DataPrivacyBR

CURSO

# Segurança da Informação e Proteção de Dados: da Gestão à Resposta a Incidentes

**EMENTA**

# PROFESSORES

## ISABELLA HAMAOUI BECKER

IIsabella é advogada formada pela FGV-SP, tendo migrado para a área de segurança cibernética após experiência internacional em threat intelligence e monitoramento ativo de dados vazados em ambientes de deep web e surface.

Especializou-se em proteção de dados e implementou programas de governança de dados e gestão de privacidade em inúmeras instituições ao longo da sua carreira como gerente de cibersegurança na KPMG. É certificada pela Exin (DPO) e pela IAPP (CIPP e CIPM). Recentemente assumiu a cadeira de DPO do Grupo Boticário, onde é responsável pela prática de proteção de dados.

## ADRIANA PRADO

Adriana Prado é Diretora-Executiva e líder no Brasil do segmento de Comunicação Estratégica da consultoria internacional FTI Consulting. Com mais de 15 anos de experiência e passagens por alguns dos principais veículos de imprensa e agências de comunicação do país, é especialista em Comunicação de Crise, tendo ajudado dezenas de empresas a se prepararem para e responderem a situações críticas, incluindo incidentes cibernéticos. É apontada pela Leaders League como uma das principais profissionais em Comunicação de Crise e de Gestão de Crises do Brasil. Também foi membro dos comitês de Crise e de Compliance da Associação Brasileira de Comunicação Empresarial (Aberje). Faz palestras e workshops sobre resposta a incidentes cibernéticos em parceria com grandes instituições do mercado, no Brasil e em outros países da América Latina. Antes da FTI, foi diretora da consultoria internacional de comunicação Brunswick Group. Também já trabalhou para a agência de comunicação brasileira FSB e em alguns dos principais veículos de imprensa do país, como os jornais O Globo e Extra, a rádio CBN e a revista ISTOÉ. Colaborou por mais de dois anos como blogueira e tradutora com o Centro Knight para o Jornalismo nas Américas, da Universidade do Texas em Austin, Estados Unidos. É formada pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) e tem pós-graduação em Comunicação, Mercados e Tecnologia da Informação da Fundação Instituto de Administração (FIA-SP).”

# 1. DESCRITIVO

Proteção de dados e cibersegurança são elementos distintos mas que possuem uma íntima conexão, sendo a segurança da informação um importante elemento para garantir a conformidade com as regras de proteção de dados e os direitos dos titulares.

Muito anteriormente à promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, "LGPD"), o Marco Civil da Internet (Lei nº 12.965/2014, "MCI") e seu decreto regulamentador (Decreto nº 8.771/2016) já haviam estabelecido um primeiro patamar de regulação sobre o tema no contexto brasileiro, em conjunto com os padrões internacionais amplamente adotados pelo mercado, como os ISOs 27001, 27002 e 27701, NIST CSF e CIS Controls.

A LGPD adicionou uma nova camada a essa legislação e contribuiu para o amadurecimento da regulação existente, elevando a segurança da informação ao status de agenda prioritária para diferentes stakeholders, como organizações, autoridades de enforcement e os próprios cidadãos e consumidores.

Dados recentes do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) são ilustrativos desse cenário: com base nas estatísticas de incidentes reportados ao CERT.br, considerados os valores acumulados da série histórica de 1999 a 2020, houve um aumento expressivo de incidentes de segurança no Brasil. Até a primeira metade dos anos 2000, o número de incidentes reportados anualmente não ultrapassava a casa dos 50.000. Em 2014, foram reportados mais de 1 milhão de incidentes, número que se estabiliza na casa dos 750 mil nos últimos anos.[1]

Com o crescente reconhecimento da segurança da informação enquanto elemento de vantagem competitiva e a cada vez maior conscientização dos cidadãos sobre os direitos,  há também um crescimento exponencial dos custos reputacionais e financeiros associados à ocorrência de um incidente.

De acordo com o relatório "Cost of a Data Breach"[2] de 2024 feito pela IBM, um incidente de segurança de dados pessoais gera um prejuízo médio 4.88 milhões de dólares (incluindo recuperação do incidente, custos judiciais, custo de comunicação com autoridades e titulares e perda de receita em decorrência do incidente). Esse é o maior valor da série histórica do relatório, que está em seu décimo nono ano. No caso Brasileiro há um crescimento notável entre 2021 e 2022, intimamente ligado ao amadurecimento da regulamentação.

Dentro deste cenário, a Data Privacy Brasil realiza o curso "Segurança da Informação e Proteção de Dados: Gestão Estratégica e Resposta a Incidentes", com objetivo de capacitar profissionais a partir de uma abordagem teórica e prática.

1 https://www.cert.br/stats/incidentes/

2 https://www.ibm.com/uk-en/security/data-breach

Ao longo de quatro aulas, iremos tratar de aspectos jurídicos e regulatórios da segurança da informação, a obrigação de reportar incidentes de segurança e boas práticas ao fazê-lo, aspectos técnicos de ferramentas de segurança e compreender como ataques e vulnerabilidades ocorrem e são exploradas. Por fim, iremos também trazer um olhar estratégico para a gestão de risco e como desenhar e gerir de forma adequada um plano de resposta a incidentes de segurança, pensando tanto em aspectos jurídicos quanto reputacionais.

Comumente abordados em tópicos separados, neste curso propomos uma análise integrada e interdisciplinar da Segurança da Informação e da Proteção de Dados Pessoais. A partir da apresentação dos principais termos, técnicas e conceitos de tecnologia e segurança da informação aplicados à proteção de dados pessoais, o curso pretende trazer aprendizados sobre o tema a partir da análise comentada de casos e experiências reais, auxiliando gestores, advogados, analistas e tomadores de decisão a terem uma visão mais integrada dos desafios relacionados à segurança da informação com objetivo de possibilitar a criação de uma estratégia de cibersegurança.

## 1.1. OBJETIVO GERAL

Compreender como pensar e estruturar uma estratégia de cibersegurança voltada para a privacidade e proteção de dados, conectando aspectos jurídicos relativos à proteção de dados com aspectos técnicos ligados à segurança da informação, privacy by design, arquitetura e bancos de dados.

## 1.2. OBJETIVOS ESPECÍFICOS:

1. Demonstrar de forma simples e tangível conceitos tecnológicos voltados para a proteção de dados;
2. Compreender tecnologias envolvidas em protocolos, softwares e mecanismos de segurança;
3. Analisar e compreender tecnicamente tipos de ataques;
4. Debater casos e situações em que medidas técnicas mitigam riscos e danos em incidentes de segurança.
5. Analisar os pontos críticos de uma estratégia de cibersegurança.
6. Desenvolver um vocabulário unificado entre segurança da informação e proteção de dados pessoais.
7. Desenvolver habilidades de desenhar um plano de resposta à incidente, da montagem do time à gestão reputacional;

## 1.3. PÚBLICO ALVO

O Curso se destina a profissionais de diferentes áreas que se interessem em se capacitar e compreender um dos instrumentos mais comentados quando se fala em proteção de dados, a política de privacidade de uma organização.

Assim, espera-se que advogados, gestores, profissionais de compliance, especialistas em proteção de dados, administradores de organizações de pequeno e médio porte e pesquisadores possam se capacitar e atualizar seus conhecimentos na área. O curso possui um pré-requisito de conhecimento básico sobre proteção de dados. Espera-se que os alunos saibam os principais conceitos, como o que são dados pessoais, os princípios de proteção de dados e o que são bases legais.

## 1.4. CARGA HORÁRIA

Carga horária de 12h, ao longo de quatro aulas que ocorrerão de forma ao vivo entre 18h30 e 21h30.

## 1.5. METODOLOGIA

As aulas expositivas contarão com linguagem acessível, sem “juridiquês” ou “tecniquês”. O curso contará com a intersecção entre uma abordagem acadêmica, para trabalhar  e problematizar conceitos, e uma abordagem prática, analisando situações concretas e aplicando os conceitos previamente desenvolvidos.

Ao longo da exposição, os alunos serão chamados para interagir com os professores, além dos momentos dedicados a responder dúvidas e questionamentos. Cada aula terá um caso concreto que será usado como guia para as discussões.

Ainda, o curso contará com a utilização de ferramentas de ensino global de participação ativa dos alunos e alunas, por meio do problem-based learning, fornecendo fundamentos teóricos e práticos sobre segurança da informação e sua relação com a proteção de dados pessoais.

Na última aula do curso haverá um dia inteiramente dedicado a realização de uma atividade prática, sob supervisão de professoras que conduzirão a atividade e farão considerações acerca do trabalho desenvolvido pelos alunos ao final.

# 2. CRONOGRAMA

**AULA 01**
30/06

**SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS**
**Isabella Becker**
**1.** Introdução aos conceitos e pilares de segurança da informação. **1.1.** Disponibilidade **1.2.** Confidencialidade. **1.3** Integridade **2.** Proteção de Dados e Segurança da Informação: Intersecção e diferenças. **2.1.** Obrigações de proteção de dados e obrigações de segurança da informação na LGPD e outras legislações. **3.** Registro e Comunicação de Incidentes de Segurança: Obrigações ligadas à proteção de dados pessoais.

**AULA 02**
01/07

**PARÂMETROS TÉCNICOS DE SEGURANÇA DA INFORMAÇÃO**

**1.** Tecnologias envolvidas na gestão da segurança da informação. **2.** Tipos de ataques e principais vulnerabilidades. **3.** Medidas técnicas e organizacionais de mitigação de incidentes

**AULA 03**
02/07

**GESTÃO ESTRATÉGICA DE SEGURANÇA DA INFORMAÇÃO E RESPOSTA A INCIDENTES**
**Isabella Becker e Adriana Prado**
**1.** Gestão Estratégica de Segurança da Informação. **1.1** Mapeamento de ativos da organização. **1.2.** Ciclo de vida dos dados. **1.3.** Estrutura interna e externa de segurança. **1.4.** Monitoramento ativo e métricas **1.5.** Colaboração entre equipe jurídica e CISO. **1.6.** Avaliação de maturidade e etapas de uma boa política interna de segurança da informação. **2.** Resposta à incidentes: Gestão, comunicação e elementos de reputação da organização. **2.1.** Preparando um plano de resposta a incidentes. **2.2.** Composição de um time de respostas e papéis. **2.3.** Preparando a comunicação e assumindo o controle da narrativa

**AULA 04**
03/07

**ATIVIDADE FINAL: RESPOSTA A UM INCIDENTE DE SEGURANÇA**
**Isabella Becker e Adriana Prado**
**1.** Exercício prático: Desenvolver e executar um plano de resposta a incidente de segurança

# 3. ESTRUTURA DA BIBLIOGRAFIA

## LEITURA ESSENCIAL

Para melhor compreender a aula é essencial a leitura do material indicado. Sempre será sugerido um texto curto, em português e acessível.

## LEITURA COMPLEMENTAR

A leitura fundamental compreende um conjunto de textos que consideramos basilares para o tema da aula. É altamente recomendável a sua leitura como forma de estudo complementar.

## LEITURA APROFUNDADA

Textos voltados para alunos e alunas que desejarem se aprofundar no tema. São textos mais densos e que trazem mais informações e perspectivas sobre o assunto.

## LEITURA PRÁTICA E CONTEÚDO MULTIMÍDIA

Aqui você irá encontrar casos, julgados, reportagens, vídeos, podcasts, lives, seminários além de textos com enfoque eminentemente prático, ou seja, como aquele tema se aplica no dia-a-dia. Recomendações de autoridades de proteção de dados também se encontram nessa seção.

Aula 01

# Segurança da Informação e Proteção de Dados

Isabella Becker

## EMENTA

**1.** Introdução aos conceitos e pilares de segurança da informação. **1.1.** Disponibilidade **1.2.** Confidencialidade. **1.3.** Integridade **2.** Proteção de Dados e Segurança da Informação: Intersecção e diferenças. **2.1.** Obrigações de proteção de dados e obrigações de segurança da informação na LGPD e outras legislações. **3.** Registro e Comunicação de Incidentes de Segurança: Obrigações ligadas à proteção de dados pessoais.

## LEITURA ESSENCIAL

**MENKE, Fabiano. GOULART, Guilherme Damasio.** Segurança da Informação e Vazamento de Dados. In: BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (org.). Tratado de proteção de dados pessoais. Sp: Forense, 2020.

**LUCIANO, Maria.** Vazamentos de dados na LGPD: em busca do significado de "incidentes de segurança". Revista do Advogado, n. 144, nov 2019.

## LEITURA COMPLEMENTAR

Contribuição Data Privacy Brasil - Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais

## LEITURA APROFUNDADA:

**ABREU, Jacqueline.** Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Revista UniCEUB.

**BIONI, Bruno Ricardo. CANABARRO, Diego R.** Ainda sobre o bloqueio mais recente do WhatsApp no Brasil. Jota, 2016.

**SOMBRA, Thiago. BIONI, Bruno Ricardo.** O bloqueio do LinkedIn na Rússia: não falta mais combinar com os russos. Jota, 2016.

## LEITURA PRÁTICA E CONTEÚDO MULTIMÍDIA:

**MONTEIRO, Renato Leite.** Decreto Regulamentador do Marco Civil da Internet. CGI.br e NIC.br. VII Seminário de Proteção à Privacidade e aos Dados Pessoais.

**SOLOVE. Daniel.** The FTC Zoom Case: Does the FTC Need a New Approach? Linkedin. 2020

**Observatório da Privacidade.** Dadocracia – Episódio 38 – Piratas de computador. 2020.

**FENNESSY, Caitlin.** The Skill Set Needed to Implement a Global Privacy Standard: ISO/IEC 27701 alignment with IAPP CIPM and CIPP/E certifications. IAPP.

**EDPB.** Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01). 2018.

**HBO.** Last Week Tonight: Equifax. 2017.

**Information is Beautiful.** World's Biggest Data Breaches.

**Live Data Privacy Brasil.** Vazamento de dados. 2020

**MPDFT.** Caso Netshoes. Portaria de Instauração do Inquérito Civil Público – ICP.

**MPDFT.** Termo de ajustamento de conduta entre Netshoes e MPDFT.

**WIRED.** Inside the Twitter Hack—and What Happened Next. 2020

**Autoriteit Persoonsgegevens (DPA-Holanda)**. Multa Booking.com por incidente de segurança. 2020

Aula 02

# Parâmetros Técnicos de Segurança da Informação

## EMENTA

**1.** Tecnologias envolvidas na gestão da segurança da informação. **2.** Tipos de ataques e principais vulnerabilidades. **3.** Medidas técnicas e organizacionais de mitigação de incidentes

## LEITURA ESSENCIAL

**BUENO, Samira; LIMA, Renato Sérgio de; SOBRAL, Isabela.** Roubos e furtos de celulares são portas de entrada do crime organizado para o mundo virtual e peça-chave no crescimento do medo e da insegurança da população. In:FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 18º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2024. p. 82-85.

**SILVERGUARD; SOS GOLPE.** Estudo Golpes com Pix 2024. São Paulo: Silverguard, 2024.

**BUENO, Samira; LIMA, Renato Sérgio de; SOBRAL, Isabela.** Roubos e furtos de celulares são portas de entrada do crime organizado para o mundo virtual e peça-chave no crescimento do medo e da insegurança da população. In:FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 18º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2024. p. 82-85.

## LEITURA COMPLEMENTAR

Cert.br - Cartilha de Segurança para Internet: Senhas

Cert.br - Cartilha de Segurança para Internet: Dispositivos móveis

CERT.br e ANPD - Cartilha de Segurança para Internet: FASCÍCULO VAZAMENTO DE DADOS

## LEITURA PRÁTICA E CONTEÚDO MULTIMEDIA

Clube Data Convida Carlos Cabral, Especialista na área de Cyber Threat Intelligence na Tempest

Dadocracia - ep. 172 - O golpe taí. Como proteger as vítimas?

Dadocracia - ep. 171 - O golpe taí. E tá todo mundo caindo

Aula 03

# Gestão Estratégica de Segurança da Informação e Resposta a Incidentes

Isabella Becker e Adriana Prado

## EMENTA

**1.** Gestão Estratégica de Segurança da Informação. **1.1.** Mapeamento de ativos da organização. **1.2.** Ciclo de vida dos dados. **1.3.** Estrutura interna e externa de segurança. **1.4.** Monitoramento ativo e métricas **1.5.** Colaboração entre equipe jurídica e CISO. **1.6.** Avaliação de maturidade e etapas de uma boa política interna de segurança da informação. **2.** Resposta à incidentes: Gestão, comunicação e elementos de reputação da organização. **2.1.** Preparando um plano de resposta a incidentes. **2.2.** Composição de um time de respostas e papéis. **2.3.** Preparando a comunicação e assumindo o controle da narrativa.

## LEITURA ESSENCIAL:

**SOMBRA, Thiago Luís. CASTELLANO, Ana Carolina Heringer.** Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. Revista do Advogado, n. 144, nov 2019. 6 páginas.

**CARVALHO, André Castro. SOUZA, Vinícius Lobianco.** Segurança da informação e resposta a incidentes de vazamento no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD). Revista do Advogado, n. 144, nov 2019.

**MARTINS, Pedro Bastos Lobo; SANTOS, Pedro Henrique.** Descomplicando a LGPD: comunicação de incidentes de segurança nos moldes da ANPD. São Paulo: Data Privacy Brasil Ensino, 2024.

**ANPD** - Formulário para envio de Comunicados de Incidentes de Segurança

## LEITURA COMPLEMENTAR:

**COSTA, Eduarda; SANTOS, Pedro Henrique M.** Análise de decisões #6: poder público sob sanção. São Paulo: Data Privacy Brasil, 2024.

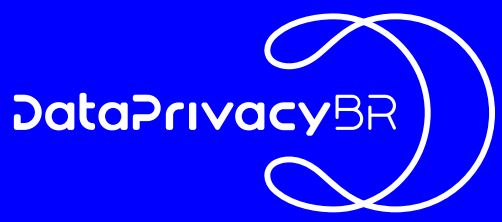
**ANPD** - Guia orientativo: segurança da informação para agentes de tratamento de pequeno porte

**OIAC -** Plano de resposta a incidentes de segurança (Data breach response plan)

## LEITURA PRÁTICA E CONTEÚDO MULTIMÍDIA:

**Ford Foundation** - Ferramenta de avaliação de segurança cibernética

**Oficina** - Estratégias de Cibersegurança para Privacidade e Proteção de Dados


DataPrivacyBR