# Melhores Práticas de Segurança Cibernética

ANBIMA

# MELHORES PRÁTICAS DE SEGURANÇA CIBERNÉTICA

ANBIMA

TIMELINE

JUL | OUT | 2014 | JAN | ABR | JUL | OUT | 2015 | JAN | ABR | JUL | OUT | 2016 | JAN | ABR

**Jul 2013**

IOSCO e WFE publicam resultados de pesquisa com 45 bolsas de valores

**Dez 2013**

Target Corp anuncia Cyber ataque violando info 40 mi de clientes

**Dez 2013**

Financial Stability Oversight Council organiza reunião para falar sobre Cybersecurity no sistema financeiro

**Jan 2014**

FINRA Cybersecurity é prioridade na supervisão

**Fev 2014**

CFTC publica Guia sobre Práticas de Segurança de Dados

**Mar 2014**

US SEC promove mesa redonda para discutir Cybersecurity

**Abr 2014**

US SEC promove iniciativa em Cybersecurity

**Mar 2014**

*SEC Chair Mary Jo White*

*"SEC have been focused on cybersecurity-related issues for some time"*

**Aug 2014**

JP Morgan reporta ataque que violou 83 milhões de contas e estabelece gastos anuais de **US$ 250 mi**

**Nov 2014**

Sony Pictures Custo divulgado foi de US$ 15 mi , podendo chegar a US$ 100 mi

**Jan 2014**

US SEC Estabelece Cybersecurity prioridade na supervisão

**Jan 2015**

FINRA Cybersecurity continua prioridade na supervisão

**Fev 2015**

FINRA Relatório de Práticas de Cybersecurity

**Fev 2015**

US SEC publica resultados de revisão temática

**Jun 2015**

OCC/FFIEC lança a ferramenta Cybersecurity Risk Assessment

**Jun 2015**

FFIEC estabelece Cybersecurity prioridade

**Jan 2016**

FINRA Cybersecurity continua prioridade na supervisão

**Out 2015**

US Senate aprova Lei Cybersecurity Info Sharing

**Ago 2014**

ANBIMA Supervisão foca em Cybersecurity

**Mai 2016**

CPI de Crimes Cibernéticos recomenda mudanças no SFN

**Mai 2016**

ANBIMA Promove debate sobre o assunto

**Abr 2016**

IOSCO publica Cyber Security in Securities Market

**Jun 2016**

*Robert Van Dijk Presidente da ANBIMA*

*"Cybersecurity é tema relevante no mercado"*

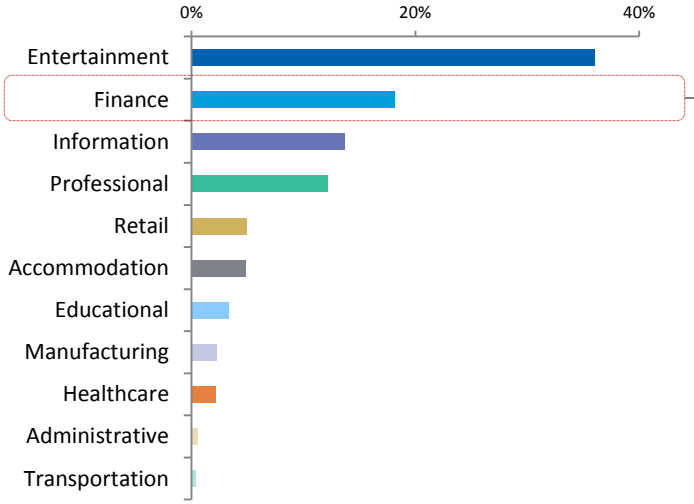
**ANBIMA**

Lança Guia de Cybersecurity

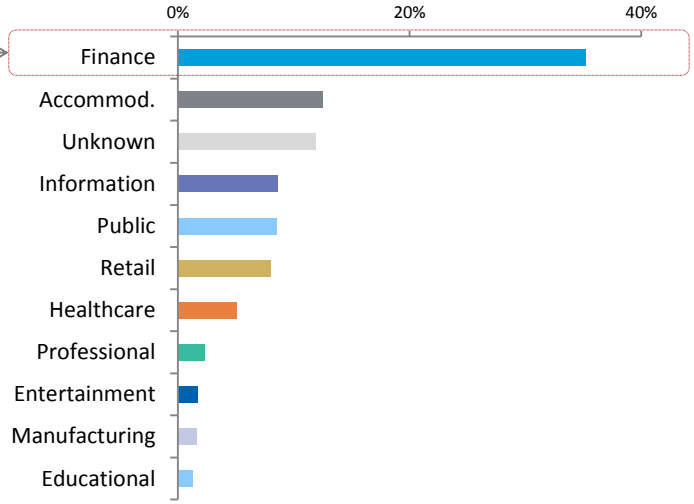
# Posição do Setor Financeiro em Violações de Dados

## Violações tem sido financeiramente motivadas

### 1. Incidentes por Setor[1]




### 2. Violação de Dados por Setor



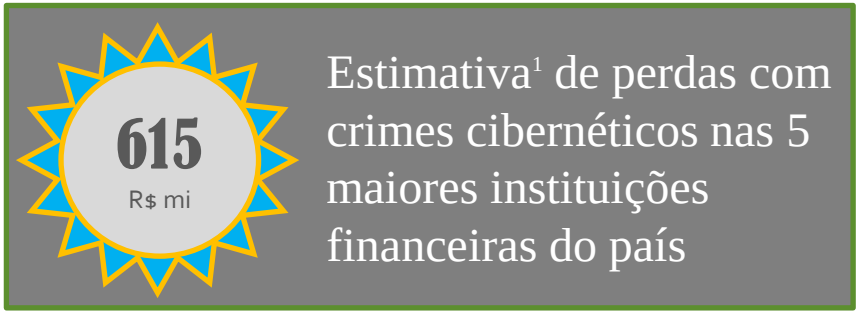

- **64.199** acidentes de violação de dados avaliados
- O Setor Financeiro vem sendo listado entre os 3 maiores alvos nos últimos anos
- **80%** das violações de dados foram motivadas por questões financeiras
- Espionagem esta em segundo lugar das motivações para violação de dados com 15%

- 5% dos incidentes resultaram em violação, exposição de dados
- Setor financeiro apresenta maior percentual de violação de dados
- 63% das violações envolveram questões com senhas fracas, comprometidas ou padrões

1. 2016 Data Breach Investigations Report. Visando uma melhor visualização dos dados relativos por setores, foram retirados das estatísticas os dados do setor público e os não categorizados (“unkown”) por computarem aproximadamante 74% (47,237) e 15% dos incidentes respectivamente.

# Tendências Regulatórias

## O mercado financeiro atualmente necessita de iniciativas dos reguladores




### Código Penal (Decreto-Lei 2.848/40)

Já prevê o crime de invasão de dispositivo informático (computador ou celular)

### CVM cria FinTech Hub (13/06/16)

Núcleo de Inovação em Tecnologias Financeiras que considera a intensificação do monitoramento das mudanças tecnológicas, mitigando eventuais riscos decorrentes e avaliar judiciosamente a necessidade de ajustes na **regulação e na supervisão de mercado**

### NECESSIDADES DE REGULAMENTAÇÃO

- Normatização para exigir das instituições financeiras o reporte compulsório da ocorrência de crimes cibernéticos
- Banco Central do Brasil deve criar mecanismos para contabilizar de maneira segregada o risco cibernético

### VARAS ESPECIAIS

- A criação de Varas Judicias Especializadas em Crimes Eletrônicos deverá dar maior celeridade ao tratamento desses crimes através da criação de equipes especializadas no âmbito da justiça
- Bloqueio e confisco de bens de criminosos cibernéticos

### PARCERIAS

- Banco Central do Brasil e Polícia Federal devem estabelecer relacionamento para compartilhar informações e manter bancos de dados

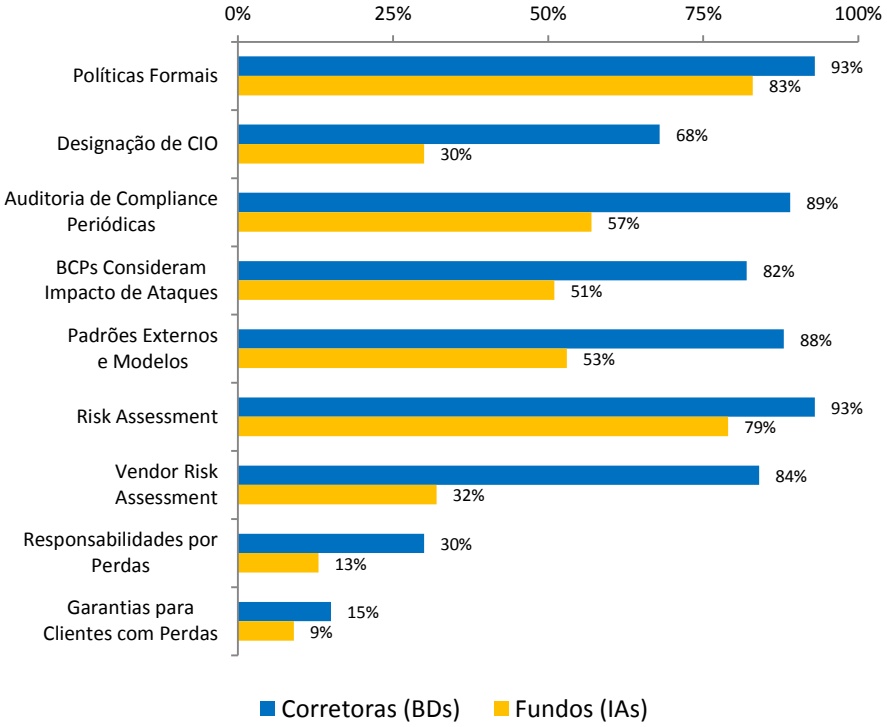
1. Relatório Final CPI dos Crimes Cibernéticos

# Inspeções Temáticas da Comissão de Valores Americana

## Objetiva identificação de pontos fracos em segurança cibernética no mercado de capitais

### 1. Governança e Risk Assessment [1]

O que encontra-se contemplado




#### POLÍTICAS DE SEGURANÇA DE INFORMAÇÕES

- Grande maioria dos participantes adotam políticas de segurança de informações, sendo que muitas corretoras e a maioria dos assets conduzem auditoria periódicas de compliance com essas políticas.
- Muitos participantes utilizam padrões e outros recursos de modelagem dos processos e arquiteturas, tais como NIST, ISO e FFIEC.
- Os planos de continuidade de negócios frequentemente endereçam o impacto de ataques cibernéticos, incluindo mitigação dos efeitos dos incidentes e planos de recuperação.

#### RISK ASSESSMENT

- Grande maioria dos participantes conduzem avaliações de riscos periódicas e desenham suas políticas e procedimentos usando isso como base.

#### POLÍTICAS ENDEREÇAM QUESTÕES PARA PERDAS

- Questões relativas a perdas financeiras geradas por ataques cibernéticos ainda são pouco evoluídas e não contam em políticas.

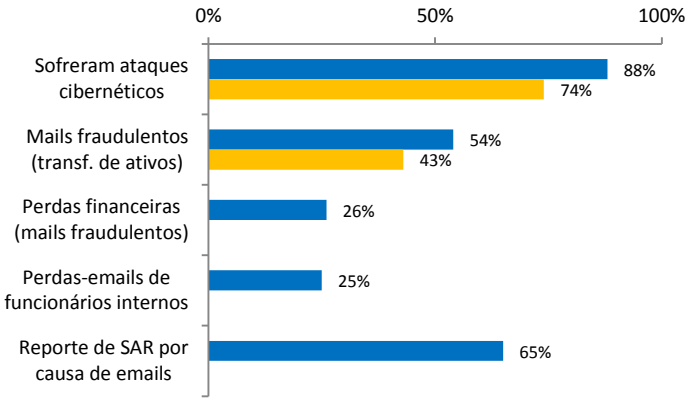
1. National Exam Program Risk Alert emitido por Office of Compliance Inspections and Examinations

# Inspeções Temáticas da Comissão de Valores Americana

## Objetiva identificação de pontos fracos de segurança cibernética no mercado de capitais

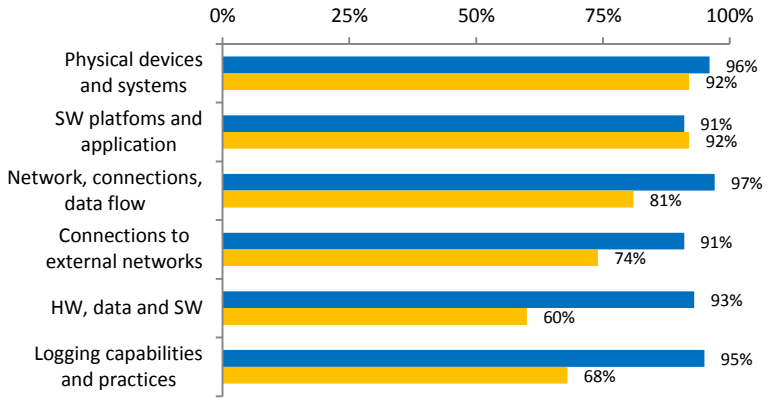
### 2. Incidentes Criminais [1]

Tipos de Incidentes e Medidas




### 3. Inventários e Mapeamento de Recursos [1]

Recursos de Tecnologia catalogados




### ATAQUES CIBERNÉTICOS (FRAUDES COM E-MAILS)

- A grande maioria reporta ter sofrido ataques cibernéticos diretos ou através de vendors. Em torno da metade reporta ter recebido e-mails fraudulentos pedindo transferência de fundos.
- Pouco mais de 1/4 das corretoras reporta perdas de mais de $5,000, mas nenhuma acima de $75,000 com tais e-mails. 1/4 dos casos desses e-mails são relativos a falhas de funcionários.
- 65% das corretoras efetuaram uma Comunicação de Atividade Suspeita (SAR) com o FINCEN.

### INVENTÁRIOS, CATALOGAÇÃO E MAPEAMENTO DE RECURSOS

- A vasta maioria reporta que efetua inventário, catalogação e mapamento, abrangendo toda a instituição, dos seus recursos de tecnologia, aparelhos, sistemas, redes.

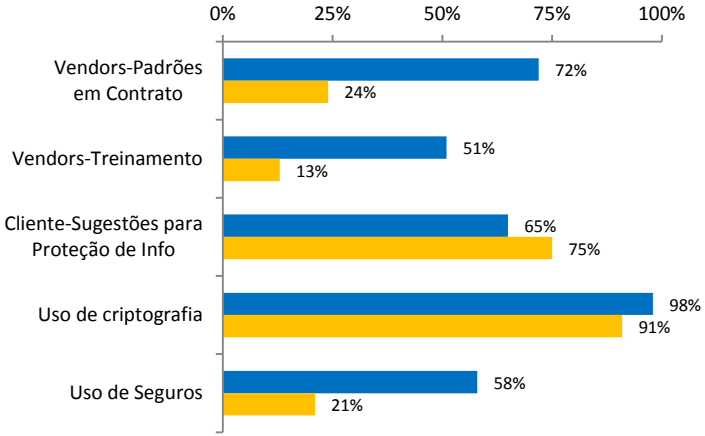
1. National Exam Program Risk Alert emitido por Office of Compliance Inspections and Examinations. Algumas informações somente disponíveis para a indústria de corretagem.

# Inspeções Temáticas da Comissão de Valores Americana

## Objetiva identificação de pontos fracos de segurança cibernética no mercado de capitais

### 4. Políticas com Vendors e Clientes [1]

Gestão do Risco com Vendors e Clientes




### POLÍTICAS DE RISCO COM VENDORS E CLIENTES

- A maioria das corretoras incorpora requerimentos sobre gestão de risco cibernético em seus contratos com vendors. Em contraste, poucos fundos assim o fazem.
- A maioria das corretoras possuem programas de treinamento para vendors e muito pouco dos fundos o faz.
- O uso da criptografia é um item já bem evoluído em ambos os setores.
- Um percentual razoável fornece alguma informação para seus clientes sobre o assunto.

### 5. Nível de Proteção de Risco da Indústria

Como a Industria está Preparada

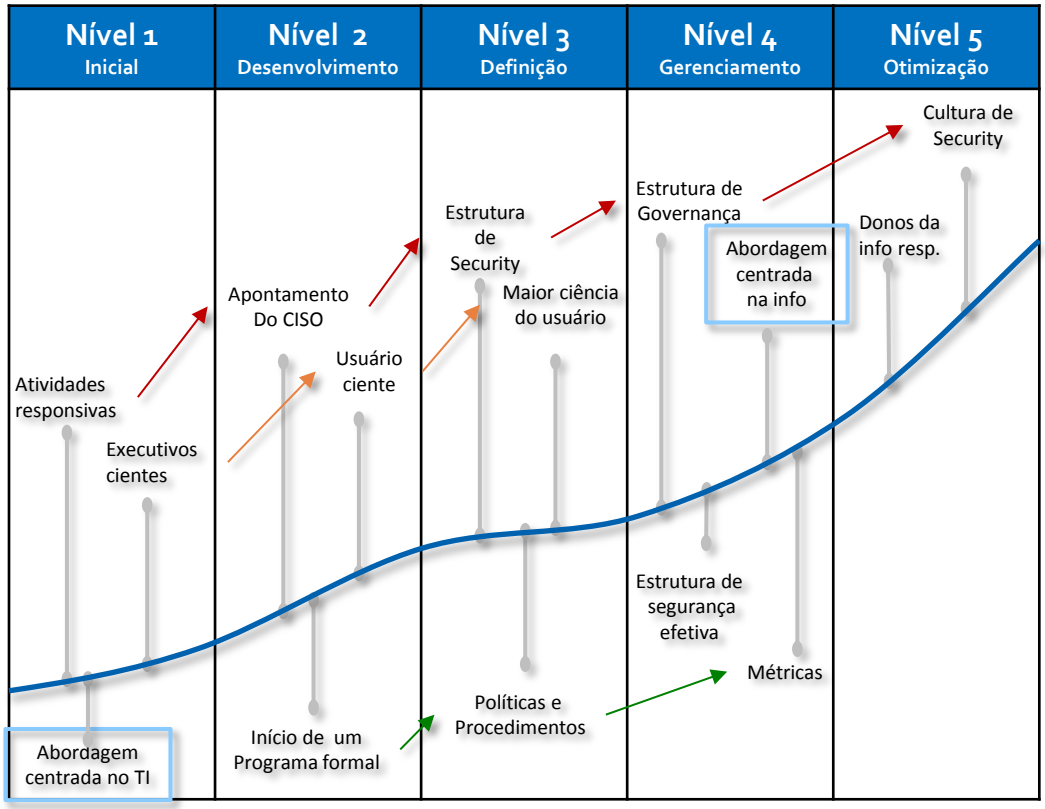
| | |
|---|---|
| BAIXO | **Ambos: Políticas Formais, Risk Assessment, Criptografia.** |
| | **Auditoria, Vendor RA, Contratos com Vendors, BCPs, Uso de Padrões Externos, Todos de Inventários e Map.** |
| | **Informações para Clientes, 4 de 6 itens de Inventários e Mapeamentos** |
| MÉDIO | CIO, Info para Clientes, Treinamento de Vendors, Seguros, |
| | Auditorias, BCPs, Uso de Padrões, 2 de 6 de Inventários e Mapeamentos. |
| ALTO | **Ambos: Definição de Responsabilidades por Perdas e Garantias para Perdas,** |
| | **CIO, Vendor RA, Uso de Seguros, Contratos com Vendors, Treinamento de Vendors.** |

1. National Exam Program Risk Alert emitido por Office of Compliance Inspections and Examinations
2. Algumas informações somente disponíveis para a indústria de corretagem.

# Avaliando a Maturidade da Sua Governança

## Evolução dos aspectos relevantes na construção de uma estrutura

### 8. ITScore Maturity Levels for Information Security [1]




- Maturidade da Estrutura
- Grau de consciência do risco de segurança da informação.
- Procedimentos e controles
- Foco da abordagem

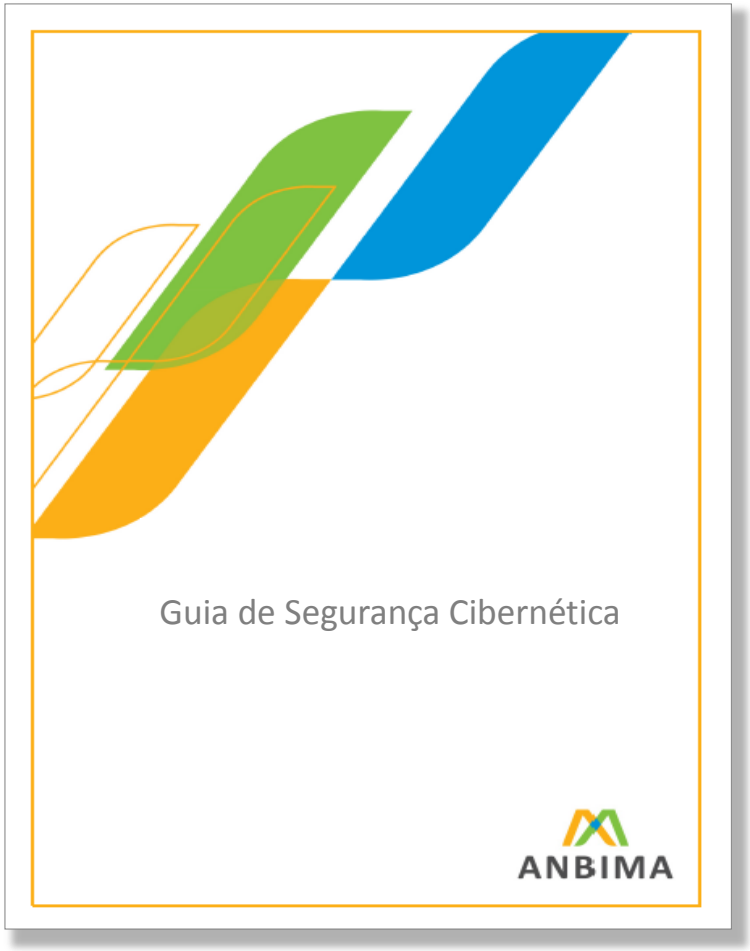
**PONTOS RELEVANTES [1]**

- Leva 1 ano para passar de um nível para outro, salvo casos de esforços extraordinários
- Um dos grandes obstáculos ainda é a questão cultural
- Comprometimento dos executivos seniores, das linhas de negócios e outros stakeholders é um fator crítico para aumentar a maturidade

1. **Gartner** (February 2016) – ITScore for Information Security

# Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos




- OBJETIVOS DESTE GUIA
- RISCO CIBERNÉTICO
- COMO COMEÇAR
- SEGURANÇA CIBERNÉTICA

PROGRAMA

- GOVERNANÇA CORPORATIVA
- CONTROLE DOS USUÁRIOS
- CONTROLES TECNOLÓGICOS
- PLANO DE RESPOSTA A INCIDENTES
- PROCESSO DE INVESTIGAÇÃO
- DIÁLOGO COM PARTES EXTERNAS
- PREVENÇÃO DOS ATAQUES INTERNOS

- DIVULGAÇÃO
- TRATATIVAS

# Melhores Práticas de Segurança Cibernética

## Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos

### Risco Cibernético

Resultados negativos potenciais de um ataque cibernético-tentativas de comprometer a confidencialidade, intergridade e disponibilitidade de dados ou sistemas.

### Segurança Cibernética

Conceito amplo que embarca todas as atividades para mitigação do risco cibernético, sendo a identificação, proteção, detecção, resposta e recuperação de um ataque cibernético.

### Avaliação do Risco

Programa baseado em necessidades, elaborando e mantendo um **risk assessment** atualizado que deve ser compatível com as características e tamanho da instituição e os recursos de defesa e respostas, proporcionais aos riscos identificados.

#### MOTIVAÇÕES

- Ganho financeiro
- Roubo de informações
- Vantagem competitiva
- Fraudes
- Exposição de fragilidade
- Terrorismo e pânico

#### PILARES

- Identificação
- Prevenção
- Detecção
- Proteção
- Tratativas
- Reciclagem

#### CHECK-LIST

- Identificação dos ativos e riscos
- Mensuração dos riscos
- Segurança dos dados
- Processos
- Contingência
- Qualificação dos profissionais
- Identificação de ameaças
- Vulnerabilidades
- Impactos

ANBIMA

# Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos

## Governança Corporativa

- Definição das responsabilidades
- Criação de um comitê
- Realização de auditoria
- Plano de continuidade de negócios
- Classificação das informações mais sensíveis
- Definição do ciclo de vida das informações

## Controle de Usuário

- Políticas de controles de acesso para trabalhos fora do escritório
- Troca periódica de senhas
- Definição do perfil de acesso dos Colaboradores e administradores de rede
- Definição do perfil de acesso dos prestadores de serviços,
- Gerenciamento e controle dos acessos privilegiados
- Treinamento
- Canais de comunicação e divulgação das políticas e procedimentos internos

## Controles Tecnológicos

- Proteção dos dados
- Rastreamento das informações nas nuvem
- Inventários dos hardwares e softwares
- Atualização dos sistemas
- Prevenção de ameaças com firewalls, antivírus
- Detecção de ameaças
- Inclusão das preocupações de segurança no desenvolvimento
- Controles de auditoria
- Utilização de dados fictícios em ambientes não produtivos
- Segregação dos ambientes de desenvolvimento, teste e produção
- Mesmo nível de segurança e proteção às aplicações que se utilizem de informações críticas

## Controle Físico

- Perfis de acesso às instalações do escritório
- Gerenciamento e controle dos acessos
- Espaço físico adequado e seguro para a guarda dos equipamentos
- Restrição de acesso físico das áreas com informações críticas/sensíveis
- Segurança e controles de acesso nas instalações de contingência
- Acesso remoto por usuários devidamente identificados e autenticados
- Uso exclusivo de equipamentos homologados

ANBIMA

# Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos

## Resposta Incidentes

- Critérios para classificação
- Lista de ativos críticos
- Procedimentos de detecção e investigação
- Plano de acionamento dos Colaboradores-chaves e contatos externos relevantes
- Tomada de decisões e ações técnicas de acordo com vários cenários possíveis de ataques
- Plano de comunicação
- Medidas de remediação; e
- Plano de continuidade dos negócios.

## Investigação

As investigações de cibersegurança incluem a coleta, a análise e a preservação de dados (conforme aplicável) com o objetivo de identificar a origem e as características de uma invasão/ataque cibernético. Para êxito nas investigações, é recomendável definir o protocolo que direcione a análise com a interrupção ou não do ataque e utilizar técnicas forenses que suportem a preservação das provas em caso de requerimentos legais.

É recomendável manter o histórico das análises com o objetivo de obter indicadores que permitam identificar, de forma preditiva, tendências e comportamentos.

## Diálogo Externo

Fornecedores, prestadores de serviços e parceiros (“Partes Externas”) podem representar uma fonte significativa de riscos para as instituições.

Recomenda-se que as instituições discutam com as Partes Externas os controles estabelecidos por eles a respeito da cibersegurança antes de celebrar um contrato de prestação de serviços e durante sua execução. Em geral, o nível de diligência desejável depende do risco que a relação com o fornecedor pode criar para a instituição.

## Ataques Internos

Boas práticas na prevenção dos ataques internos juntam ferramentas tecnológicas (por exemplo, de monitoramento das redes) com o conhecimento interno dos fatores humanos das instituições. Alguns indicadores podem revelar comportamentos duvidosos (fracassos repetidos no login, downloads massivos de dados etc., mas, também, conflitos entre Colaboradores ou ameaças).

# Estudo de Caso:
# Ataque ao Banco Central de Bangladesh

ANBIMA

ANBIMA

## O ATAQUE CIBERNÉTICO

Em fevereiro de 2016 hackers desviaram cerca de **USD 81 milhões** da conta do Banco Central de Bangladesh mantida no Federal Reserve de Nova York em um dos maiores assaltos cibernéticos da atualidade.

- 35 mensagens fraudulentas enviadas através do sistema de mensageria "SWIFT";
- Mensagens continham credenciais necessárias para autenticação (obtidas através de softwares "keylogger");
- Ataque ocorreu na véspera do fim de semana de Bangladesh (quinta);
- Ausência de firewall
- Terminal SWIFT conectado a plataforma de pagamentos do banco comercial expôs servidor a vários ataques *(phishing, trojans, etc);*
- Mallware instalado no terminal SWIFT inibiu a impressão das mensagerias do FED questionando a validade das ordens;
- Transferências fragmentadas (diversos destinos e pessoas).

## SEGURANÇA CIBERNÉTICA FRÁGIL E AMBIENTE PROPÍCIO

Ataque parcialmente bem sucedido devido à:

- Vulnerabilidades tecnológicas básicas (firewall, servidor, e-mails, sistema de pagamentos);
- Conhecimento da infraestrutura (sistemas, senhas, rotinas e procedimentos);
- Diferenças culturais (fim de semana dos EUA é diferente de Bangladesh);
- Pouca colaboração entre as jurisdições e partes envolvidas, reatividade;
- Remessas enviadas para jurisdições com regulamentação de prevenção à lavagem relativamente fracas (Filipinas e Sri Lanka);
- Uso de empresas de remessa de dinheiro, casinos, empresas de aposta online e pessoas físicas "laranjas";
- Fragilidade no processo de abertura de conta (KYC) e falsificação de documentos.

## SEGURANÇA CIBERNÉTICA E COMPLIANCE

Apenas 04 das 35 mensagerias fraudulentas foram processadas. 31 ataques foram inibidos pelos bancos intermediários por suspeita de lavagem de dinheiro. Funcionários bem treinados no FED de Nova York, Sri Lanka e Deutsche Bank identificaram comportamentos suspeitos e sistema de monitoramento alertou uma movimentação atípica durante os ataques:

- Alto volume de recursos para beneficiários de perfil improvável (contas "private bank", pessoas físicas, ONGs e instituições financeiras nas Filipinas e Sri Lanka);

- Erro de digitação no nome de um dos beneficiários levou analista do Deutsche Bank bloquear e questionar a transferência para uma ONG recém constituída;

- Falta de informações devido a impossibilidade de se comunicar com Bangladesh;

- Apesar da aparente legitimidade, ausência de fundamento econômico para efetivar as transferências levaram o FED a suspender os pagamentos;

## SEGURANÇA CIBERNÉTICA E COMPLIANCE

### O que aprendemos com este episódio?

- Criminosos sofisticados podem detectar e explorar as fraquezas existentes em países com fraca regulamentação e baixo investimento em infraestrutura;
  - México, Camboja e Índia são países que não obrigam cassinos a reportar atividades suspeitas;
  - Filipinas não permite que autoridades obriguem cassinos a colaborar com investigações;
  - Modernidade e agilidade tecnológica de cada país pode garantir anonimato e celeridade dos ataques (empresas de remessa);

Bancos intermediários com seu programa de monitoramento e prevenção à lavagem de dinheiro evitaram uma perda de quase **U$D 1 bilhão.**

Caso Bangladesh demonstra que a ausência de itens de segurança cibernética básica alinhada ao conhecimento e *timing* perfeito expõem o banco a perdas relevantes e muitas vezes irrecuperáveis.

## SEGURANÇA CIBERNÉTICA E COMPLIANCE

### O que aprendemos com este episódio?

O Programa de Segurança Cibernética e de Compliance aliado ao sistemas de monitoramento, analistas bem treinados e ativamente analisando tendências e alertas podem mitigar e evitar ataques uma vez que o hacker ganha acesso aos sistemas do banco.

***Rio de Janeiro***
*Av. República do Chile, 230  13º andar*
*20031-170  Rio de Janeiro  RJ  Brasil*
*+ 55 21 3814 3800*

***São Paulo***
*Av. das Nações Unidas, 8.501  21º andar*
*05425-070  São Paulo  SP  Brasil*
*+ 55 11 3471 4200*

ANBIMA