Supervisão de Segurança Cibernética

Fernando Abreu | Analista Técnico CGCON

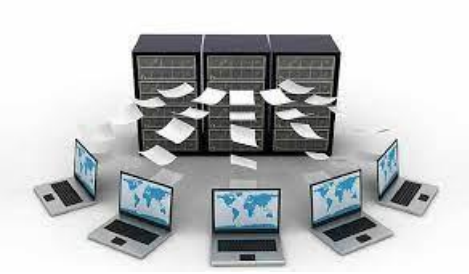
SUSEP
Superintendência
de Seguros Privados

Transformação Digital e Pandemia

Transformação Digital

Impulsionadores:

- Novas tecnologias (ex.: Inteligência Artificial, Blockchain, 5G, IoT, etc.)
- Pressão de concorrentes e consumidores
- Novas necessidades (ex.: pandemia COVID-19)
- Ambiente regulatório



SRO

Sandbox

Open Insurance

Pesquisa Segurança Cibernética

Objetivo

- Avaliar a estrutura de gestão de riscos das empresas pertencentes ao mercado supervisionado, bem como permiti-las uma reflexão para se tornarem mais resistentes a ataques cibernéticos, garantindo que os consumidores sejam protegidos e a integridade do mercado seja mantida.

Referência

- O questionário aplicado ao mercado foi uma adaptação do formulário elaborado pelos reguladores do Reino Unido, Financial Conduct Authority e Prudential Regulation Authority, com base nas recomendações do BIS e da IOSCO.

SUSEP

Pesquisa Segurança Cibernética

Da análise das respostas submetidas pelas companhias, conclui-se que:

- Grande parte do mercado supervisionado (74%) não sofreu ataques cibernéticos durante a pandemia;
- As supervisionadas que sofreram ataques informam não terem sofrido qualquer tipo de perda;
- Grande parte do mercado supervisionado respondeu que estão em linha com as boas práticas de resiliência cibernética (em 56 questões, 75% das vezes a supervisionada marcou a opção que seria “Muito bom” ou “bom”;
- As supervisionadas “S1” atingiram pontuações mais altas, em linhas gerais, que as supervisionadas “S2” e as “S2” pontuações mais altas que as “S3”;
- As companhias “Resseguradoras” atingiram pontuações mais altas, seguidas pelas companhias “Seguradora”, “Capitalização” e “EAPC”, respectivamente; e
- A seção com o menor número de respostas “Muito bom” é a Resposta e Recuperação, o que pode significar que elas não estejam tão preparadas no caso de um ataque cibernético bem-sucedido.

SUSEP

SARC – Risco Operacional

Risco Cibernético:

- Trata-se de risco incorrido pela supervisionada no processamento informatizado de seus produtos e serviços que pode impactar a segurança das informações e dos dados, comprometendo algum de seus atributos, em especial, a confidencialidade, a integridade e a disponibilidade.

Relacionamento com outras partes:

- Avaliar o risco de perdas decorrente da interação com prestadores de serviços, especialmente aqueles que prestem serviços relevantes de processamento, armazenamento de dados e computação em nuvem.

Interrupção do negócio ou falha de sistemas:

- Trata-se de risco de perdas decorrentes da interrupção do negócio ou de falha no processamento informatizado de seus produtos e serviços. Essas falhas podem envolver pessoas, recursos e processos da supervisionada ou prestadores de serviços empregados na operação da supervisionada.

SUSEP

SARC – Gestão do Risco Operacional

Governança de TI e de segurança da informação:

- Neste item procura-se avaliar os processos de TI, com a verificação da adequação de suas capacidades às necessidades operacionais e de negócio da supervisionada.

Controle da integridade da informação:

- Avaliam-se os controles destinados a mitigar os riscos incorridos pela supervisionada no processamento e manuseio de dados que podem impactar a integridade da informação utilizada na operação de seus processos de negócio ou providos para outras entidades ou partes relacionadas.

SUSEP

A regulação da Susep

SCI/EGR como Plano de Fundo

Res. CNSP nº 416/21

- SCI/EGR
- Política de Gestão de Riscos
- Plano de Continuidade de Negócios (PCN)

Circ. Susep nº 638/21

- Política de Segurança Cibernética
- Terceirização
- Prevenção e tratamento de incidentes

Circ. 638/21 - Segurança Cibernética

- Política de Segurança Cibernética
- Prevenção e tratamento de incidentes
- Terceirização de serviços de processamento e armazenamento de dados

SUSEP

Circ. 638/21 - Segurança Cibernética

- Política de Segurança Cibernética
- Prevenção e tratamento de incidentes
- Terceirização de serviços de processamento e armazenamento de dados

- Diretrizes para:
  - Classificação de dados, incidentes e serviços quanto a sua relevância
  - Implementação de processos, procedimentos e controles de segurança cibernética
  - Terceirização de serviços de processamento e armazenamento de dados

SUSEP

Circ. 638/21 - Segurança Cibernética

- Política de Segurança Cibernética
- Prevenção e tratamento de incidentes
- Terceirização de serviços de processamento e armazenamento de dados

- Identificação e redução proativa de vulnerabilidades
- Resposta a incidentes
- Incidentes relevantes:
  - Compartilhamento de informações
  - Comunicação à Susep
- Relatório anual

SUSEP

Circ. 638/21 - Segurança Cibernética

- Política de Segurança Cibernética
- Prevenção e tratamento de incidentes
- Terceirização de serviços de processamento e armazenamento de dados
  - Capacidade para administrar o contrato
  - Requisitos para prestação do serviço
  - Serviços relevantes:
    - Notificação à Susep
    - Segurança não inferior à da própria supervisionada (certificação ou due diligence)
    - Estratégia para execução própria ou para substituição do prestador
  - Acesso da Susep aos dados e a informações sobre a prestação do serviço

SUSEP

O questionário de aderência à Circular 638

O Questionário

06	Apresentação
20	Aderência
08	Melhores Práticas
34 Perguntas	

OBRIGADO!

SUSEP

youtube.com/suseptv @susepgovbr susep www.gov.br/susep