Patrocínio

STROHL Brasil

1st securityfirst

MINDSEC
SEGURANÇA E TECNOLOGIA
WWW.MINDSEC.COM.BR

WEBINAR
Resolução 4658
BACEN

Realização

MINUTO DA SEGURANÇA
O SEU BLOG DE SI

Junho / 2018

Resolução 4658

WEBINAR

Palestrantes

Fernando Correia

19 anos de experiência nas áreas de Tecnologia, Segurança da Informação, Continuidade de Negócios, Controles Internos, Compliance, Auditoria Interna e Auditoria Externa em empresas do mercado financeiro como Bancos, Consultorias (BIG4), Adquirentes, Central de Custódia e de Liquidação Financeira de Títulos. Professor de cursos de pós-graduação e instrutor de treinamentos para as certificações em auditoria de sistemas, gestão de riscos, continuidade de negócios, segurança da informação e cybersecurity. CEH, CISM, CISA, CBCI, CIA, CRISC, Graduação em Processamento de Dados e pós graduações em Segurança da Informação (IPEN/USP), Gerenciamento de Projetos (FIA/USP) e Cyber Security (DARYUS).

fernando.correa@securityfirst.com.br

Kleber Melo

CISSP, ISO27001 Lead Aduitor, Mestre em Engenharia pelo Mackenzie, possui mais de 27 anos dedicados a Segurança da Informação liderando times regionais em empresas multinacionais. Membro do LAAC – Latin América Advisory Council Board do ISC2, é Sócio Diretor & Consultor da MindSec Segurança e Tecnologia da Informação, Expert Partner Drivelock no Brasil. Grande experiência em gestão de riscos de segurança, proteção a informação, gestão e controles de acessos e privilégios em ambientes heterogêneos de pequenas, médias e grandes empresas.

kleber.melo@mindsec.com.br

Sidney Modenesi

Profissional em continuidade de negócios, resiliência organizacional e DRP. Bacharel em Ciências da Computação pela USP, pós graduado em Empreendedorismo, certificado MBCI pelo BCI, ISO 22301 Technical Expert pelo BSI, LDRM pelo PECB. 20 anos de experiência em Continuidade de Negócios, 30 em DRP e 40 em TIC.

sidney_modenesi@strohlbrasil.com.br

WEBINAR

Resolução 4658

- Guia ANBIMA de Cibersegurança v1 em 08/2016 e v2 em12/2017

- BACEN EDITAL DE CONSULTA PÚBLICA 57/2017, DE 19 DE SETEMBRO DE 2017

- BACEN 26/ABRIL/2018 - Resolução 4.658 que "*Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem*" , com ***datas previstas para final de Outubro 2018, Maio de 2019 e Dezembro de 2021***.

Objetivo da resolução:

I - POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sessão I - Implementação da Política de Segurança Cibernética
Sessão II - Divulgação da Política de Segurança Cibernética
Sessão III - Plano de Ação e de Resposta a Incidentes

II - CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Implementação da Política de Segurança Cibernética;

- ✓ Assegurar a confidencialidade, a integridade e a disponibilidade;
- ✓ Porte, Perfil e Complexidade;
- ✓ Se admite política única por conglomerado prudencial e sistema cooperativo de crédito;
- ✓ Aprovação em reunião do conselho de administração ou *Diretoria;
- ✓ Objetivos, procedimentos e controles incluindo controles específicos;
- ✓ Gestão de incidentes relevantes em cibersegurança;
  - ✓ Registro, classificação, causa raiz, impactos;
- ✓ Elaboração de cenários de incidentes; (NIST)
- ✓ Classificação de dados;
- ✓ Disseminação da Cultura;
- ✓ Capacitação e avaliação periódica do pessoal; (CISSP)
- ✓ Aculturamento do cliente;
- ✓ Comprometimento da alta administração;
- ✓ Melhoria contínua;
- ✓ Capacidade da instituição para prevenir, detectar e reduzir;

Implementação da Política de Segurança Cibernética (continuação);

Procedimentos mínimos:

- Autenticação;
- Criptografia;
- Prevenção e a detecção de intrusão;
- Prevenção de vazamento de informações;
- Testes e varreduras para detecção de vulnerabilidades periódicos;
- proteção contra softwares maliciosos;
- Rastreabilidade;
- Controles de acesso e de segmentação da rede;
- Backup de dados e informações.

Aplicação dos controles no processo de desenvolvimento de sistemas;

Divulgação da Política de Segurança Cibernética;

Plano de Ação e de Resposta a Incidentes.

- Adequação das estruturas organizacional e operacional;
- Rotinas, procedimentos, os controles e as tecnologias utilizados;
- Papéis e responsabilidades (Diretor responsável e níveis operacionais);
- Devem elaborar relatório anual, até 31 de dezembro contendo:
  - Efetividade da implementação das ações;
  - Resumo dos resultados obtidos;
  - Incidentes relevantes;
  - *Resultados dos testes de continuidade;
  - Deve ser submetido ao comitê de riscos e apresentado ao conselho de administração ou diretoria;

Politica e plano devem ser aprovados pelo conselho de administração ou *Diretoria, documentados e revisados anualmente;

Art. 13

1. Processamento, Armazenamento ou Infraestrutura
2. Aplicativos utilizando recursos de terceiros
3. Uso de aplicativos de internet de terceiros, usando recursos de terceiros

Art. 14 ,15 e 16

1. A instituição é responsável pelos serviços, quanto a confidencialidade, integridade, disponibilidade, segurança e sigilo.
2. A instituição é responsável pelo cumprimento das leis vigentes
3. Deve ser comunicado ao Bacen 60 dias antes da Contratação
    a. Informar empresa
    b. Informar serviços relevantes a serem contratados
    c. Local/País de “hosting” e processamento
    d. Alterações contratuais
4. Deve garantir atuação do Bacen e haver convênio entre os países
5. Seguir regulamentação de todos os países envolvidos
6. Prever a Continuidade de Negócios
7. Garantir transmissão segura dos dados
8. Comunicação de subcontratação (quarteirização)
9. Condições especificas sobre encerramento dos serviços

Resolução 4658

WEBINAR

Requerimentos p/ Nuvem

1. Data para plano de ação: 26/Out/2018 e Dez/2021
2. Políticas de Risco e Segurança devem ser ajustadas
3. Devem definir:
    1. Governança e gestão sobre os serviços
    2. Capacidade do provedor em atender aos serviços
    3. Cumprimento da legislação
    4. Acesso da instituição aos dados processados (serviço SW contratado)
    5. Confidencialidade, Integridade, Disponibilidade e Recuperação de dados
    6. Certificações exigidas pela instituição
    7. Acesso a resultados de auditorias externas feitas no terceiro relativos a procedimentos e controles)
    8. Informações de monitoramento dos serviços
    9. Segregação de dados , lógico e físico, de outras instituições
    10. Qualidade na proteção dos dados e informações
    11. A instituição deve avaliar relevância do serviço e classificação da Informação
    12. Avaliar relevância do serviço e confidencialidade da Informação
4. Controle e mitigação de vulnerabilidades do aplicativo
5. Recursos e Competência necessários do terceiro para manter o serviço contratado

- Está inserida no escopo da Resolução;
- Art. 3º, parágrafo V, alínea a) a elaboração de cenários de incidentes considerados nos testes de **continuidade de negócios**;
- Art. 8º, inciso § 1º, parágrafo IV, os resultados dos testes de **continuidade de negócios**, considerando cenários de indisponibilidade ocasionada por incidentes;
- Art. 16, parágrafo IV, a instituição contratante deve prever alternativas para a **continuidade dos negócios**, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.
- Art. 19, As instituições referidas no art. 1º devem assegurar que suas políticas para gerenciamento de riscos previstas na regulamentação em vigor disponham, no tocante **à continuidade de negócios**, sobre: ...
    - III - os cenários de incidentes considerados nos testes de **continuidade de negócios** de que trata o art. 3º, inciso V, alínea "a".
- Art. 20. Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à **continuidade de negócios**: ...

Continuidade de Negócios

- Os fundamentos da Continuidade de Negócios se aplicam à Resolução:
  - Análise de Riscos ➔ identificar e desenvolver as contingências para mitigar os riscos de segurança cibernética ou de computação em nuvem;
  - Análise de Impacto nos Negócios ➔ quantificar os impactos decorrentes de um incidente de interrupção de segurança cibernética ou de computação em nuvem:
    - Múltiplos cenários;
    - Quantificar MTPDs, MBCOs, RTOs e RPOs;
  - Estratégias de Recuperação x Apetite a Risco da organização
    - Modelos tradicionais de **Continuidade de Negócios** podem não se aplicar a incidentes de interrupção de segurança cibernética;
  - Desenvolver os planos (ou procedimentos) de recuperação e de continuidade de negócios;
  - Divulgar, exercitar e testar;
  - Melhoria Contínua

Obrigado !!!

Perguntas

&

Respostas

OBRIGADO !

A gravação será disponibilizada no Blog
minutodaseguranca.blog.br

Patrocínio

STROHL Brasil

1ST securityfirst

MINDSEC
SEGURANÇA E TECNOLOGIA
WWW.MINDSEC.COM.BR

Realização

MINUTO DA SEGURANÇA
O SEU BLOG DE SI