# SEGURANÇA DA INFORMAÇÃO

eBook 5

*Neste eBook vamos abordar sobre o gerenciamento de incidentes, sobre o uso de serviços de nuvem e aplicativos de terceiros, sobre o uso de dispositivos pessoais nas empresas e sobre parcerias com fornecedores confiáveis.*

## Gerenciamento de incidentes

Um incidente pode ser definido como qualquer **evento que interrompe ou prejudica** a prestação de serviços da empresa, incluindo falhas de hardware ou software, problemas de rede, problemas de segurança, desastres naturais, entre outros.

E no âmbito das empresas, o gerenciamento de incidentes é um processo de **identificação**, **resposta**, **análise**, **mitigação**, **documentação** e **solução** de incidentes que podem afetar a sua operação normal.

Ele é importante porque permite que a organização possa responder rapidamente a qualquer incidente que possa afetar seus negócios. E um **plano de gerenciamento** bem estruturado ajuda a minimizar o tempo de inatividade e os impactos financeiros.

Além dos impactos para as empresas, podem haver possíveis impactos para os **clientes**. Nestes casos, as empresas também devem considerar as **normas e regulamentações**, em especial as relacionadas com a segurança de dados pessoais como a LGPD.

## Uso de serviços de nuvem e aplicativos de terceiros

O uso de serviços de nuvem e aplicativos de terceiros tem se tornado cada vez mais comum, mas também pode apresentar riscos à segurança da informação.

Por isso, é importante seguir algumas boas práticas para minimizar esses riscos, como:

### Reputação do Provedor

Antes de escolher um serviço ou aplicativo de um provedor de serviços de nuvem ou fornecedor de aplicativos de terceiros, a empresa deve realizar uma avaliação completa do provedor ou fornecedor, incluindo sua reputação, segurança e histórico de incidentes de segurança.

### Monitoramento

O monitoramento das atividades dos usuários nos serviços de nuvem e aplicativos de terceiros deve ser contínuo, para que se possa detectar e responder rapidamente a qualquer atividade suspeita.

### Políticas de Segurança

Ter políticas de segurança claras, incluindo quais tipos de dados podem ser armazenados e compartilhados e quais requisitos de segurança devem ser atendidos.

### Criptografia

Os dados devem ser criptografados, para garantir que não possam ser acessados por usuários não autorizados.

### Backups

Os backups devem ser frequentes, para garantir que os dados possam ser restaurados em caso de perda ou corrupção de dados.

### Senhas de Acessos

A empresa deve garantir que os usuários tenham senhas fortes e exclusivas para acessar os serviços de nuvem e aplicativos de terceiros, e limitar o acesso somente aos usuários autorizados.

### Atualizações

E os softwares de acesso aos serviços de nuvem e aplicativos de terceiros devem estar sempre atualizados, para garantir que quaisquer vulnerabilidades sejam corrigidas.

## Uso de dispositivos pessoais

Quando permitido na empresa, o uso de dispositivos pessoais oferece algumas vantagens, como permitir uma maior flexibilidade. No entanto, também pode apresentar riscos e, por isso, é importante seguir algumas boas práticas para garantir a segurança da informação.

#1
**Política de Segurança da Informação**

As empresas devem ter uma seção clara e destinada ao "traga o seu próprio dispositivo", mais conhecido em inglês como BYOD, que estabeleça regras para o uso de dispositivos pessoais e profissionais no local de trabalho.

#2
**Senhas fortes**

Os funcionários devem usar senhas fortes e exclusivas para seus dispositivos e contas de trabalho; e também devem configurar a autenticação de dois fatores sempre que possível.

#3
**Atualizações regulares**

Os dispositivos devem ser mantidos atualizados com as últimas verificações de segurança e correções de software.

#4
**Criptografia de dados**

Os funcionários devem criptografar os dados armazenados nos dispositivos utilizados, especialmente dados confidenciais relacionados ao trabalho.

#5
**Restrições de uso**

A empresa pode impor restrições ao uso de dispositivos pessoais, como a proibição de uso em redes públicas ou a exigência de usar uma VPN para se conectar à rede corporativa.

#6
**Segregação de dados**

Os funcionários devem separar dados pessoais e profissionais nos dispositivos utilizados, evitando o armazenamento de dados confidenciais da empresa em dispositivos pessoais.

#7
**Controle de acesso**

A empresa pode adotar soluções de controle de acesso para limitar o acesso aos dados corporativos apenas aos funcionários autorizados.

#8
**Limpeza remota**

A empresa pode estabelecer uma seção na política de SI sobre dispositivos pessoais em caso de perda ou roubo, para garantir que dados confidenciais não caiam em mãos erradas.

## Parcerias com Fornecedores Confiáveis

A escolha de fornecedores confiáveis é uma parte importante da estratégia de segurança da informação de qualquer empresa, pois pode afetar diretamente a segurança e a privacidade dos seus dados confidenciais.

Os fornecedores confiáveis são aqueles que atendem a padrões rigorosos de segurança e privacidade. Eles são confiáveis porque implementam medidas robustas de segurança em seus produtos e serviços, incluindo criptografia forte, autenticação e autorização adequadas, testes de segurança regulares e conformidade com regulamentações e normas de segurança relevantes.

Além disso, os fornecedores confiáveis geralmente têm uma reputação sólida e histórico de sucesso no fornecimento de produtos e serviços de segurança da informação para outras empresas. Eles também fornecem transparência em relação às suas políticas e práticas de segurança da informação, incluindo a divulgação de violações e a implementação de medidas para corrigir vulnerabilidades.