# Introdução da aula



Caro estudante,

Ao longo da Aula 6 teremos a oportunidade de estudar e debater a temática vinculada à proteção de dados.

Muito tem se falado da Lei Geral de Proteção de Dados Pessoais (LGPD), e iniciaremos nossa jornada sobre a temática de privacidade e proteção de dados com uma visão mais ampla, ou seja, pelo olhar da proteção de dados das empresas. A temática vinculada à LGPD é exclusiva para a proteção de dados pessoais das pessoas naturais, o que será objeto da Aula 7.

Compõe uma parcela relevante do patrimônio de qualquer empresa (lato sensu) a proteção de seus dados, de seus segredos comerciais e industriais e mesmo de suas estratégias de lançamentos de produtos e serviços, de forma que a segurança da informação e a adoção de boas práticas para a segurança de tais dados é fundamental para o bom desenvolvimento da atividade empresarial.

# Segurança da informação dentro das empresas



Usualmente quando pensamos em segurança da informação cibernética, temos como referência os ataques hackers, vírus e ransomware – um tipo de sistema utilizado para a prática de extorsão que pode bloquear o computador e depois exigir um resgate para desbloqueá-lo, também identificado nas hipóteses de criptografia de todos os dados de um servidor ou computadores.

No entanto, muitas vezes a falta de segurança cibernética tem origem nos próprios usuários internos da empresa e na falta de boas práticas e de uma regra clara e correta de segurança da informação (SI).

**E o que é segurança da informação (SI)?**

É a estratégia adotada dentro das empresas para evitar a perda ou roubo de informações. O termo é usado para se referir à defesa de dados, e sua prática assegura que as informações sigilosas sejam acessadas apenas por aqueles às quais elas pertencem ou pelos seus responsáveis de direito.

Para as empresas a segurança de informação – que é controlada pelo departamento de Tecnologia da informação (TI) de uma empresa – é uma grande aliada e assegura que as informações de uma empresa não sejam distribuídas de forma indevida.

De acordo com a Pesquisa Global de Segurança da Informação realizada em 2018 pela PwC, 46% dos incidentes de segurança no Brasil atingem as informações dos clientes das empresas. Outros 34%, dos seus funcionários. (PWC, 2018)

De maneira geral a segurança da informação protege e analisa:

* Uso.
* Acesso não autorizado.
* Uso indevido.
* Divulgação.
* Modificação.
* Gravação.
* Destruição.
* Interrupção de informações.

Os três pilares da segurança da informação são: Confidentiality (confiança), Integrity (integridade) e Availability (disponibilidade), termos que formam o acrônimo “CIA”.

* (**C**IA) confidencialidade: garante que as informações não sejam divulgadas a pessoas ou entidades não autorizadas.
* (C**I**A) integridade: mantém a precisão da informação durante todo seu ciclo de vida.
* (CI**A**) disponibilidade: garante que qualquer informação esteja disponível quando necessário.

Para a preservação mínima de uma SI (segurança da informação), é recomendável que a empresa aplique os seguintes controles de segurança:

**Controle de segurança lógicos**

* Controle de acesso: senhas, cartões de acesso, biometria.
* Criptografia: mecanismo para tornar alguma informação ilegível a outra pessoa ou outro sistema.
* Assinatura digital: mecanismo para gerar e validar dados digitais.
* Hashing: uma forma de checagem de arquivos para garantir sua integridade.
* Certificação: atesta a validade de um documento.

**Controles de segurança físicos**

* Câmeras de segurança.
* Portas.
* Fechaduras.
* Muros.
* Alarmes de fumaça e incêndio.
* Guardas de segurança.

A segurança da informação não é apenas mais uma questão de estratégia dentro das empresas, mas uma peça fundamental no funcionamento do negócio. A conhecida expressão “Scientia potentia est” – “conhecimento é poder” – nunca esteve tão correta: com a quantidade de informações produzidas diariamente o conhecimento se torna realmente um poder, por isso a segurança da informação é tão importante hoje em dia para uma empresa.

# Da segurança e do sigilo de dados, fiscalização e posse sobre arquivos digitais



A proteção de dados e informações tem como base a privacidade de informação, de comunicação e de opinião, e aplica-se a qualquer operação de tratamento de dados e informações realizadas por pessoa natural ou jurídica de direito público ou privado. Dada a gravidade do tema, o tratamento dos dados e informações deve ser conduzido com ética, responsabilidade, transparência, segurança e privacidade.

A segurança e o sigilo de dados ditam expressamente o que é preciso para proteger os dados dos seus clientes – sem essa proteção, qualquer organização estará sujeita a sofrer um ataque. Há inúmeras maneiras de ocorrer um vazamento de dados, e conhecer suas possíveis vulnerabilidades possibilita a proteção preventiva, reduzindo os riscos de ataques.

Quando falamos de ataques cibernéticos devemos focar dois tipos:

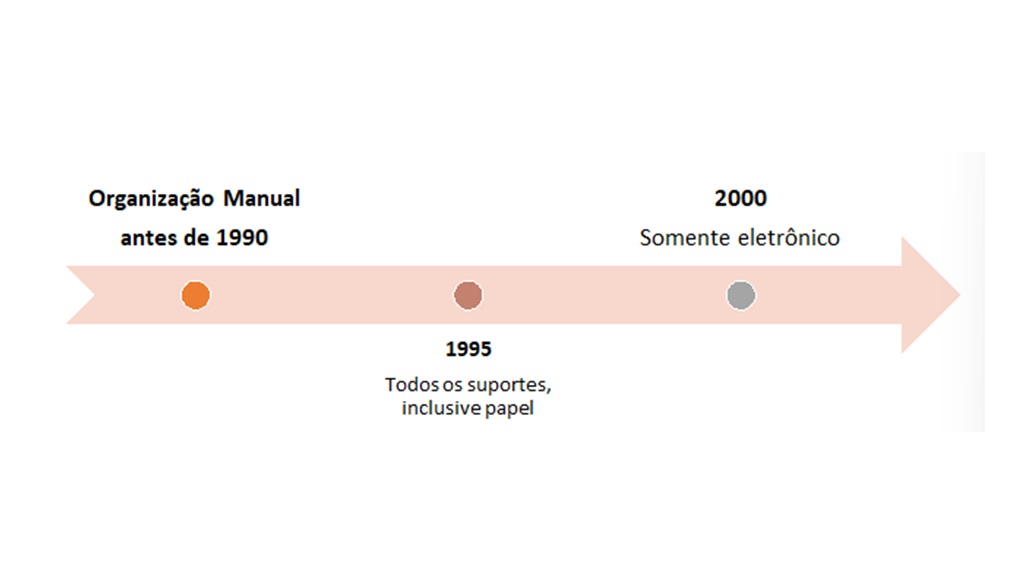
* Outsider: o atacante não está dentro da instituição.
* Insider: o atacante está dentro da instituição.

Para uma boa política de segurança da informação, seja em relação a ataques cibernéticos vindos de dentro ou de fora da empresa/instituição, é fundamental que as empresas estejam focadas em boas práticas de gestão eletrônica de documentos (GED).

**Gestão Eletrônica dos Documentos (GED)**

A inovação tecnológica tem ajudado na otimização do desempenho; o CRM (software para a gestão do relacionamento com o cliente) ajuda a função de vendas e marketing, o LMS (software de gestão da aprendizagem em instituições de ensino) ajuda o aprendizado e o desenvolvimento vertical, e um software de recursos humanos baseado em nuvem ajuda o departamento de recursos humanos. Um sistema de gerenciamento de documentos é o que ajuda os hospitais, por exemplo, a simplificar suas operações, e um sistema de gerenciamento de dados (DMS) é usado para rastrear e armazenar documentos reduzindo o uso de papel, capaz de guardar registros que podem ser criados e modificados por diferentes usuários.

A Figura 1 apresenta aspectos inerentes às características provenientes do gerenciamento eletrônico, mostrando um modelo baseado na gestão de documentos de arquivo.



Até 2012 havia, no Poder Judiciário, processos físicos em grande parte dos Estados do Brasil. Por questões orçamentárias, alguns Estados ainda estão fazendo a transição de arquivos físicos para eletrônicos em 2022. Mas, de acordo com regras do Conselho Nacional de Justiça (CNJ), todo o Poder Judiciário já deveria ter migrado para o formato eletrônico desde 2012.

Um processo físico no fórum pode passar por algum controle de circulação, mas há várias ocorrências de autos de processo que sumiram ou que tiveram documentos extraviados e/ou subtraídos – e há, ainda, as situações de acidentes como enchentes, incêndios etc. O próprio Código de Processo Civil sempre manteve a previsão do procedimento de restauração de autos.

Um processo físico gerava um grande esforço dos advogados e das partes. Constantes idas e vindas aos fóruns, muitas vezes infrutíferas, e grande dispêndio de tempo e dinheiro.

Compare com a atual situação dos processos eletrônicos, os quais estão disponíveis 24 horas por dia, sete dias por semana para qualquer interessado nos processos públicos ou para qualquer dos interessados cadastrados nos processos sob segredo de justiça. Até mesmo a gestão de acesso aos processos em segredo de justiça tornou-se mais eficiente.

A probabilidade de extravio e/ou perda de um processo eletrônico é remota, embora saibamos das situações de ataques cibernéticos em diversos tribunais pelo país, incluindo os tribunais superiores. Mas uma boa gestão de segurança da informação e uma adequada estrutura de backups torna todo o sistema inúmeras vezes mais seguro e eficiente.

# Boas práticas e cuidados vinculados ao uso da Internet



Boas práticas no uso de recursos de TI partem do princípio do bom senso. A falta de prudência acaba afetando outros usuários; portanto, deve-se ter consciência das limitações e dependências dos recursos.

É fundamental que o tema segurança da informação e boas práticas esteja constantemente sob escrutínio dos executivos responsáveis pela gestão de empresa, independentemente do porte empresarial. O assunto é de importância crucial para a empresa, pois além das questões vinculadas à própria segurança da informação, também há a preocupação com as questões reputacionais em tempos de comunicação massificada, como ocorre com as redes sociais e a própria internet.

Considere a situação de um escritório de advocacia que deixe de adotar boas práticas de segurança da informação e tenha os seus dados sequestrados? A comunicação de tal fato aos seus clientes pode resultar em falta de credibilidade no escritório e até no fechamento da empresa. Veja o quanto é grave a situação.

Usar a internet para fazer compras, acessar dados bancários ou navegar pelas redes é algo muito prático hoje em dia, por isso o cuidado deve ser redobrado – com apenas um clique você poderá divulgar suas informações e ter sua máquina contaminada por malwares, os vírus. Entretanto há maneira seguras de se proteger, conforme segue:

* Aprenda a respeito do mundo virtual: procure informações que tratem de segurança e proteção na internet. Informe-se.
* Não salve suas senhas: o mundo da internet é muito perigoso e um deslize pode fazer você ter seus dados descobertos. Portanto, por mais que o computador não salve a sua senha. E alterá-la de forma periódica é um ótimo meio de segurança.
* Não instale softwares suspeitos, e atenção aos downloads: na dúvida, não instale.

A abordagem de privacidade é caracterizada por medidas proativas e não reativas, antecipando eventos evasivos – uma ação preditiva e preventiva sempre com ênfase no binômio segurança e prevenção.

Quando o assunto é segurança, todo cuidado ainda é pouco. A praticidade oferecida pelos smartphones pode se tornar uma arma nas mãos de pessoas má intencionadas, que procuram qualquer brecha para obter dados sensíveis e particulares. As redes sociais, por terem grande apelo, são sítios muito frequentados, e as pessoas são atacadas por vírus, pishing ou cyberbullying.

Portanto, procure sempre informações na internet sobre maneiras de se proteger.

# Videoaula: Privacidade e proteção de dados empresarial

Caro estudante, ao longo desta aula tratamos de privacidade de dados, segurança da informação e boas práticas com ênfase nas relações jurídico-empresariais.

Como sabemos, o patrimônio de uma empresa é formado por diversos bens (materiais e imateriais), direitos e deveres/obrigações.

Entre os bens que compõem o patrimônio de uma empresa está sua reputação perante o mercado (direito da personalidade), além de seus dados e informações, os quais podem compor todo o histórico das relações mantidas com clientes, dados e informações de segredos comerciais e/ou industriais e muito mais. E é deste tipo de informação e dado que tratamos na presente aula.

Na próxima aula trataremos especificamente dos dados pessoais das pessoas naturais, os quais são protegidos pela LGPD e pelo resto do sistema legal.

# Saiba mais



Ao longo da presente aula tivemos a oportunidade de analisar brevemente os institutos vinculados à segurança da informação e boas práticas.

Tal instituto está diretamente vinculado a regras internacionais de qualidade e metodologia de trabalhos de prevenção e segurança, conhecidos no Brasil pelas regras da ISO ABNT 27000, 27001, 27002 e 18044.

Recomendamos a leitura das respectivas regras e comentários apresentados pela Patrícia Peck no capítulo 8.13. de seu livro Direito Digital Segurança da Informação e as ISOs 27002, 18044 e 27001, disponível na base eletrônica da Minha Biblioteca.

PECK, P. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016. E-book. ISBN 9788502635647. Disponível na base eletrônica da Minha Biblioteca.

Além do artigo referido, igualmente indicamos o estudo e a análise de [questões vinculadas à segurança da informação quanto ao monitoramento de correspondência eletrônico (e-mail) dos empregados pelo empregador](https://www.conjur.com.br/2014-nov-24/rodrigo-reboucas-lei-12965-nao-aplicavel-relacao-trabalho).

Bons estudos!

# Referências



ASSIS, C. de. **Confira 10 importantes dicas de segurança na internet**. Uninassau, 31 mar. 2017. Disponível em: <https://www.uninassau.edu.br/noticias/confira-10-importantes-dicas-de-seguranca-na-internet>. Acesso em: 21 nov. 2022.

BRASIL. **Guia de Boas Práticas**. Lei Geral de Proteção de Dados (LGPD). Governo Federal, ago. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>. Acesso em: 21 nov. 2022.

CENTRO DE TECNOLOGIA DA UNIVERSIDADE FEDERAL DO RIO GRANDO DO NORTE. **Boas práticas no uso da internet**. CT-UFRN, 1 dez. 2012. Disponível em: <https://www.ct.ufrn.br/boas-praticas-do-uso-da-internet/>. Acesso em: 21 nov. 2022.

DOCUSERVE. Por que os hospitais precisam de um sistema de gerenciamento de documentos. Docuserve, [s. d.]. Disponível em: <https://docuserve.com/blog-post/why-hospitals-need-document-management-systems/>. Acesso em: 19 jun. 2020.

HENRIQUE, E. **Boas práticas para garantir a segurança no uso da internet**. BrunSker, 23 out. 2020. Disponível em: <https://www.brunsker.com.br/boas-praticas-para-garantir-a-seguranca-no-uso-da-internet/>. Acesso em: 21 nov. 2022.

NEOWAY. Segurança da Informação: O que é, e seus impactos e soluções nas empresas. Neoway, 23 dez. 2020. Disponível em: <https://blog.neoway.com.br/seguranca-da-informacao/>. Acesso em: 21 nov. 2022.

PECK, P. **Direito Digital**. 6 ed. São Paulo: Saraiva, 2016. E-book. ISBN 9788502635647. Disponível em: Minha Biblioteca. Acesso em: 28 nov. 2022.

PWC. The Global State of Information Security® Survey**2018** - Fortalecendo a sociedade digital contra o caos cibernético. PWC, 2018. Disponível em: <https://www.pwc.com.br/pt/global-state-of-information-security-survey-2018.html>. Acesso em: 28 nov. 2022.

RESH CYBER DEFENSE. LGPD: Segurança e Sigilo de Dados. Resh, [s. d.]. Disponível em: <https://resh.com.br/blog/lgpd-seguranca-e-sigilo-de-dados/>. Acesso em: 21 nov. 2022.

SERPRO. **Quem vai regular a LGPD?** Serpro, [s. d.]. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 21 nov. 2022.

THOMAZ, K. P.; SANTOS, V. M. Metadados para o gerenciamento eletrônico de documentos de caráter arquivístico – GED/A: estudo comparativo de modelos e formulação de uma proposta preliminar. **Revista DataGramaZero**, v. 4, n. 4, ago. 2003. Disponível em: <https://brapci.inf.br/_repositorio/2010/01/pdf_2c9b077fe3_0007504.pdf>. Acesso em: 19 jun. 2020.

TUTIDA, D. **O que é segurança da informação?** Saiba como garantir a sua. Encontre um Nerd S/A, 10 ago. 2021. Disponível em: <https://encontreumnerd.com.br/blog/o-que-e-seguranca-da-informacao>. Acesso em: 21 nov. 2022.

VELASCO, A. **O que é Segurança da Informação?** CanalTech, 23 dez. 2019. Disponível em: <https://canaltech.com.br/seguranca/seguranca-da-informacao-o-que-e-158375/>. Acesso em: 21 nov. 2022.