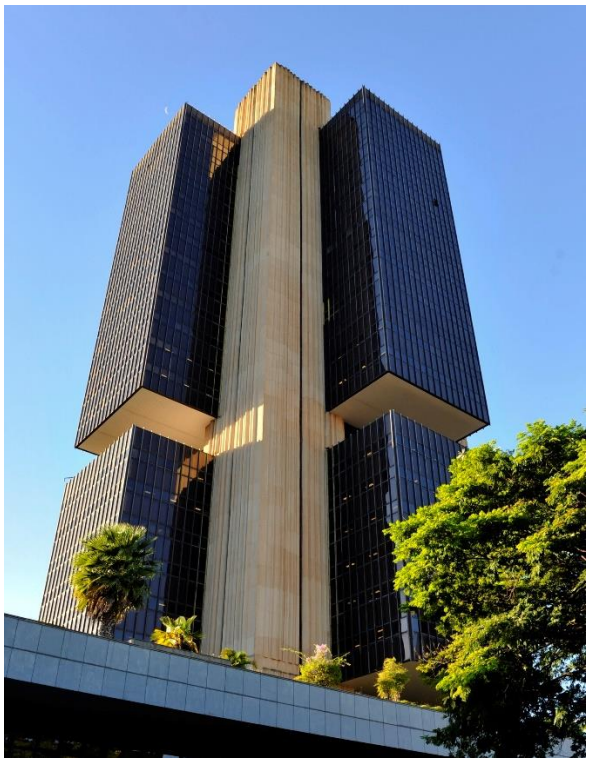


Foto: Jonas Pereira/Agência Senado Licença CC BY

POLÍTICA SEGURANÇA CIBERNÉTICA

COMPUTAÇÃO EM NUVEM

Resolução Banco Central do Brasil 4658:2018

Considerações Edison Fontes

Prof. Ms. Edison Fontes, CISM, CISA, CRISC

Controles de segurança da informação exigidos pela Resolução do Banco Central do Brasil 4658 de 26-04-2018: política de segurança cibernética e computação em nuvem

DOC ELGF.0102.01.0

São Paulo, maio, 2018 - Brasil

Licença para uso deste documento

Este documento

Este documento descreve a interpretação do autor para os principais controles de segurança da informação relacionados à política de segurança cibernética e à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, exigidos para as instituições que estão sob a regulamentação do Banco Central do Brasil (Resolução BC 4658:2018).

Este documento não é suficiente para a implementação dos controles da Resolução BC 4658 de 26 de abril de 2018. Para a implementação desta resolução o leitor deve ler por completo a mesma, os demais normativos do Banco Central, as estruturas de arquitetura da segurança da informação, ter experiência em Processo Organizacional de Segurança da Informação, avaliar a maturidade da organização em segurança da informação e elaborar um plano de ação aprovado pelo Corpo Diretivo.

Técnica e muito cuidado foram utilizados na elaboração deste documento. Porém erros podem acontecer, tipo digitação ou reprodução. Qualquer erro encontrado, qualquer dúvida de interpretação, solicitamos que seja enviada uma mensagem para edison@pobox.com para a devida verificação e resposta. O autor não assume qualquer responsabilidade por eventuais danos ou perdas a pessoas, organizações ou bens originados do uso deste documento.

Este documento é conceitual e didático sobre os temas apresentados.

O Autor

Edison Fontes é Mestre em Tecnologia, certificado internacional CISA, CISM, CRISC e profissional de segurança da informação. É professor de MBAs, autor de livros e desenvolve atividades de Estrategista, Gestor, Consultor em Segurança Informação, Continuidade de Negócio, Risco Operacional, Conformidade *(Compliance)* da Informação e Combate à Fraude de Informação.

É sócio consultor da Núcleo Consultoria em Segurança

Contato: edison@pobox.com, ef@nucleoconsult.com.br

Livros do Autor

- Segurança da informação: Orientações práticas, Publicação Amazon
- Políticas e Normas para a Segurança da Informação, Editora Brasport.
- Praticando a segurança da informação, Editora Brasport.
- Clicando com segurança, Editora Brasport.
- Segurança da informação: o usuário faz a diferença, Editora Saraiva.
- Vivendo a segurança da informação, Editora Sicurezza.

Documentos do Autor

- Políticas de Segurança da Informação: uma contribuição para o estabelecimento de um padrão mínimo, Dissertação de Mestrado, Centro Paula Souza, Governo Estado de São Paulo.
- GDPR – General Data Protection Regulation – Considerações Edison Fontes. DOC ELGF.0101.02.0

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018

A Resolução do Banco Central do Brasil No. 4.658 de 26 de abril de 2018, 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 a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

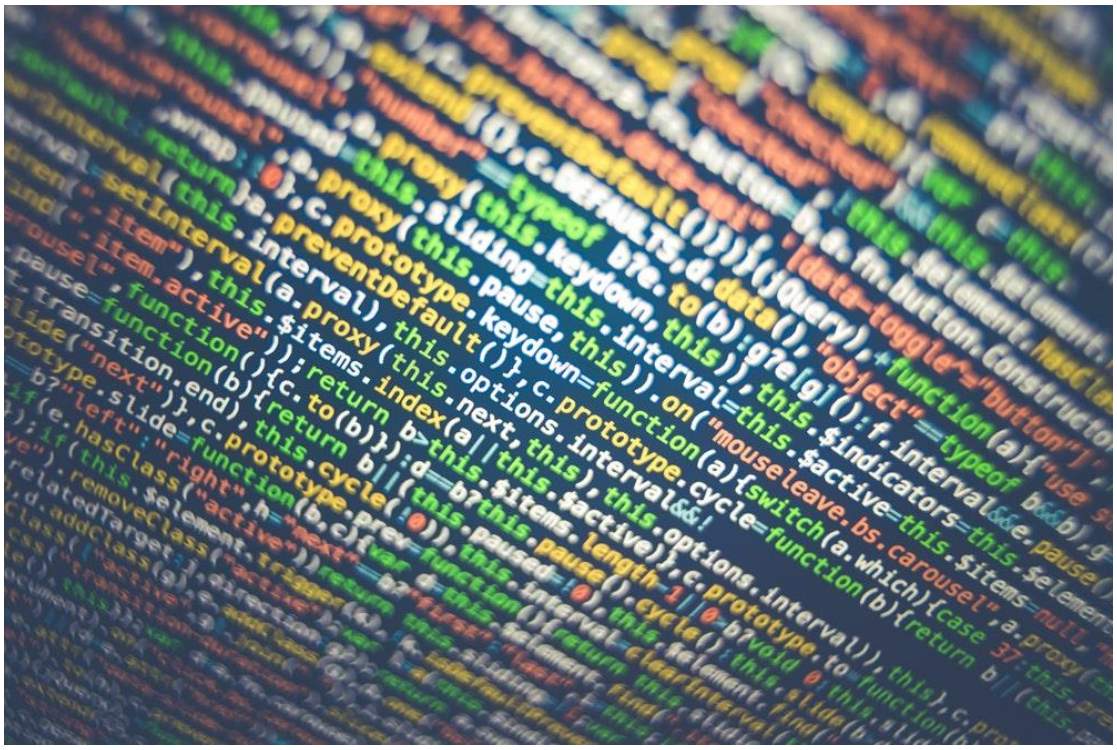


Foto: unsplash.com, sem reservas

INTRODUÇÃO

Após uma consulta pública que terminou em novembro de 2017, o Banco Central do Brasil divulgou a Resolução 4658 em 26 de abril de 2018. Foram poucas as alterações para o texto final em vigor.

Esta resolução afeta as instituições financeiras e as demais instituições autorizadas a funcionar. Porém, afeta outras organizações como citado no artigo 3º, V.b:

> *Empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.*

A Resolução BC 4658:2018, tem claramente os seguintes direcionadores:

Foto: unsplash.com, sem reservas

a. Existência de regulamentos aprovados pela direção ou conselho.

b. Existência de controles para a implementação dos regulamentos.

c. Obrigatoriedade de implementação de específicas boas práticas.

d. Responsabilização de gestor em nível de diretoria.

e. Gestão de incidentes com aprovação pela direção ou conselho.

f. Continuidade do negócio.

g. Contratação de serviços de computação em nuvem.

Os controles de segurança da informação considerados na Resolução BC 4658:2018, sejam como diretrizes ou sejam como regras detalhadas, estão baseados em diversos normativos e em regras específicas do Banco Central.

Como normativos, podemos destacar os que estão diretamente conectados com os controles da resolução do BC:

Foto: unsplash.com, sem reservas

Norma NBR ISO 22301:2013 – Segurança da sociedade – Sistemas de Gestão de continuidade de negócio – Requisitos.

Norma NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos.

Norma NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

Norma NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

Norma NBR ISO/IEC 27014:2013 – Tecnologia da Informação – Técnicas de segurança – Governança de segurança da informação.

Norma NBR ISO/IEC 27017:2016 – Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação para serviços em nuvem.

A Resolução BC 4658:2018 considerou as orientações destes e outros normativos, porém para alguns deles concretizou em controles bem específicos. Exemplo: "...tem que ser aprovado pelo Conselho de Administração, e na falta dele pela Diretoria da Instituição."

Entendo que as instituições que possuem um Processo Organizacional de Segurança da Informação, terão mais facilidade para implementar o detalhamento dos controles exigidos pelo Banco Central. Elas já possuem a estrutura, a arquitetura para os controles de proteção da informação.

DIRETRIZES E CONTROLES

Relaciono a seguir as diretrizes e os principais controles da resolução. O objetivo deste item é transmitir para o leitor, de uma forma simples, o que contempla esta resolução. Agrupei em tópicos para atender a este objetivo.

1. Controles Básicos (art. 2º, 3º, 9º.)

São exigidos alguns controles básicos de segurança da informação:

a. Política de Segurança Cibernética e Plano de Ação que precisam ser aprovados pelo Conselho de Administração ou Diretoria.

b. Confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados.

c. Controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados.

d. Controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis.

e. Classificação de dados ou de informações.

f. Diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes.

Foto: unsplash.com, sem reservas

2. Gestão de Incidentes (art. 3º)

A Gestão de Incidentes toma uma importância muito grande na resolução do BC. É exigido a existência e formalização dos seguintes controles relacionados à Gestão de Incidentes:

a. Identificação da causa e impactos dos incidentes.

b. Planos de ação e planos de resposta para incidentes.

c. Área específica para os registros de incidentes.

d. Plano de Continuidade de Negócio.

e. Relatório anual – Andamento plano de ação e resposta para incidentes.

f. Revisão anual pela direção ou conselho administração.

g. Tem que ser adotada por empresas prestadoras de serviços para a instituição, que manuseiem informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

Foto: unsplash.com, sem reservas

3. Cultura em segurança (art. 3º)

Um aspecto que a resolução exige é o tratamento para as pessoas que fazem a instituição ter vida. São obrigatórios os seguintes controles:

a. Implementação de programas de capacitação em segurança.

b. Comunicação para clientes e usuários.

c. Comprometimento da alta administração.

Foto: unsplash.com, sem reservas

Foto: unsplash.com, sem reservas

4. Controles Técnicos Mínimos (3º)

A resolução do BC descreve os controles técnicos mínimos que devem ser implementados. Ela não descreve o como implementar. Esta será uma responsabilidade dos profissionais de segurança da instituição que deverão implementar o melhor controle possível considerando a organização específica. Este fato também exige dos profissionais o entendimento de outros regulamentos. A resolução exige pelo menos os seguintes controles de tecnologia:

a. Autenticação.

b. Criptografia.

c. Prevenção e detecção de intrusão.

d. Prevenção de vazamento de informações.

e. Realização periódica de testes e varreduras.

f. Proteção contra software malicioso.

g. Mecanismos de rastreabilidade.

h. Segmentação de redes de computadores.

i. Cópias de segurança de informações.

j. Desenvolvimento de sistemas de informação seguros.

Foto: unsplash.com, sem reservas

5. Computação em Nuvem (art. 10º ao 17º)

A contratação de serviços de processamento e armazenamento de dados e computação na nuvem deve obrigatoriamente:

a. Ser considerado nas políticas, estratégias e estruturas para o gerenciamento de riscos.

b. Verificar a capacidade da empresa prestadora de serviço (competência, recursos) e aderência as exigências da instituição.

c. Cumprir a legislação em vigor.

d. Ter acesso da instituição aos relatórios de auditorias recebidas pelo prestador de serviço.

e. Monitorar os serviços prestados.

f. Garantir de controles físicos e lógicos pela empresa prestadora de serviço para a proteção dos dados dos clientes da instituição.

g. Avaliar a criticidade do serviço e a sensibilidade dos dados que serão processados e armazenados pelo prestador de serviço.

h. Possibilitar o processamento dos serviços da instituição de maneira adequada à necessidade da instituição.

i. Garantir que a instituição é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

j. Ser comunicada com sessenta dias de antecedência ao Banco Central do Brasil, indicando a empresa, os serviços, os países e regiões onde os dados serão processados e armazenados. Alterações contratuais também devem ser comunicadas.

k. A contratação dos serviços prestados no exterior deve ter como requisitos:
- existência de convênio BC com autoridades dos países,
- definição país e região onde os dados serão processados e armazenados,
- continuidade de negócio caso impossibilidade da prestação de serviço,
- autorização do BC caso não exista convênio com os países,

- legislação dos países permitam acesso das instituições e do BC,
- medidas para garantir a segurança da transmissão e armazenamento da informação.

l. Quando da extinção do contrato, obrigatoriedade de transferência de dados para o novo prestador de serviço de maneira a garantir a continuidade do serviço.

m. Diversos controles para garantir o efetivo cumprimento do contrato.

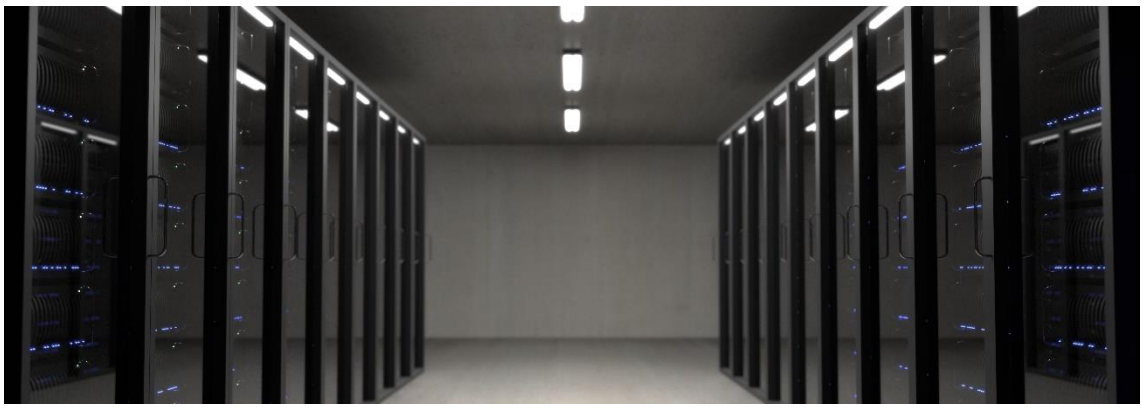
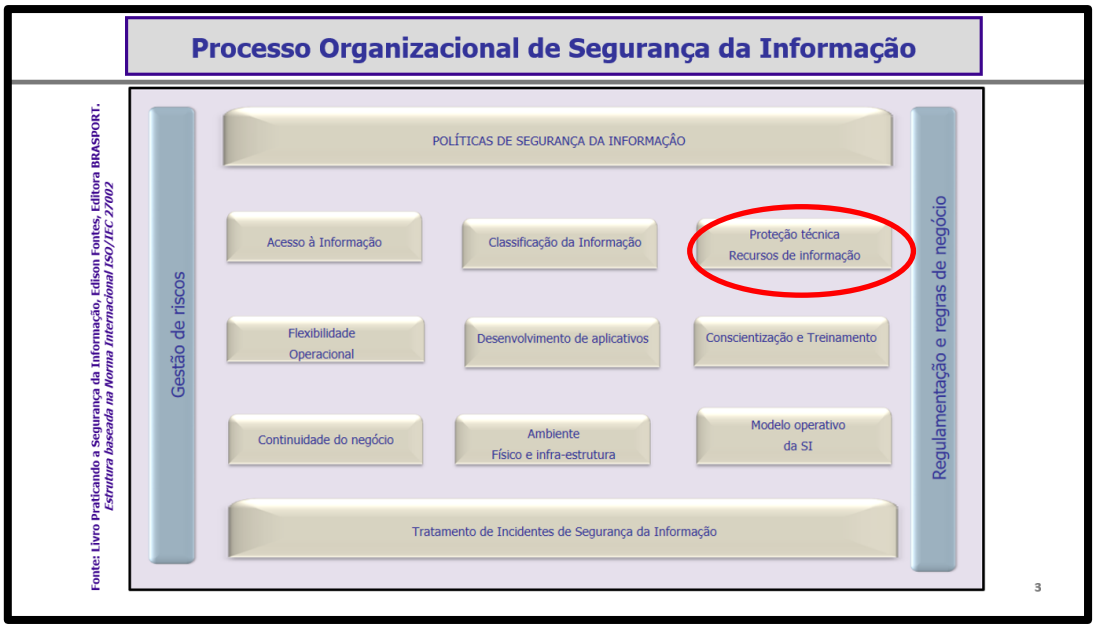


Foto: unsplash.com, sem reservas

CONCLUSÃO

O Processo Organizacional da Segurança da Informação, baseado nas Normas da Família 27000 e outras complementares facilita o atendimento aos requisitos da Resolução BC 4658:2018.



O Processo Organizacional de Segurança da Informação é a base para que a instituição tenha condições de cumprir os controles definidos pela Resolução BC 4658:2018 e outros regulamentos.

A Arquitetura da Segurança da Informação contempla a Segurança Cibernética!

Entendo que em médio prazo a grande maioria das organizações estarão obrigadas a seguir controles como esta resolução do BC. Seja porque a organização começou a prestar (direta ou indiretamente) serviços para instituições financeiras ou outros órgãos de controle emitiram resoluções similares ao BC. Uma questão é certa: cada vez mais os controles de segurança da informação serão mais rígidos e atingirão um maior número de tipos de organizações.

Foto: unsplash.com, sem reservas

Edison Fontes, CISM, CISA, CRISC
Sócio Núcleo Consultoria
Estrategista, Consultor e Gestor: Segurança da Informação, Riscos, Continuidade e Combate à Fraude, Compliance.
Coordenador do Comitê de Segurança da Informação da ABSEG.

edison@pobox.com
ef@nucleoconsult.com.br
www.nucleoconsult.com.br

++++++++++++++++++++++++++++++++ **Fim do Documento**++++++++++++++++++ **maio/2018.**