1 GESTÃO DE SEGURANÇA DA INFORMAÇÃO

1.1 Introdução

Quem nunca se perguntou sobre os conhecimentos que envolvem este universo de ataques e defesas em sistemas informatizados? Todo este tema surge com a denominada segurança da informação, mas o que significa isto?

A segurança da informação é um conceito amplo que considera a aplicação de medidas (controles), que visam a proteção de pessoas, processos e tecnologias em face às ameaças que podem vir a se concretizar em riscos significativos às pessoas e/ou empresas.

O resumo deste conceito consiste em criar e posicionar defesas que impeçam ou possibilite a concretização de danos, que em geral resultam em perda de credibilidade de vítimas, podendo causar ao limite destas consequências a falência de negócios e até mesmo a exposição de cidadãos à fatos ou eventos de forma irreversível.

Entender os princípios (pilares) da segurança da informação auxilia a compreender quais são às bases à qual este processo está estruturado, vamos partir para a próxima seção deste material para entender melhor sobre o que estamos tratando.

1.2 Pilares da Segurança da Informação

A segurança da informação por alguns autores (LAU, 2008), consideram como pilares em segurança da informação a confidencialidade, integridade e disponibilidade, conforme podemos identificar a definição destes termos a seguir:

A confidencialidade trata da disseminação da informação apenas àqueles que necessitam ou requerem acessá-la para seus propósitos. Considera-se confidencial algo que não deve ser de conhecimento público ou de conhecimento de outras pessoas senão aquelas envolvidas em um projeto ou em um assunto de interesse restrito (LAU, 2008).

Muitos leigos em segurança da informação, considera que a segurança da informação é apenas proteção da confidencialidade, mas isto não é verdade, pois não é só o que “vaza na Internet”, pode ser considerado único aspecto negativo possível atrelado à falta de segurança da informação.

A integridade trata na certeza de se ter o conteúdo exato dos dados a qualquer momento que de deseje. Considera-se íntegra uma informação que podemos confiar em função de refletir um conteúdo atualizado conforme nossas necessidades (LAU, 2008).

Pense neste caso que você tem uma conta bancária, mesmo que a mesma seja mantida confidencial, pode ser muito desagradável se você souber que por meio de uma ação fraudulenta, você deixou de ter metade de seus recursos financeiros em sua conta bancária de um dia para o outro.

A disponibilidade é a propriedade de algo ou alguma coisa ser ou estar acessível em um determinado momento para uma específica necessidade. Consideram-se disponíveis acessos, informações, serviços e demais considerações que tratem de se acessar algo ou alguém em um determinado período (LAU, 2008).

Como exemplo neste caso, considere que você precisa muito de uma informação via GPS para chegar em uma reunião, mas por algum motivo seu aparelho deixou de funcionar. Chamamos isto perda de disponibilidade, que

neste caso, pode vir a te impedir a chegar até seu destino, ou até mesmo fazer que você chegue atrasado em seu compromisso.

Visando facilitar a memorização destes pilares em sequência (Confidencialidade, Integridade e Disponibilidade), recomenda-se que o leitor memorize estes termos como C.I.D. (ou simplesmente CID), conforme ilustrado na imagem a seguir.

Figura 1 – Pilares da Segurança da Informação[1]

Apesar disto, no Brasil, a Administração Pública Federal, considera como pilares da segurança da informação a Disponibilidade, Integridade, Confidencialidade e Autenticidade (DSIC,2015), um acrônimo similar foi proposto para estes termos, denominado DICA. A Administração Pública Federal, ainda adota a denominação de outro acrônimo conhecido como SIC (Segurança da Informação e Comunicações), que está presente em diversos textos pertencentes e utilizados pelo Governo Federal brasileiro.

[1] Fonte: https://securitycommunity.tcs.com/infosecsoapbox/sites/default/files/styles/article_image_full_node/public/field/image/CIA%20Triad.jpg?itok=Z7_leMG6

Ainda de acordo com a Administração Pública Federal, são apresentados alguns desafios quanto à segurança da informação que são os seguintes (DSIC,2015):

- Redes Sociais;
- Computação em nuvem;
- Aumento exponencial da utilização de dispositivos móveis;
- Problemas tecnológicos;
- Aumento da demanda de informações pelos cidadãos;
- Convergência digital;
- Leis, regulamentações e normas não unificadas;
- Aumento exponencial de compartilhamento de informações;
- Redução do custo de aquisição de tecnologias de comunicação e processamento;
- Acesso a conexões de internet em banda larga;
- Fragilidade na identificação de usuário ao acesso à internet;
- Ampla disponibilidade de técnicas e ferramentas de ataque e invasão na rede e no mercado, aliado à facilidade de uso dessas ferramentas;
- Compartilhamento de informações e ferramentas de ataque e invasão entre grupos anônimos;
- Crescimento exponencial do crime virtual;
- Exaltação por práticas ilícitas com utilização de tecnologias de informação;
- Diversificação dos perfis de ameaça: concorrente, sabotador, especulador, hacker, servidores insatisfeitos e criminosos;
- Necessidade de tratar a informação como um recurso estratégico e econômico;

- Crescente valorização da informação como principal ativo de gestão do Estado;
- Crescentes transações bilaterais com suporte da tecnologia da informação e comunicações;
- Crescente dependência da gestão do Estado por recursos de tecnologia da informação e comunicações;
- Forte dependência tecnológica;
- Interdependência entre os ativos de informação;
- Aumento dos riscos associados aos ativos de informação;
- Processos de continuidade dos serviços públicos sem um grau de maturidade adequado;
- Desconhecimento das tecnologias embutidas nas arquiteturas proprietárias; e
- Alinhamento estratégico da SIC com as atribuições institucionais dos órgãos e entidades públicos.

Ainda de acordo com (LAU, 2008), ele menciona que apesar de definição clássica em segurança da informação, há outros pilares e conceitos em segurança da informação como o não-repúdio, entretanto ele lembra que a ética é um dos aspectos que não estão associados à informação e sim ao caráter pessoal. Algo que hoje pode ser considerando como um pilar em segurança da informação.

1.3 Normas e Padrões em Segurança da Informação (ISO / NIST / PCI)

As normas, padrões e boas práticas em segurança da informação são guias que auxiliam profissionais (dos menos experientes aos mais experientes) à avaliação, implementação e manutenção de boas práticas em segurança da informação, que em geral se resumem à controles (sejam estes baseados em processos ou tecnologias). Em ambos os casos, espera-se que tais controles venham a contribuir à melhoria e aprimoramento da segurança em empresas de pequeno, médio e grande porte possibilitando que estas estejam em aderência à padrões consagrados e conhecidos em segurança da informação.

Para isto, espera-se que estes controles sejam acompanhados de evidência, preferencialmente documentados, possibilitando a constatação de que as pessoas (sejam estes funcionários, prestadores de serviço e até mesmo clientes) estejam aderentes ao modelo de segurança adotado em âmbito corporativo.

Espera-se ainda que tais aspectos relacionados à segurança sejam sempre relembrados ao seu respectivo público afetado por estes controles, onde esperam-se que ações como campanhas de conscientização, venham a manter e melhorar da segurança da informação.

1.3.1 ISO 27001

A ABNT NBR ISO/IEC 27001:2013, segundo a ABNT é uma norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

Esta norma é utilizada por diversas empresas que estão em busca de conformidade em segurança da informação, com base que esta norma é a principal, dentre a família ISO 27000, onde se espera que ela seja parte integrante aos processos em uma organização, além de estar integrada aos sistemas de informação e respectivos controles em segurança da informação.

Esta norma pode ser aplicada às partes internas e externas de uma empresa, podendo caber aderência à mesma à clientes, parceiros, fornecedores, prestadores de serviço e demais outras partes interessadas, se esperando ainda que esta norma seja compatível com demais sistemas de gestão adotados pela empresa.

A estrutura desta norma nos remete à diversas seções compostas pelos seguintes itens:

- Escopo;
- Referências normativas;
- Termos e definições;
- Contexto da organização:
    - Entendendo a organização e seu contexto;
    - Entendendo as necessidades e as expectativas das partes interessadas;
    - Determinando o escopo do sistema de gestão da segurança da informação; e
    - Sistema de gestão da segurança da informação.
- Liderança:
    - Liderança e comprometimento;
    - Política; e
    - Autoridades, responsabilidades e papeis organizacionais.
- Planejamento:
    - Ações para contemplar riscos e oportunidades:
        - Geral;
        - Avaliação de riscos de segurança da informação; e
        - Tratamento de riscos de segurança da informação.
    - Objetivo de segurança da informação e planos para alcançá-los.

- Apoio:
    - Recursos;
    - Competência;
    - Conscientização; e
    - Comunicação.
    - Informação documentada:
        - Geral;
        - Criando e atualizando; e
        - Controle da informação documentada.
- Operação:
    - Planejamento operacional e controle;
    - Avaliação de riscos de segurança da informação; e
    - Tratamento de riscos de segurança da informação.
- Avaliação do desempenho:
    - Monitoramento, medição, análise e avaliação;
    - Auditoria interna; e
    - Análise crítica pela direção.
- Melhoria:
    - Não conformidade e ação corretiva; e
    - Melhoria contínua.

1.3.2 ISO 27002

A ABNT NBR ISO/IEC 27002:2013, segundo a ABNT é uma norma que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Os controles em segurança da informação consistem, segundo a ISO 27002:2013 em uma norma que traz um total de 114 controles, neste caso segregados em 14 seções e 35 objetivos de controle.

A relação de controles que esta norma sugere não pode ser considerado algo exaustivo, já que controles adicionais podem vir a ser propostos.

Ao se considerar a existência de tais controles, deve-se ter ciência que os mesmos somente devem ser adotados considerando a existência de riscos e ameaças que possam comprometer a segurança da informação, portanto a seleção dos controles deve estar diretamente associada à necessidade de controles, visando mudar o nível de risco de uma informação, preferencialmente com objetivo de se atotar o controle visando a redução deste risco.

A estruturação de seções, objetivos de controles e controles auxilia a uma melhor compreensão dos controles, onde a norma NBR ISO IEC 27002:2013 traz uma estrutura de seções de 5 a 18 (pois as seções anteriores são compostas respectivamente por: “introdução”, “escopo”, “referência normativa”, “termos e definições” e “estrutura desta norma”.

Começamos com a descrição da primeira seção da ISO 27002:2013 para melhor compreensão da seção 5:

- Seção 5 – Políticas de segurança da informação:
    - Objetivo de controle 5.1 – Política de segurança da informação.
        - Objetivo: prover orientação da Direção e apoio para a segurança da informação de acordo com os

requisitos do negócio e com as leis e regulamentações relevantes.

- Controle 5.1.1 – Políticas para segurança da informação.
  - Este controle consiste nas diretrizes para implementação da política de segurança, considerando que a mesma deve ser comunicada a todas as partes interessadas, sendo que se espera apoio de todos (inclusive da alta administração) para que ocorra o devido apoio a este instrumento normativo.
- Controle 5.1.2 – Análise crítica da política de segurança da informação.
  - Este controle consiste na análise crítica pela direção da organização a intervalos planejados ou quando mudanças significativas ocorrerem junto ao conjunto normativo de segurança da informação.

Nas demais seções serão apenas mencionadas as seções de forma mais resumida evitando alongar-se excessivamente sobre o conteúdo das mesmas, possibilitando uma visão abrangente em relação a este tema

- Seção 6 – Organização da segurança da informação:
  - Objetivo de controle 6.1 – Organização Interna.
    - Controle 6.1.1 – Responsabilidade e papéis pela segurança da informação.
    - Controle 6.1.2 – Segregação de funções.
    - Controle 6.1.3 – Contato com autoridades.
    - Controle 6.1.4 – Contato com grupos especiais.
    - Controle 6.1.5 – Segurança da informação no gerenciamento de projetos.
  - Objetivo de controle 6.2 – Dispositivos móveis e trabalho remoto.

        - Controle 6.2.1 – Política para uso de dispositivo móvel.
        - Controle 6.2.1 – Trabalho remoto.

- Seção 7 – Segurança em Recursos Humanos:
    - Objetivo de controle 7.1 – Antes da contratação.
        - Controle 7.1.1 – Seleção.
        - Controle 7.2.1 – Termos e condições de contratação.
    - Objetivo de controle 7.2 – Durante a contratação.
        - Controle 7.2.1 – Responsabilidade da direção.
        - Controle 7.2.2 – Conscientização, educação e treinamento em segurança da informação.
        - Controle 7.2.3 – Processo disciplinar.
    - Objetivo de controle 7.3 – Encerramento e mudança da contratação.
        - Controle 7.3.1 – Responsabilidades pelo encerramento ou mudança da contratação.
- Seção 8 – Gestão de ativos:
    - Objetivo de controle 8.1 – Responsabilidade pelos ativos.
        - Controle 8.1.1 – Inventário dos ativos.
        - Controle 8.1.2 – Proprietário dos ativos.
        - Controle 8.1.3 – Uso aceitável dos ativos.
        - Controle 8.1.4 – Devolução dos ativos.
    - Objetivo de controle 8.2 – Classificação das informações.
        - Controle 8.2.1 – Classificação da informação.
        - Controle 8.2.2 – Rótulos e tratamento da informação.
        - Controle 8.2.3 – Tratamento dos ativos.

    - Objetivo de controle 8.3 – Tratamento de mídias.
        - Controle 8.3.1 – Gerenciamento de mídias removíveis.
        - Controle 8.3.2 – Descarte de mídias.
        - Controle 8.3.3 – Transferência física de mídias.
- Seção 9 – Controle de acesso:
    - Objetivo de controle 9.1 – Requisitos do negócio para controle de acesso.
        - Controle 9.1.1 – Política de controle de acesso.
        - Controle 9.1.2 – Acesso às redes e aos serviços de rede.
    - Objetivo de controle 9.2 – Gerenciamento de acesso do usuário.
        - Controle 9.2.1 – Registro e cancelamento de usuário.
        - Controle 9.2.2 – Provisionamento para acesso de usuário.
        - Controle 9.2.3 – Gerenciamento de direitos de acesso privilegiados.
        - Controle 9.2.4 – Gerenciamento da informação de autenticação secreta de usuários.
        - Controle 9.2.5 – Análise crítica dos direitos de acesso de usuário.
        - Controle 9.2.6 – Retirada ou ajuste dos direitos de acesso.
    - Objetivo de controle 9.3 – Responsabilidade dos usuários.
        - Controle 9.3.1 – Uso da informação de autenticação secreta.

    - Objetivo de controle 9.4 – Controle de acesso ao sistema e à aplicação.
        - Controle 9.4.1 – Restrição de acesso à informação.
        - Controle 9.4.2 – Procedimentos seguros de entrada no sistema (*log-on*).
        - Controle 9.4.3 – Sistema de gerenciamento de senha.
        - Controle 9.4.4 – Uso de programas utilitários privilegiados.
        - Controle 9.4.5 – Controle de acesso lógico ao código-fonte de programas.
- Seção 10 – Criptografia:
    - Objetivo de controle 10.1 – Controles criptográficos.
        - Controle 10.1.1 – Política para o uso de controles criptográficos.
        - Controle 10.1.2 – Gerenciamento de chaves.
- Seção 11 – Segurança física e do ambiente:
    - Objetivo de controle 11.1 – Áreas Seguras.
        - Controle 11.1.1 – Perímetro de segurança física.
        - Controle 11.1.2 – Controle de entrada física.
        - Controle 11.1.3 – Segurança em escritórios, salas e instalações.
        - Controle 11.1.4 – Proteção contra ameaças externas e do meio ambiente.
        - Controle 11.1.5 – Trabalhando em áreas seguras.
        - Controle 11.1.6 – Áreas de entrega e de carregamento.
    - Objetivo de controle 11.2 – Equipamento.

        - Controle 11.2.1 – Localização e proteção do equipamento.
        - Controle 11.2.2 – Utilidades.
        - Controle 11.2.3 – Segurança do cabeamento.
        - Controle 11.2.4 – Manutenção dos equipamentos.
        - Controle 11.2.5 – Remoção dos ativos.
        - Controle 11.2.6 – Segurança de equipamentos e ativos fora das dependências da organização.
        - Controle 11.2.7 – Reutilização ou descarte seguro de equipamentos.
        - Controle 11.2.8 – Equipamento de usuário sem monitoração.
        - Controle 11.2.9 – Política de mesa limpa e tela limpa.
- Seção 12 – Segurança nas operações:
    - Objetivo de controle 12.1 – Responsabilidade e procedimentos operacionais.
        - Controle 12.1.1 – Documentação dos procedimentos de operação.
        - Controle 12.1.2 – Gestão de mudanças.
        - Controle 12.1.3 – Gestão de capacidade.
        - Controle 12.1.4 – Separação dos ambientes de desenvolvimento, teste e produção.
    - Objetivo de controle 12.2 – Proteção contra *malware*.
        - Controle 12.2.1 – Controles contra *malware*.
    - Objetivo de controle 12.3 – Cópias de segurança.
        - Controle 12.3.1 – Cópias de segurança das informações.

- Objetivo de controle 12.4 – Registros e monitoramento.
    - Controle 12.4.1 – Registros de eventos.
    - Controle 12.4.2 – Proteção das informações dos registros de eventos (*logs*).
    - Controle 12.4.3 – Registro de eventos (*log*) de administrador e o operador.
    - Controle 12.4.4 – Sincronização dos relógios.
- Objetivo de controle 12.5 – Controle de *software* operacional.
    - Controle 12.5.1 – Instalação de *software* nos sistemas operacionais.
- Objetivo de controle 12.6 – Gestão de vulnerabilidades técnicas.
    - Controle 12.6.1 – Gestão de vulnerabilidades técnicas.
    - Controle 12.6.2 – Restrições quanto à instalação de *software*.
- Objetivo de controle 12.7 – Considerações quanto à auditoria de sistemas da informação.
    - Controle 12.7.1 – Controle de auditoria de sistemas de informação.

- Seção 13 – Segurança nas comunicações:
    - Objetivo de controle 13.1 – Gerenciamento da segurança em redes.
        - Controle 13.1.1 – Controle de redes.
        - Controle 13.1.2 – Segurança dos serviços de rede.
        - Controle 13.1.3 – Segregação de redes.
    - Objetivo de controle 13.2 – Equipamento.

        - Controle 13.2.1 – Políticas e procedimentos para transferência de informações.
        - Controle 13.2.2 – Acordos para transferência de informações.
        - Controle 13.2.3 – Mensagens eletrônicas.
        - Controle 13.2.4 – Acordos de confidencialidade e não divulgação.

- Seção 14 – Aquisição, desenvolvimento e manutenção de sistemas:
    - Objetivo de controle 14.1 – Requisitos de segurança de sistema de informação.
        - Controle 14.1.1 – Análise e especificação dos requisitos de segurança de informação.
        - Controle 14.1.2 – Serviços de aplicação seguros em redes públicas.
        - Controle 14.1.3 – Protegendo as transações nos aplicativos de serviços.
    - Objetivo de controle 14.2 – Segurança em processos de desenvolvimento e suporte.
        - Controle 14.2.1 – Políticas de desenvolvimento seguro.
        - Controle 14.2.2 – Procedimentos para controle de mudanças de sistemas.
        - Controle 14.2.3 – Análise crítica técnica das aplicações após mudanças nas plataformas operacionais.
        - Controle 14.2.4 – Restrições sobre mudanças em pacotes de software.
        - Controle 14.2.5 – Princípios para proteger sistemas seguros.

        - Controle 14.2.6 – Ambiente seguro para desenvolvimento.
        - Controle 14.2.7 – Desenvolvimento terceirizado.
        - Controle 14.2.8 – Teste de segurança do sistema.
        - Controle 14.2.9 – Teste de aceitação de sistemas.
    - Objetivo de controle 14.3 – Dados para teste.
        - Controle 14.3.1 – Proteção dos dados para teste.
        -

- Seção 15 – Relacionamento na cadeia de suprimento:
    - Objetivo de controle 15.1 – Segurança da informação na cadeia de suprimento.
        - Controle 15.1.1 – Política de segurança da informação no relacionamento com os fornecedores.
        - Controle 15.1.2 – Identificando segurança da informação nos acordos com fornecedores.
        - Controle 15.1.3 – Cadeia de suprimento na tecnologia da informação e comunicação.
    - Objetivo de controle 15.2 – Gerenciamento da entrega do serviço do fornecedor.
        - Controle 15.2.1 – Monitoramento e análise crítica de serviços com fornecedores.
        - Controle 15.2.2 – Gerenciamento de mudanças para serviços com fornecedores.
- Seção 16 – Gestão de incidentes de segurança da informação:
    - Objetivo de controle 16.1 – Gestão de incidentes de segurança da informação e melhorias.
        - Controle 16.1.1 – Responsabilidades e procedimentos.

        - Controle 16.1.2 – Notificação de eventos de segurança da informação.
        - Controle 16.1.3 – Notificando fragilidades de segurança da informação.
        - Controle 16.1.4 – Avaliação e decisão dos eventos de segurança da informação.
        - Controle 16.1.5 – Resposta aos incidentes de segurança da informação.
        - Controle 16.1.6 – Aprendendo com os incidentes de segurança da informação.
        - Controle 16.1.7 – Coleta de evidências.
- Seção 17 – Aspectos da segurança da informação na gestão da continuidade do negócio:
    - Objetivo de controle 17.1 – Continuidade da segurança da informação.
        - Controle 17.1.1 – Planejando a continuidade da segurança da informação.
        - Controle 17.1.2 – Implementando a continuidade da segurança da informação.
        - Controle 17.1.3 – Verificação, análise crítica e avaliação da continuidade da segurança da informação.
    - Objetivo de controle 17.2 – Redundâncias.
        - Controle 17.2.1 – Disponibilidade dos recursos de processamento da informação.
- Seção 18 – Conformidade
    - Objetivo de controle 18.1 – Conformidade com requisitos legais e contratuais.

        - Controle 18.1.1 – Identificação da legislação aplicável e de requisitos contratuais.
        - Controle 18.1.2 – Direitos de propriedade intelectual.
        - Controle 18.1.3 – Proteção de registros.
        - Controle 18.1.4 – Proteção e privacidade das informações de identificação pessoal.
        - Controle 18.1.5 – Regulamentação de controles de criptografia.
    - Objetivo de controle 18.2 – Análise crítica independente da segurança da informação.
        - Controle 18.2.1 – Análise crítica independente da segurança da informação.
        - Controle 18.2.2 – Conformidade com as políticas e procedimentos de segurança da informação.
        - Controle 18.2.3 – Análise crítica da conformidade técnica.

Ressalta-se que o objetivo de controle 18.2, que é o último objetivo de controle apresentado nesta norma, visa aferir por meio de análise independente em períodos regulares a aderência da segurança da informação, face à política, normas, procedimentos, instruções de trabalho e demais outras necessidades operacionais que exijam a aplicação da segurança da informação, seja por ação preventiva aos riscos, seja por força de lei e/ou regulamentar e/ou imposta pelo mercado corporativo, dado como exemplo a exigência de empresas tomadoras de serviço.

Neste exemplo, pode-se comentar que instituições financeiras, em geral exigem de seus fornecedores aderência aos controles mantidos nesta relação, podendo ainda ser exigida uma verificação *In Loco* (no local) antes de se aceitar uma empresa como fornecedora de instituição financeira no Brasil. Lembremos ainda que diversas outras empresas estão caminhando para exigir de seus fornecedores aderência à esta norma.

Por mais que sejam estabelecidos os controles, considera-se árduo torná-la conhecida a todos dentro de uma organização. Para isto, tem o propósito a próxima seção deste material, que traz boas práticas à divulgação destas boas práticas em segurança da informação no âmbito corporativo.

Esta estrutura de seções, objetivos de controle e controles são trazidos neste material, também podem ser consultados em material disponibilizado pela RNP[2] que visa mostrar aos interessados como é que se faz a gestão da segurança da informação por meio das normas e controles em segurança da informação.

[2] Gestão da segurança da informação – Disponível em: https://pt.scribd.com/doc/58008255/Gestao-da-Seguranca-da-Informacao-NBR-27001-e-NBR-27002

1.3.3 NIST 800-53

O NIST 800-53, também conhecido como NIST *Special Publication* 800-53, está em sua quarta revisão, sendo esse documento intitulado *Security and Privacy Controls for Federal Information Systems*. Este documento traduz as recomendações adotadas pelo governo norte americano, sob a recomendação do NIST (*National Institute of Standards and Technology*), pertencente ao departamento de comércio dos Estados Unidos da América, sendo um documento composto por 462 páginas.

O documento está dividido em três seções (Introdução, Fundamentos e Processo), sendo que a riqueza do documento é traduzida por seus anexos que contêm diversos controles em segurança da informação, contendo em suas descrições aspectos claros atrelados aos mesmos. Diferente do conjunto normativo que compõe a família ISO 27000, os documentos produzidos pelo NIST são gratuitos e podem ser obtidos e utilizados por qualquer empresa que deseje entender e implementar seus respectivos controles. Diferente também da ISO 27002, os controles são identificados pelas seguintes famílias e identificados por 2 letras que indicam o acrônimo desta família:

- AC - Access Control;
- AU - Audit and Accountability;
- AT - Awareness and Training;
- CM - Configuration Management;
- CP - Contingency Planning;
- IA - Identification and Authentication;
- IR - Incident Response;
- MA – Maintenance;
- MP - Media Protection;
- PS - Personnel Security;
- PE - Physical and Environmental Protection;
- PL – Planning;

- PM - Program Management;
- RA - Risk Assessment;
- CA - Security Assessment and Authorization;
- SC - System and Communications Protection;
- SI - System and Information Integrity; e
- SA - System and Services Acquisition.

1.3.4 PCI-DSS

O PCI-DSS tem somo significado o termo *Payment Card Industry – Data Security Standard*, e representa um padrão de segurança de dados (formado por 12 requisitos) produzido e recomendado pela indústria de cartões de crédito. O PCI-DSS tem como objetivo, garantir que estabelecimentos comerciais e prestadores de serviço atendam aos requisitos mínimos de segurança durante o armazenamento e processamento relacionado aos dados de portadores de cartão.

O PCI-DSS, tem como patrono o PCI-SSC (PCI *Security Standards Council*) que é um fórum composto por diversas empresas relacionadas ao universo de cartões de crédito, cm objetivo de atualizar-se frequentemente, frente às ameaças, com objetivo de estimular às empresas que lidam com dados de cartão de crédito, o desenvolvimento, aprimoramento, armazenamento, disseminação e implementação de padrões de segurança para a proteção de dados relacionados ao cartão de crédito.

Os documentos relacionados ao PCI-DSS estão em sua versão 3.2 (atualizada em abril de 2016).

Os padrões de segurança exigidos pelo PCI-DSS se aplicam a todas as entidades envolvidas nos processos de pagamento do cartão, inclusive comerciantes, processadores, adquirentes, emissores e prestadores de serviço.

O quadro a seguir ilustra uma visão geral de alto nível:

Padrão de segurança de dados do PCI – Visão geral alto nível	
Construir e manter a segurança de rede e sistemas	**1.** Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão **2.** Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os dados do titular do cartão	**3.** Proteger os dados armazenados do titular do cartão **4.** Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas
Manter um programa de gerenciamento de vulnerabilidades	**5.** Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus **6.** Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas rigorosas de controle de acesso	**7.** Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio **8.** Identificar e autenticar o acesso aos componentes do sistema **9.** Restringir o acesso físico aos dados do titular do cartão
Monitorar e testar as redes regularmente	**10.** Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão **11.** Testar regularmente os sistemas e processos de segurança
Manter uma política de segurança de informações	**12.** Manter uma política que aborde a segurança da informação para todas as equipes

Figura 2 – Padrão de segurança de dados do PCI[3]

Neste documento, descreve-se os dados contidos em cartão, conforme indicados no quadro indicado a seguir:

Dados contábeis	
Os dados do titular do cartão incluem:	**Os dados de autenticação confidenciais incluem:**
▪ O número da conta principal (PAN) ▪ Nome do titular do cartão ▪ Data de vencimento ▪ Código de serviço	▪ Dados de rastreamento completo (dados em tarja magnética ou equivalentes em chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/Bloqueios de PIN

Figura 3 – Dados relacionados às informações mantidas em cartão de crédito[4]

Consequentemente, há dados que devem ser protegidos obrigatoriamente, onde algumas destas informações podem ser armazenadas, e outras o armazenamento não é permitido, mesmo considerando-os ilegíveis

[3] Disponível em: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_pt-BR.pdf?agreement=true&time=1499084409401

[4] Disponível em: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_pt-BR.pdf?agreement=true&time=1499084409401

em sistema de armazenamento, conforme pode ser observado no quadro a seguir:

		Elemento de dados	Armazenamento permitido	Converter dados armazenados ilegíveis conforme Requisito 3.4
Dados contábeis	Dados do titular do cartão	O número da conta principal (PAN)	Sim	Sim
		Nome do titular do cartão	Sim	Não
		Código de serviço	Sim	Não
		Data de vencimento	Sim	Não
	Dados de autenticação confidenciais[2]	Dados de rastreamento completo[3]	Não	Não armazenável conforme Requisito 3.2
		CAV2/CVC2/CVV2/CID[4]	Não	Não armazenável conforme Requisito 3.2
		PIN/Bloco de PIN[5]	Não	Não armazenável conforme Requisito 3.2

Figura 4 – Tabela de indicação do nível de proteção aos dados do cartão de crédito[5]

O processo adotado em PCI-DSS difere um pouco às demais outras recomendações, contidas em normas da família ISO 27000, pois diferente deste conjunto normativo a ISO 27000, introduz um termo ao longo de seus controles, dentro da ABNT NBR ISO/IEC 27002:2013, que é a palavra “convém”. Neste caso, os controles são apresentados, mas não há elementos que tragam a obrigatoriedade à implementação dos mesmos às empresas objeto de uma certificação perante a esta norma. No caso das recomendações do NIST 800-53, os controles são melhor detalhados, comparados aos controles dispostos em ABNT NBR ISO/IEC 27002:2013, mas não trazem também aspectos que obriguem as empresas a seguirem tais recomendações.

Já no caso do PCI-DSS, os controles dispostos são obrigatórios, sendo que há momentos que os mesmos podem não vir a ser aplicáveis, em função de alguma particularidade, ou se não forem possíveis de implementação, há a disposição de controles compensatórios, desde que:

- Atendam a intenção e o rigor do requisito original do PCI-DSS;
- Forneçam um nível semelhante de defesa ao requisito original do PCI-DSS, como o controle de compensação que contrabalança o

[5] Disponível em: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_pt-BR.pdf?agreement=true&time=1499084409401

risco de modo suficiente para o qual o requisito original do PCI-DSS tenha sido criado para fornecer uma defesa; e

- Sejam superiores (o que é descrito no PCI-DSS como “acima e além”) e comparação a outros requisitos do PCI_DSS, pois não se aceita que estar em conformidade com outros requisitos do PCI DSS consista em controle compensatório.

1.4 Ameaças, Vulnerabilidades, Riscos e Tipos de ataques em Segurança

A segurança da informação somente se justifica, tendo como tema a potencial concretização de riscos que podem vir a afetar significativamente empresas, sendo que a maior preocupação por parte das corporações é que as mesmas tenham reflexos negativos que contribuam à perda ou desvalorização financeira.

O risco tende a se concretizar quando há alguma ameaça (ou agente) que venha a contribuir à ocorrência de um potencial risco. É possível oferecer um exemplo simples sobre a diferença entre ameaça e risco quando mencionamos o cenário de roubo ou furto de veículos automotores, onde o risco é o roubo ou furto, enquanto isto o ladrão (contraventor) é a ameaça é o responsável pela ação que irá provocar à ocorrência e concretização do risco.

Apesar disto, sabe-se que somente ter a existência do ladrão, não garante que este tenha sucesso ao roubo ou furto de um automóvel, pois este veículo precisa estar acessível ao contraventor, ou mesmo ser considerável viável ao roubo ou furto, para isto, trazemos o elemento vulnerabilidade.

A vulnerabilidade é situação pela qual a segurança pode ser comprometida pela existência de falhas ou fraquezas em segurança que resultam ao aumento à propensão à concretização de riscos.

Voltando ao exemplo em questão, considera-se propenso ao furto ou roubo de veículo àquele que possa estar estacionado em local ermo, com vidros abertos ou mesmo portas destrancadas, permitindo ao agente a ação (a ameaça) identificar que pode ser mais fácil furtar um veículo desprotegido em detrimento de um veículo trancado.

A vulnerabilidade nem sempre é algo tão fácil de ser identificado como é o caso exemplificado, pois falhas de implementação em tecnologias por exemplo, trazem potenciais exposições que somente serão descobertas quando as mesmas forem exploradas pelos atacantes (as ameaças indicadas neste nosso modelo).

Apesar da existência de ameaças, vulnerabilidades e risco, há algo que pode nos auxiliar a nos proteger, que são os controles.

Os controles nada mais são que processos e tecnologias, tais quais já nos foram apresentados na seção anterior deste material, compostos pelas normas e padrões adotados pelas empresas quando estas estão aderentes à segurança da informação.

Os controles são mecanismos que diminuem a propensão à concretização de riscos ou mesmo o impacto causado à ocorrência dos mesmos. Ao exemplo ainda, consideram-se controles à proteção de veículos automotores a providência de contratação de seguro, caso ocorra a perda do veículo, reduzindo o impacto (ou seja, os prejuízos) causados pela ocorrência de roubo ou furto do mesmo. Ainda consistem em controles, mecanismos que possibilitem a proteção do veículo, como a providência de estacionamento em garagem e até mesmo o uso do automóvel em locais (ou vias) menos propensas à abordagem de criminosos. É certo que nem sempre todos os controles são empregados à proteção de uma informação, pois cada um destes componentes irá também incidir em um custo de implementação, operação e manutenção, mas é importante estar ciente que os mesmos existem visando atingir equilíbrio quanto à exposição ao risco e o apetite quanto a este risco.

Existem normas relacionadas à riscos que auxiliam os profissionais a melhor entender e aplicar as mesmas através de metodologias que visam a padronização da aplicação da análise, avaliação, tratamento, comunicação e monitoramento de riscos em âmbito corporativo baseado em um contexto (ou escopo) que visa estar sempre atento às mudanças que tais riscos apresentam, e o quanto estas mudanças interferem ao dia-a-dia em empresas, suas respectivas estratégias, seus clientes e seus respectivos produtos.

Os riscos são bem compreendidos dentro da segurança da informação por meio das normas ISO 27005 e ISO 31000.

1.5 Política e Conscientização em Segurança da Informação

Conscientizar, como o próprio nome diz é trazer a consciência sobre algum assunto ou tema a uma ou mais pessoas que desejam adquirir conhecimentos.

Em segurança da informação há um grande desafio, pois, o público a ser conscientizado, em geral tem como elemento preliminar às regras e boas práticas em segurança um conjunto normativo, composto por uma diretriz, normas e procedimentos.

Este documento, em geral é composto por diversas páginas, onde o leitor não se sente atraído em tomar conhecimento em relação ao seu conteúdo.

Uma forma de tornar as recomendações em segurança da informação, informações mais acessíveis a todos os públicos é a adoção de cartilhas lúdicas como as dispostas pelo CERT.br, por meio da Cartilha de Segurança para Internet[6].

Hoje o CERT.br disponibiliza uma cartilha[7] contendo 140 páginas, mas evitando o desestímulo à leitura, o material foi dividido em seções, conforme disposto a seguir:

- Segurança na Internet;
- Golpes na Internet;
- Ataques na Internet;
- Códigos Maliciosos (Malware);
- Spam;
- Outros riscos;
- Mecanismos de segurança;
- Contas e senhas;
- Criptografia;

[6] Disponível em: https://cartilha.cert.br/
[7] Disponível em: https://cartilha.cert.br/livro/

- Uso seguro da Internet;
- Privacidade;
- Segurança de computadores;
- Segurança de redes;
- Segurança em dispositivos móveis; e
- Glossário.

Em adição a este material foram propostos fascículos[8] contendo assuntos atualizados e relacionados às mais recentes ameaças em segurança da informação, onde estes fascículos denominam-se:

- Fascículo Códigos Maliciosos;
- Fascículo Redes Sociais;
- Fascículo Redes;
- Fascículo Verificação em Duas Etapas;
- Fascículo Computadores;
- Fascículo Internet Banking;
- Fascículo Dispositivos Móveis;
- Fascículo Privacidade;
- Fascículo Comércio Eletrônico;
- Fascículo Senhas.

E em função as atuais ameaças relacionadas ao sequestro de dados, foi lançada mais uma cartilha atrelada ao *ramsomware*[9].

Além deste conteúdo disponibilizado, diversos outros subsídios relacionados à conscientização são disponibilizados em sites, consistindo de material de estudo, onde se incluem os trabalhos acadêmicos, glossários de termos relacionados à segurança da informação, conteúdo de palestras e apresentações relacionados à segurança da informação, panfletos, infográficos,

[8] Disponível em: https://cartilha.cert.br/fasciculos/
[9] Disponível em: https://cartilha.cert.br/ransomware/

vídeos, conteúdos atrelados à entrevistas de profissionais que atuam na área de segurança da informação, perguntas e respostas em páginas denominadas FAQ (*frequently asked questions*), além de outras cartilhas que podem ser interativas e que contêm orientações quanto à segurança da informação.

1.6 Segurança em Internet das Coisas, Cyber ataques e Ransomware

Tendências quanto à segurança da informação também são tratadas pelos profissionais, onde cientes que a evolução dos riscos está presente às novas tecnologias estes profissionais precisam estar incansavelmente atentos às novidades quanto às fragilidades e vulnerabilidades que podem vir atingir não só empresas, mas também usuários domésticos e todos que possam produzir, manipular ou mesmo consumir informação.

Internet das Coisas, também conhecido como IoT são compostos por dispositivos denominados inteligentes que permitem conexão do mesmo a outros dispositivos, se valendo em geral de comunicação por meio de comunicação sem fio (WiFi e Bluetooth), apesar de existirem dispositivos relacionados à IoT também conectados a redes cabeadas.

Estes dispositivos contêm um sistema operacional e no mínimo uma aplicação que em geral permite acesso remoto de um ou mais controladores, sendo que estes dispositivos podem ser destinados a uso pessoal ou corporativo.

Normalmente estes dispositivos não contam com a implementação de mecanismos ou controles em segurança, tornando-os vulneráveis e frágeis à ataques.

Dado o cenário potencialmente destrutivo e inseguro que vivemos, foi proposto pelo NIST denominado *Cybersecurity Framework*. Este documento apresenta uma visão abrangente sobre a segurança da informação, devendo esta ser implementada em nível executivo, ao nível de negócios e processos e ao nível de implementação e operação, conforme proposto pelo modelo descrito a seguir:

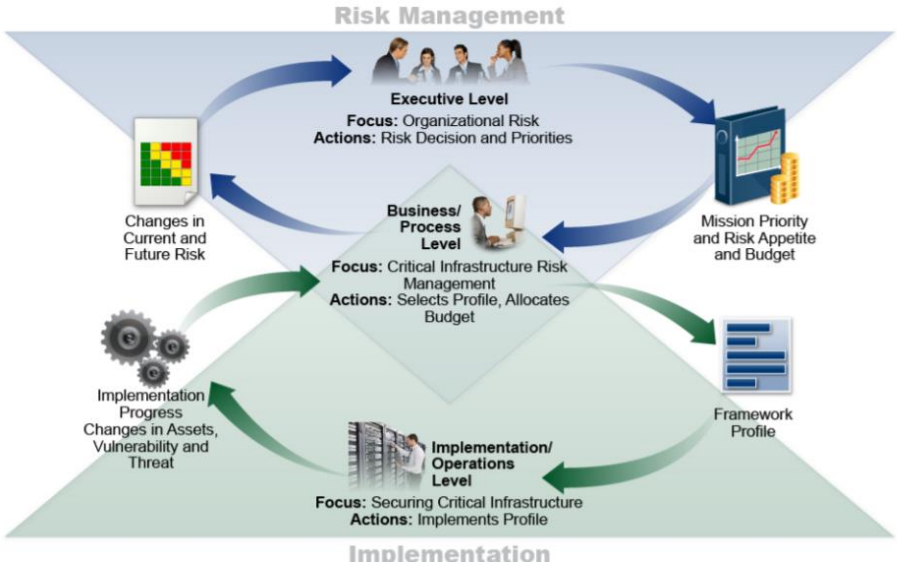

Figura 5 – Gestão de riscos e processo decisório da segurança em uma organização [10]

Este modelo ainda considera a adoção de funções e categorias, possibilitando que em etapas a cibersegurança esteja presente junto à organização por meio de controles, conforme pode ser observado a seguir:

[10] Disponível em: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figura 6 – Identificação de categorizações e funções no Cybersecurity Framework [11]

Apesar da existência destes modelos indicados neste material de estudo, não é possível garantir a proteção absoluta de informações, sistemas, pessoas, empresas e demais ativos mantidos em uma organização. O exemplo mais recente relacionado aos problemas em segurança da informação são os processos relacionados ao sequestro de dados, provocado pelos denominados ransomwares, ou softwares destinados ao sequestro de dados.

[11] Disponível em: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

1.7 Segurança em Cloud Computing e segurança em dispositivos móveis

Tecnologias trouxeram novos desafios à segurança da informação, pois o uso de dispositivos móveis cresceu nos últimos anos, assim como o consumo de dados.

Com a maior exposição de indivíduos à Internet e o frenético consumo de serviços dispostos neste ambiente por empresas, surgiu uma modalidade de serviço que hoje está em forte crescente que são denominados serviços de computação em nuvem.

Os principais modelos de serviços constituem aos denominados IaaS (Infraestrutura como serviço), PaaS (Plataforma como Serviço) e SaaS (Software como Serviço).

Infrastructure As A Service ou IaaS é o modelo onde a infraestrutura de servidores é contratada como serviço, para fazer a hospedagem de uma ou mais aplicações. Essa infraestrutura disponibilizada normalmente por um data center e os servidores são virtuais, onde o cliente paga pelo seu uso.

Platform As A Service ou PaaS é o modelo disponibilizado pelo fornecedor que apresenta uma plataforma para desenvolvimento de aplicações oferecidas na nuvem, proporcionando todo um sistema de infraestrutura, armazenamento e comunicação.

E *Software As A Service* ou SaaS é um modelo onde as aplicações são disponibilizadas na nuvem, com objetivo de se compartilhar este serviço a diversos usuários, neste cenário é comum que estes serviços sejam acessados via navegador (browser) ou por um aplicativo disponibilizado pelo provedor.

Em qualquer um destes três modelos há necessidade de se proteger bem este ambiente, onde em função da consumerização, muitas empresas estão preocupadas em como proteger dispositivos móveis de seus funcionários aos riscos e impactos atrelados à falta de segurança em informações.

1.7.1 Segurança em Cloud Computing

A segurança em ambiente disposto em nuvem, exige em princípio grande parte dos controles em segurança dispostos e exigidos em ambiente de infraestrutura tradicional também conhecido como *On Premisses*.

Entretanto, algumas responsabilidades são segregadas entre o provedor do serviço de nuvem e o usuário contratante de tais serviços.

O princípio que rege a proteção da informação, está relacionado ao ciclo de vida da informação, onde dados são criados, armazenados, utilizados, compartilhados, arquivados e destruídos.

Partindo deste princípio é necessário saber se os dados são classificados, se há políticas que definam o gerenciamento desta informação, se há questões que tratam de restrições quanto à localização da informação, em especial no que tangem questões legais, assim como os responsáveis pela autorização e propriedade e tutela da informação.

Conhecendo as necessidades em jogo, espera-se que tecnologias, processos e pessoas colaborem para a adoção de um modelo de segurança à devida proteção destes dados em nuvem que podem envolver adoção de soluções que visam evitar ou dificultar o vazamento de dados como DLP (*data loss prevention*), assim como soluções que visam evitar o acesso aos dados por pessoas não autorizadas, incluindo controles de acesso e criptografia.

Monitorar a movimentação, armazenamento e tráfego de dados e suas respectivas informações é essencial para que empresas possam se tranquilizar à adoção deste modelo de tecnologia, já que este serviço em muitos momentos está disponível a um potencial atacante 24 horas por dia, 7 dias da semana e 365 dias ao ano.

Neste aspecto a segurança junto às aplicações, torna-se essencial e com isto, espera-se que tanto desenvolvedores quanto profissionais responsáveis pela aferição da segurança destes sistemas estejam atentos à possíveis ameaças, vulnerabilidades e falhas que possam comprometer a credibilidade destes serviços.

Neste aspecto, há algumas recomendações em segurança indicado pela Cloud Security Alliance[12], dispostos nos itens a seguir:

- Compreenda a arquitetura de armazenamento em nuvem em uso, o que o ajudará a determinar os riscos de segurança e os potenciais controles;
- Quando disponível, escolha o armazenamento com dispersão dos dados;
- Utilize a segurança do ciclo de vida dos dados para identificar exposições de segurança e determinar os controles mais adequados;
- Monitore os bancos de dados internos e repositórios de arquivos chaves com o DAM e o FAM para identificar grandes migrações de dados, o que poderia indicar dados migrando para a nuvem;
- Monitore o acesso à Internet dos funcionários com filtragem de URL e/ou ferramentas de DLP para identificar dados confidenciais sendo movidos para a nuvem. Selecione ferramentas que incluem categorias predefinidas para serviços em nuvem. Considere utilizar a filtragem para bloquear a atividade não autorizada;
- Criptografe todos os dados confidenciais que se movem para ou dentro da nuvem na camada de rede, ou em nós antes da transmissão de rede. Isso inclui todos os modelos de serviços e implantações;
- Ao utilizar qualquer criptografia de dados, preste especial atenção ao gerenciamento de chaves;
- Utilize a descoberta de conteúdo para fazer a varredura do armazenamento em nuvem e identificar a exposição de dados confidenciais;
- Criptografe os volumes confidenciais na IaaS para limitar a exposição devido a instantâneos, ou o acesso não autorizado do

[12] Disponível em: https://chapters.cloudsecurityalliance.org/brazil/files/2017/02/Guia-CSA-v-3.0.1-PT-BR-Final.pdf

administrador. A técnica específica vai variar conforme as necessidades operacionais;

- Criptografe os dados confidenciais em armazenamento de objetos, geralmente com arquivos/pastas ou de criptografia do cliente/agente;
- Criptografe os dados confidenciais de aplicações e de armazenamento na PaaS. A criptografia em nível de aplicação é muitas vezes a melhor opção, especialmente porque alguns bancos de dados em nuvem oferecem suporte à criptografia nativa;
- Ao utilizar criptografia de aplicação, as chaves devem ser, sempre que possível, armazenadas externamente à aplicação;
- Se a criptografia é necessária para o SaaS, tente identificar um provedor que ofereça a criptografia nativa;
- Utilize a criptografia em Proxy, caso esta não tenha uma disponível e/ou os níveis de confiança devam ser assegurados;
- Utilize a DLP para identificar os vazamentos de dados confidenciais de implantações em nuvem;
- Normalmente, só está disponível para a IaaS e, pode não ser viável para todos os provedores de nuvem pública;
- Monitore os bancos de dados confidenciais com o DAM e gere alertas sobre as violações das políticas de segurança. Utilize uma ferramenta preparada para nuvem (*cloud-aware*);
- Considere o armazenamento para preservar a privacidade ao propor infraestrutura ou aplicações onde o acesso normal poderia revelar informações confidenciais do usuário;
- Lembre-se que a maioria das grandes falhas de segurança de dados resulta da aplicação de segurança precária;

- Os provedores de nuvem não devem apenas seguir estas práticas, mas também expor as ferramentas e as opções de segurança de dados para seus clientes;
- A remoção de dados de um fornecedor de nuvem, quer devido à expiração do contrato ou por qualquer outro motivo, deverá ser abordada em detalhes durante a configuração do SLA. Ela deve abranger a exclusão de contas de usuários, a migração ou a exclusão de dados de armazenamento primário/redundante, a transferência de chaves, entre outros.

1.7.2 Segurança em dispositivos móveis e pessoais

Dispositivos móveis no momento atual, consistem em diversas tecnologias, dentre estes são smartphones, tablets, smartwatches dentre outros. Por estes equipamentos (também denominados *gadgets*) serem nos dias atuais de fácil acesso pela disponibilidade à aquisição e uso dos mesmos para fins pessoais e corporativos, considera-se importante que os mesmos sejam protegidos às diversas ameaças que podem vir a comprometer a segurança da informação.

Segundo o CERT.br[13] há algumas características que tornam os dispositivos móveis tão peculiares quando se trata da necessidade de segurança e proteção de suas respectivas informações:

- **Grande quantidade de informações pessoais armazenadas**: informações como conteúdo de mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, números de cartão de crédito e senhas costumam ficar armazenadas nos dispositivos móveis.
- **Maior possibilidade de perda e furto**: em virtude do tamanho reduzido, do alto valor que podem possuir, pelo status que podem representar e por estarem em uso constante, os dispositivos

[13] Segurança em dispositivos móveis – Disponível em: https://cartilha.cert.br/dispositivos-moveis/.

móveis podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes.

- **Grande quantidade de aplicações desenvolvidas por terceiros**: há uma infinidade de aplicações sendo desenvolvidas, para diferentes finalidades, por diversos autores e que podem facilmente ser obtidas e instaladas. Entre elas podem existir aplicações com erros de implementação, não confiáveis ou especificamente desenvolvidas para execução de atividades maliciosas.
- **Rapidez de substituição dos modelos**: em virtude da grande quantidade de novos lançamentos, do desejo dos usuários de ter o modelo mais recente e de pacotes promocionais oferecidos pelas operadoras de telefonia, os dispositivos móveis costumam ser rapidamente substituídos e descartados, sem que nenhum tipo de cuidado seja tomado com os dados nele gravados.

No que tangem as observações do CERT.br, ainda vale considerar que os dispositivos móveis concentram praticamente todas as aplicações relacionadas à comunicação, entretenimento, compromissos, e demais outros essenciais aos cidadãos e respectivos profissionais dispostos em ambiente corporativo, tornando-se um equipamento muitas vezes essencial ao desempenho de nossas atividades diárias, sejam estas laborais ou não.

Considerando que para muitos cidadãos, os dispositivos móveis são essenciais à vida diária, considera-se também importantes a adoção de medidas que visam o aumento da segurança destes respectivos equipamentos, onde estas também são recomendações indicadas pelo CERT.br.

Os cuidados recomendados, antes de adquirir seu dispositivo móvel são s seguintes:

- Considere os mecanismos de segurança que são disponibilizadas pelos diferentes modelos e fabricantes e escolha aquele que considerar mais seguro;

- Caso opte por adquirir um modelo já usado, procure restaurar as configurações originais, ou "de fábrica", antes de começar a usá-lo; e
- Evite adquirir um dispositivo móvel que tenha sido ilegalmente desbloqueado (*jailbreak*) ou cujas permissões de acesso tenham sido alteradas. Esta prática, além de ser ilegal, pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho.

Atenta-se que além do (*jailbreak*), adotado ao desbloqueio de dispositivos com sistema operacional iOS (Apple), há demais outros sistemas alternativos que podem vir a ser instalados e de origem desconhecida que podem vir a comprometer a segurança de seus respectivos usuários.

Os cuidados recomendados, ao usar seu dispositivo móvel são os seguintes:

- Se disponível, instale um programa antimalware antes de instalar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros;
- Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;
- Fique atento às notícias veiculadas no site do fabricante, principalmente as relacionadas à segurança;
- Seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e plug-ins. Procure ainda usar aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários. Verifique comentários de outros usuários e se as permissões necessárias para a execução são coerentes com a destinação da aplicação; e
- Seja cuidadoso ao usar aplicativos de redes sociais, principalmente os baseados em geolocalização, pois isto pode comprometer a sua privacidade.

Ao considerar a instalação de um programa antimalware, considere programas inclusive gratuitos como os que são denominados como antivírus, desde que os mesmos possibilitem atualização frequente frente às novas ameaças.

Os cuidados recomendados, ao acessar redes são os seguintes:

- Seja cuidadoso ao usar redes Wi-Fi públicas;
- Mantenha interfaces de comunicação, como Bluetooth, infravermelho e Wi-Fi, desabilitadas e somente as habilite quando for necessário; e
- Configure a conexão Bluetooth para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível").

Os cuidados recomendados às informações armazenadas em dispositivo móvel são as seguintes:

- Mantenha as informações sensíveis sempre em formato criptografado;
- Faça backups periódicos dos dados nele gravados;
- Mantenha controle físico sobre ele, principalmente em locais de risco (procure não o deixar sobre a mesa e cuidado com bolsos e bolsas quando estiver em ambientes públicos);
- Use conexão segura sempre que a comunicação envolver dados confidenciais;
- Não siga links recebidos por meio de mensagens eletrônicas;
- Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas);
- Configure-o para que seja localizado e bloqueado remotamente, por meio de serviços de geolocalização (isso pode ser bastante útil em casos de perda ou furto); e

- Configure-o, quando possível, para que os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso (use esta opção com bastante cautela, principalmente se você tiver filhos e eles gostarem de "brincar" com o seu dispositivo).

É importante considerar que nos dias atuais, links são recebidos por comunicadores instantâneos, incluindo WhatsApp, Facebook Messenger e até mesmo SMS, não sendo esta uma lista exaustiva dos diversos softwares de comunicação utilizados pelos usuários de dispositivos móveis.

Em caso de uso de criptografia, considera-se também importante que o usuário não se esqueça da senha de acesso ao dispositivo, pois neste caso o usuário do mesmo pode vir perder acesso à todas as informações, sendo que se deve evitar que as senhas sejam iguais em todas as aplicações que o usuário tenha em seu dispositivo.

Os cuidados recomendados ao se desfazer do seu dispositivo móvel são as seguintes:

- Apague todas as informações nele contidas; e
- Restaure a opções de fábrica.

Esteja ciente que mesmo que este processo seja adotado, caso o dispositivo móvel não tenha sido previamente criptografado, há forte possibilidade à recuperação de informações por meio de técnicas utilizadas em perícia computacional, algo que será detalhado em aula específica nesta disciplina.

E as ações recomendadas em caso de perda ou furto são as seguintes:

- Informe sua operadora e solicite o bloqueio do seu número (chip);
- Altere as senhas que possam estar nele armazenadas (por exemplo, as de acesso ao seu e-mail ou rede social);
- Bloqueie cartões de crédito cujo número esteja armazenado em seu dispositivo móvel; e

- Se tiver configurado a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados nele armazenados.

Sabe-se que nos dias atuais, criminosos são capazes de alterar a identificação dos smartphones, algo conhecido como IMEI (*international mobile equipment identity*). Neste caso, a solicitação de bloqueio do dispositivo junto à operadora é recomendada, apesar da propensão desta medida se torna pouco eficaz, por conta do conhecimento dos criminosos, relacionados à capacidade dos mesmos ao processo de desbloqueio de smartphones.

REFERÊNCIAS

LAU, Marcelo. **Pilares da segurança da informação**. 2008. Disponível em: <http://marcelolau.blogspot.com.br/2008/09/pilares-da-segurana-da-informao-voc-j.html?m=0>. Acesso em: 11 de maio de 2018.

DSIC. **Guia básico de orientações ao gestor em segurança da informação e comunicações**. 2015. Disponível em: < http://dsic.planalto.gov.br/documentos/guiagestor.pdf>. Acesso em: 11 de maio de 2018.

ABNT NBR ISO/IEC 27001. **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306580>. Acesso em: 11 de maio de 2018.

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 11 de maio de 2018.

NIST Special Publication 800-53. **Security and Privacy Controls for Federal Information Systems and Organizations**. Disponível em: < http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf >. Acesso em: 11 de maio de 2018.

PCI-SSC. **PCI Security Standards Council**. Disponível em: < https://www.pcisecuritystandards.org/>. Acesso em: 11 de maio de 2018.

NIST. **CYBERSECURITY FRAMEWORK** Disponível em: < https://www.nist.gov/cyberframework >. Acesso em: 11 de maio de 2018.

CSA. **GUIA DE SEGURANÇA PARA ÁREAS CRÍTICAS FOCADO EM COMPUTAÇÃO EM NUVEM V3.0**. Disponível em: https://chapters.cloudsecurityalliance.org/brazil/files/2017/02/Guia-CSA-v-3.0.1-PT-BR-Final.pdf>. Acesso em: 11 de maio de 2018.

CERT.br. **Cartilha de Segurança para Internet**. Disponível em: < https://cartilha.cert.br/>. Acesso em: 11 de maio de 2018.

RNP. **Gestão da Segurança da Informação NBR 27001 e NBR 27002**. Disponível em: <https://pt.scribd.com/doc/58008255/Gestao-da-Seguranca-da-Informacao-NBR-27001-e-NBR-27002>.Acesso em: 11 de maio de 2018.