para limpar o céu a respeito de Nuvem, vamos definir alguns poucos elementos importantes da Nuvem usando as definições neutras do Instituto Nacional de Normas e Tecnologias dos Estados Unidos (NIST). De acordo com o NIST, os três modelos de serviço computacional em Nuvem são como segue:

### **Software como Serviço (SaaS)**

É fornecido acesso aos clientes para uma aplicação executada em uma infraestrutura de Nuvem. A aplicação é acessível a partir de vários dispositivos e interfaces do cliente, mas o cliente não tem conhecimento e não gerencia ou controla a infraestrutura de Nuvem subjacente. O cliente pode ter acesso a configurações de aplicação limitadas específicas para o usuário, e a segurança dos dados do cliente ainda é responsabilidade do cliente.

### **Plataforma como Serviço (PaaS)**

Os clientes podem implementar aplicações suportadas na infraestrutura de Nuvem do provedor, mas o cliente não tem conhecimento e não gerencia ou controla a infraestrutura de Nuvem subjacente. O cliente tem controle sobre as aplicações implementadas e definições de configuração limitadas para o ambiente de hospedagem da aplicação. A empresa possui as aplicações implementadas e dados, e é, portanto, responsável pela segurança dessas aplicações e dados

### **Infraestrutura como Serviço (IaaS)**

Os clientes podem provisionar o processamento, armazenamento, redes e outros recursos computacionais, e implementar e executar sistemas operacionais e aplicações, mas o cliente não tem conhecimento e não gerencia ou controla a infraestrutura de Nuvem subjacente. O cliente tem controle sobre os sistemas operacionais, armazenamento e aplicações implementadas, além de alguns componentes de rede. A empresa possui as aplicações implementadas e dados, e é, portanto, responsável pela segurança dessas aplicações e dados.



TIP

*Os diferentes modelos de serviço na Nuvem (SaaS, PaaS e IaaS) têm diferentes implicações de segurança para os clientes. Por exemplo as ofertas SaaS como o Microsoft 365 e o Salesforce fornecem segurança de infraestrutura através do provedor na Nuvem, mas a segurança e autenticação de dados são responsabilidade do cliente. As responsabilidades de segurança do cliente aumentam progressivamente nas ofertas de PaaS e IaaS. Muitas soluções na Nuvem mudam o foco de segurança da aplicação ou infraestrutura para segurança na autenticação e integridade de dados.*

O NIST também define quatro modelos de implementação computacional na Nuvem:

## **Público**

Uma infraestrutura na Nuvem que está aberta para uso pelo público. É de propriedade, gestão e operação por um terceiro (ou terceiros) e existe nas instalações do provedor de Nuvem.

## **Privado**

Uma infraestrutura na Nuvem usada exclusivamente por uma única organização. Pode ser de propriedade, gestão e operação da organização ou de um terceiro (ou uma combinação desses), e pode existir presencialmente ou não.

## **Híbrido**

Uma infraestrutura na Nuvem composta de dois ou mais dos modelos de implementação, unidos por tecnologia proprietária ou padronizada que habilite a portabilidade da aplicação e dados.

## **Comunitário (incomum)**

Uma infraestrutura na Nuvem usada exclusivamente por um grupo de organizações específico.

A jornada para a Nuvem frequentemente começa como muitas novas iniciativas, com aplicações e sistemas que não estão em produção e não são críticos, como um ambiente de desenvolvimento ou sistemas de backup. Com a continuação da jornada, muitas empresas começam a "subir e mudar" aplicações existentes para a Nuvem e implementar novas aplicações diretamente na Nuvem. Finalmente, as organizações "Nuvem Primeiro" fazem todos os esforços para implementar o máximo possível do seu am-

biente de TI na nuvem e desenvolver aplicativos “Nativos da Nuvem” para seus clientes.

Os muitos benefícios da Nuvem para as empresas incluem:

### **Maior agilidade e responsividade**

Você pode acessar aplicações e dados na Nuvem de qualquer lugar, a qualquer hora, em qualquer dispositivo.

### **Tempo de comercialização mais rápido**

Você pode desenvolver e entregar novos produtos e serviços mais rapidamente na Nuvem com o PaaS ou com recursos IaaS facilmente provisionados.

### **Escalabilidade sob demanda**

Licenciamento e/ou infraestrutura de software adicional pode ser provisionada e reduzida conforme necessário, o que suporta as necessidades de negócios cíclicos e em crescimento rápido que podem não ser capazes de prever com precisão as alterações de mercado e crescimento de negócios.

### **Estabilidade aumentada**

A infraestrutura na Nuvem é geralmente instalada em datacenters robustos construídos para desempenho, estabilidade e confiabilidade, e gerenciados por grandes times de equipes de TI especializadas.

### **Investimentos de capital reduzidos**

Você pode implementar toda sua infraestrutura de TI na Nuvem e esquecer-se dos caros investimentos de capital. A Nuvem oferece serviços previsíveis “pré-pagos” baseados em assinatura que permitem que você controle seu orçamento de TI como uma despesa operacional contínua e apenas pague pelo que usar.



AVISO

*Mover seus aplicativos e dados para a Nuvem não elimina ou transfere sua responsabilidade para a segurança das suas aplicações e dados. Ainda que o provedor de serviços na Nuvem seja responsável por certos aspectos do ambiente, você é sempre o principal responsável por proteger e assegurar suas aplicações e dados. Os fornecedores de serviço em Nuvem normalmente referem-se a um “modelo de responsabilidade compartilhada” que claramente mostra pelo que eles são responsáveis na Nuvem e pelo que você é responsável – e em lugar algum o modelo de responsabilidade compartilhada jamais mostrou o provedor de serviço na Nuvem sendo responsável pela segurança dos seus dados!*



## **Considerando provedores de serviço de segurança gerenciados e terceirização**

Manter aplicações e sistemas de TI seguros, com patches, protegidos e em conformidade em relação aos sempre crescentes riscos e ameaças cada vez mais sofisticadas é uma carga desafiadora para empresas de todos os tamanhos. Isso vale especialmente para SMEs com equipe de TI e recursos de segurança limitados. Muitas SMEs estão se voltando para provedores de serviços gerenciados (MSP) para a solução. Os benefícios e valor de um MSP para SMEs incluem:

### **Melhor controle sobre o orçamento de TI**

Os MSPs podem oferecer um portfólio completo de produtos e serviços comparado aos recursos internos relativamente limitados de SMEs. Optar pelos serviços de um MSP também leva a uma maior flexibilidade financeira e custos mais previsíveis, e com planos de cobrança ajustáveis, as SMEs também tem um melhor controle sobre seu orçamento de segurança e TI.

### **Consultor confiável com conhecimento e experiência**

As SMEs podem impulsionar o profundo conhecimento e ampla experiência da equipe de segurança e TI empregada pelos MSPs.

### **Foco no mercado e percepção**

Os MSPs que têm foco na segurança tem uma melhor percepção sobre as soluções de segurança disponíveis no mercado e podem fornecer ofertas de segurança personalizadas para seus clientes.

### **Inovação**

As equipes de segurança especializadas dos MSPs podem tornar a adoção e implementação de soluções inovadoras mais fáceis e ajudar os clientes a acompanhar os desenvolvimentos de mercado atuais.

### **Preparados para mudança**

Os MSPs permitem a seus clientes adicionar ou remover qualquer software ou hardware de acordo com suas necessidades atuais sem ter que passar pelo doloroso processo de aquisição, implementação e manutenção de novos recursos de hardware e software.



CYBERSECURITY  
EXPERTS ON YOUR SIDE

A ESET é uma empresa pioneira em proteção antivírus que nasceu há mais de 25 anos com a criação do multipremiado software para detecção de ameaças ESET NOD32 Antivírus. Agora, o objetivo da ESET é garantir que todos possam aproveitar as grandes oportunidades que a tecnologia oferece. Hoje, nossas soluções de segurança permitem que as empresas e os consumidores em mais de 180 países possam aproveitar mais o mundo digital.

© Copyright 1992-2019 por ESET, LLC y ESET, spol. s.r.o. Todos os direitos reservados.

[www.eset.com/br](http://www.eset.com/br)