SEGURANÇA DA INFORMAÇÃO

Prof. Luis Gonzaga de Paulo

TEMA 1 – NORMAS E PADRÕES

A informação é um patrimônio, um ativo da organização, que exige cuidados para ser preservado. Como já vimos, a informação, tal como qualquer outro ativo, está sujeita a riscos, e pode ter seu valor deteriorado ou totalmente perdido se usada indevidamente, ou mesmo se for roubada. Para combater esses riscos são necessárias medidas de proteção que contemplem procedimentos, técnicas e ferramentas adequadas.

No decorrer da era da informação, o uso cada vez mais intenso da computação resultou em necessidades cada vez maiores e mais complexas de medidas de proteção. Ao mesmo tempo, foram sendo experimentadas e aprimoradas – e também selecionadas – aquelas mais efetivas, cuja eficiência e eficácias foram comprovadas. Nós denominamos essas medidas de proteção como “boas práticas” e, em sua grande maioria, essas boas práticas foram submetidas a estudos e métodos que permitiram sua aplicação repetida e rotineira, sendo adaptadas e ensinadas, com possibilidade de medição dos resultados obtidos. Essa metodologia propiciou o estabelecimento de normas e de padrões mundialmente reconhecidos e aceitos que, colocados em prática de forma adequada, resultam em efetivas medidas de proteção.

Nos itens a seguir apresentamos algumas das principais normas e padrões reconhecidos e utilizados mundialmente para a garantia da Segurança da Informação no domínio das Tecnologias da Informação e da Comunicação – TICs.

1.1 ISO 15408

O Common Criteria for Information Technology Security Evaluation – ou Critério Comum – é o nome do padrão de mercado que deu origem à norma ISO 15408. É um conjunto de critérios característicos da especificação de segurança do *software*, assim da verificação e validação desses critérios. A ISO 15408 contempla três aspectos da segurança no desenvolvimento de *software*: a segurança do ambiente de desenvolvimento, a segurança de aplicação desenvolvida e a garantia de segurança da aplicação desenvolvida. São três aspectos interdependentes:

- A **segurança do ambiente de desenvolvimento**, imprescindível para a segurança do *software*: não é possível construir um *software* seguro em um ambiente inseguro.

- A **segurança da aplicação desenvolvida**, que advém da correta identificação das necessidades de segurança, sua especificação, implementação e teste. Geralmente essa segurança está diretamente ligada ao método de construção e às boas práticas de programação.
- A **garantia de segurança**, que vai além da segurança do *software* propriamente dita, pois implica a segurança do *software* e também do sistema no qual está instalado. Isso deve ser comprovado por meio de testes, inclusive de organizações independentes, com a participação do cliente ou usuário final.

1.2 ISO 27000

A ISO/IEC 27000, uma série de normas também conhecida como "Família de Padrões ISMS" – ou, de forma abreviada no inglês, "ISO27K" – apresenta os padrões de Segurança da Informação publicados em conjunto pela Organização Internacional para Padronização (International Standard Organization – ISO) e pela Comissão Eletrotécnica Internacional (International Electrotechnical Commission – IEC).

Esse conjunto ou série é a mais completa compilação de boas práticas com reconhecimento internacional e aplicação validada, sendo inclusive objeto de certificação. Originou-se no British Standard 7799, de 1999, posteriormente transformado na norma ISO IEC 17799, em 2005. De fato, contempla uma variedade de temas distribuídos de forma organizada por 45 normas específicas, relacionadas no Quadro 1 a seguir.

Quadro 1 – Conjunto de normas ISO 27000

ISO/ IEC	Descrição
27000	Sistemas de gerenciamento de Segurança da Informação – Visão geral e vocabulário.
27001	Tecnologia da informação – Técnicas de segurança – Sistemas de gerenciamento de Segurança da Informação – Requisitos. A versão de 2013 da norma especifica um sistema de gerenciamento de Segurança da Informação da mesma maneira formalizada, estruturada e sucinta, como outros padrões ISO especificam outros tipos de sistemas de gerenciamento.
27002	Código de práticas para controles de Segurança da Informação – essencialmente um catálogo detalhado de controles de Segurança da Informação que podem ser gerenciados pelo SGSI.
27003	Orientação para implementação do sistema de gerenciamento de Segurança da Informação (SGSI).
27004	Gerenciamento de Segurança da Informação – Monitoramento, medição, análise e avaliação.

ISO/ IEC	Descrição
	Continuação Quadro 1
27005	Gerenciamento de risco de Segurança da Informação.
27006	Requisitos para organismos que fornecem auditoria e certificação de sistemas de gerenciamento de Segurança da Informação.
27007	Diretrizes para auditoria de sistemas de gerenciamento de Segurança da Informação (com foco na auditoria do sistema de gerenciamento).
27008	Orientação para auditores nos controles do SGSI, com foco na auditoria dos controles de Segurança da Informação.
27009	Essencialmente um documento interno para o comitê de desenvolvimento de setores/variantes específicas do setor ou diretrizes de implementação para os padrões ISO 27K.
27010	Gerenciamento de Segurança da Informação para comunicações intersetoriais e interorganizacionais.
27011	Diretrizes de gerenciamento de Segurança da Informação para organizações de telecomunicações, baseadas na ISO/IEC 27002.
27013	Diretriz sobre a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1, derivada do Itil.
27014	Governança de Segurança da Informação.
TR 27015	Diretrizes de gerenciamento de Segurança da Informação para serviços financeiros – em processo de desativação.
TR 27016	Economia da Segurança da Informação.
27017	Código de práticas para controles de Segurança da Informação com base na ISO/IEC 27002 para serviços em nuvem.
27018	Código de prática para proteção de informações pessoalmente identificáveis (PII) em nuvens públicas que atuam como processadores de PII.
TR 27019	Segurança da informação para controle de processo no setor de energia.
27031	Diretrizes para disponibilidade de tecnologia de informação e comunicação para continuidade de negócios.
27032	Diretriz para segurança cibernética.
27033-1	Segurança de rede – Parte 1: Visão geral e conceitos.
27033-2	Segurança de rede – Parte 2: Diretrizes para o projeto e implementação de segurança de rede.
27033-3	Segurança de rede – Parte 3: Cenários de rede de referência – Ameaças, técnicas de *design* e questões de controle.
27033-4	Segurança de rede – Parte 4: Protegendo as comunicações entre redes usando *gateways* de segurança.
27033-5	Segurança de rede – Parte 5: Protegendo as comunicações entre redes usando redes virtuais privadas (VPNs).
27033-6	Segurança de rede – Parte 6: Protegendo o acesso à rede IP sem fio.
27034-1	Segurança de aplicativos – Parte 1: Diretriz para segurança de aplicativos.
27034-2	Segurança de aplicativos – Parte 2: Estrutura normativa da organização.
27034-6	Segurança de aplicativos – Parte 6: Estudos de caso.
27035-1	Gerenciamento de incidentes de Segurança da Informação – Parte 1: Princípios do gerenciamento de incidentes.
27035-2	Gerenciamento de incidentes de Segurança da Informação – Parte 2: Diretrizes para planejar e preparar a resposta a incidentes.
27036-1	Segurança da informação para relacionamentos com fornecedores – Parte 1: Visão geral e conceitos.
27036-2	Segurança da informação para relacionamentos com fornecedores – Parte 2: Requisitos.

ISO/ IEC	Descrição
	Continuação Quadro 1
27036-3	Segurança da informação para relacionamentos com fornecedores – Parte 3: Diretrizes para segurança da cadeia de fornecimento de tecnologia da informação e comunicação.
27036-4	Segurança da informação para relacionamentos com fornecedores – Parte 4: Diretrizes para segurança de serviços em nuvem.
27037	Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.
27038	Especificação para redação digital em documentos digitais.
27039	Prevenção contra intrusões.
27040	Segurança de armazenamento.
27041	Garantia de investigação.
27042	Analisando evidências digitais.
27043	Investigação de incidentes.
27050-1	Descoberta Eletrônica – Parte 1: Visão geral e conceitos.
ISO 27799	Gerenciamento de Segurança da Informação em saúde usando a ISO/IEC 27002 – orienta as organizações do setor de saúde sobre como proteger informações pessoais de saúde usando a ISO/IEC 27002.

Fonte: ABNT, 2014.

Em ABNT (2014) são apresentadas algumas dessas normas com o texto completo, em português, além de um complemento contendo a NBR 16167:2013, que trata da classificação, rotulação e tratamento da informação – que estudaremos mais à frente –, e a NBR ISO 22301:2013, que trata da continuidade dos negócios.

O conhecimento das normas desse conjunto é imprescindível para os profissionais que atuam na área da Segurança da Informação em geral e da segurança da computação (*cybersecurity*) em particular. A aplicação dessas normas requer um preparo e atualização contínuos, sendo recomendável para a organização a certificação com base nessas normas.

1.3 ISO 31000

Como já vimos nas aulas anteriores, a norma ISO 31000 é voltada para a gestão de riscos em geral. Como a área de Segurança da Informação é extremamente dependente da gestão de riscos, essa norma torna-se imprescindível para o planejamento e a efetivação das medidas de Segurança da Informação da organização. Conforme dita a própria norma, a gestão de riscos pode ser aplicada a toda a organização, em suas diversas áreas e níveis, a qualquer momento, bem como a funções, projetos e atividades específicos. O uso adequado da norma tem como propósito possibilitar à organização a gestão de riscos, com o intuito de, entre outros objetivos:

- Aumentar a probabilidade de alcançar os objetivos.
- Incentivar a gestão proativa.
- Estar ciente da necessidade de identificar e tratar o risco em toda a organização.
- Melhorar a identificação de oportunidades e ameaças.
- Cumprir os requisitos legais e regulamentares relevantes e as normas internacionais.
- Melhorar os relatórios obrigatórios e voluntários e a governança.
- Melhorar a confiança em si e a confiança das partes interessadas.
- Estabelecer uma base confiável para tomada de decisão e planejamento.
- Melhorar os controles e efetivamente alocar e usar recursos para tratamento de risco.
- Melhorar a eficácia e eficiência operacionais, o desempenho em saúde e segurança, bem como a proteção ambiental.
- Melhorar a prevenção de perdas e gestão de incidentes e minimizar perdas.
- Melhorar a aprendizagem organizacional e a resiliência organizacional.

Esses propósitos são compartilhados com diversos atores das organizações, para os quais a norma visa atender uma ampla gama de necessidades. Entre esses atores podemos relacionar os responsáveis pelo desenvolvimento da política de gestão de riscos dentro de sua organização; aqueles incumbidos de garantir que o risco seja efetivamente gerenciado dentro da organização como um todo, ou dentro de uma área, projeto ou atividade específica; aqueles que precisam avaliar a eficácia de uma organização na gestão de risco; e os desenvolvedores de normas, guias, procedimentos e códigos de práticas que, no todo ou em parte, definem como o risco deve ser gerenciado dentro do contexto específico desses documentos.

1.4 Itil

O Itil – Information Technology Infrastructure Library é um compêndio para orientar o gerenciamento mais eficiente da área de TI, bem como para prestar serviços de maneira otimizada e eficaz. É também um conjunto de melhores

práticas de gestão de TI que surgiu no final dos anos de 1980, com base em métodos criados pelo governo inglês, mais precisamente pela Secretaria de Comércio (Office of Government Commerce, OGC). Além do reflexo geral do Itil sobre a Segurança da Informação, notadamente em função da política de Segurança da Informação e do efetivo controle das TIC em geral, o Itil estabelece no livro 4 – Service Design um processo específico para o gerenciamento da Segurança da Informação com base na ISO 27000

1.5 Cobit

O Cobit – Control Objectives for Information and Related Technology é um *framework* que visa o nível de excelência na gestão de TIC. É um guia para a gestão de TI proporcionado pelo Isaca – Information Systems Audit and Control Association, formatado para apoiar os gestores que precisam constantemente avaliar o risco e controlar os investimentos de TIC em uma organização.

O Cobit também se destina aos usuários e clientes que precisam ter garantias de que os serviços de TIC – dos quais dependem os produtos e serviços internos e externos da organização – estão sendo bem gerenciados. Além disso, serve de apoio para o pessoal de controle e auditoria, que pode se apoiar nas suas recomendações para avaliar o nível da gestão de TI e aconselhar o controle interno da organização.

No domínio da Segurança da Informação, o Cobit reforça as responsabilidades e estabelece a formalização das políticas e dos mecanismos de gestão, dos indicadores e dos controles indispensáveis para o estabelecimento do nível de segurança adequado às operações da organização.

1.6 Nist CSF

O CyberSecurity Framework – CSF do Nist (National Institute Standards and Technology, ou Instituto Nacional de Padrões) foi publicado em fevereiro de 2014 como padrão para a estrutura de segurança padronizada de infraestrutura crítica nos Estados Unidos. O Nist CSF é reconhecido como recurso para ajudar a melhorar as operações de segurança e a governança de organizações públicas e privadas. É composto de cinco funções principais: identificar, proteger, detectar, responder e recuperar, distribuídas em 21 categorias de atividades que fazem referência a diversos outros padrões e normas. Além disso, o CSF estabelece quatro camadas ou níveis para a classificação do estágio atual da Segurança da

Informação na organização.

1.7 PCI-DSS

O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (Payment Card Industry Data Security Standard – PCI DSS) é um conjunto de padrões de segurança projetados para garantir que todas as empresas que aceitam, processam, armazenam ou transmitem informações de cartão de crédito mantenham seus dados e os dos portadores de cartão em um ambiente seguro. O Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI SSC) foi criado em 2006 para gerenciar a evolução contínua dos padrões de segurança PCI (Payment Card Industry), com foco na melhoria da segurança da conta de pagamento durante o processo de transações com cartões.

O PCI-DSS é administrado e gerenciado pelo PCI-SSC (www.pcisecuritystandards.org), um órgão independente criado pelas principais administradoras de cartões de pagamento no mercado dos Estados Unidos (Visa, MasterCard, American Express, Discover e JCB). É importante observar que essas marcas e as organizações que usam os serviços de pagamento por cartão de crédito são os responsáveis pela conformidade, e não o conselho do PCI.

TEMA 2 – ÁREAS DE CONTROLE

O conjunto de normas ISO/IEC 27000 aborda praticamente todos os aspectos e atividades das organizações no que se refere às TICs. A cláusula 6.1.3 da norma 27001:2013 descreve como uma organização pode responder a riscos com um plano de tratamento de riscos. Uma parte importante disso é escolher controles apropriados, embora isso não seja mais uma obrigação nem mesmo para atender às auditorias e até mesmo à certificação.

A versão anterior estabelecia que os controles identificados na avaliação de risco para gerenciar os riscos constavam no Anexo A, o que permite que a avaliação de riscos seja mais simples e muito mais significativa para a organização, ajudando consideravelmente no estabelecimento de um senso adequado de propriedade dos riscos e controles. Conforme podemos constatar pela ABNT (2014), existem 114 controles em 14 cláusulas e 35 categorias de controle (a versão anterior, de 2005, tinha 133 controles em 11 grupos), distribuídos conforme a Tabela 1.

Quadro 2 – Controles e objetivos do conjunto de normas ISO 27K

Cláusula	Objetivo	Controles
A.5	Políticas de Segurança da Informação	2
A.6	Organização da Segurança da Informação	7
A.7	Segurança de recursos humanos – controles aplicados antes, durante ou depois do emprego	6
A.8	Gerenciamento de ativos	10
A.9	Controle de acesso	14
A.10	Criptografia	2
A.11	Segurança física e ambiental	15
A.12	Segurança de operações	14
A.13	Segurança de comunicações	7
A.14	Aquisição, desenvolvimento e manutenção de *software*	13
A.15	Relações com fornecedores	5
A.16	Gerenciamento de incidentes de Segurança da Informação	7
A.17	Aspectos de Segurança da Informação do gerenciamento de continuidade de negócios	4
A.18	Conformidade; com requisitos internos, como políticas, e com requisitos externos, como leis	8

Fonte: ABNT, 2014.

Esses controles foram atualizados para refletir as mudanças nas TICs que afetam as organizações, como, por exemplo, computação móvel, computação em nuvem e internet das coisas. Porém, como já apontado, é possível usar e até mesmo obter a certificação ISO/IEC 27001:2013 sem usar esses controles. A aplicação desses controles é detalhada e especificada na norma ISO/IEC 27002:2013, o código de práticas para esses controles.

TEMA 3 – CLASSIFICAÇÃO DA INFORMAÇÃO

Já abordamos os componentes principais de um gerenciamento de Segurança da Informação, a saber: a classificação da informação, a implementação de controles de segurança, a verificação regular dos resultados dos controles, a preparação e o planejamento de respostas aos incidentes e o tratamento, a aceitação ou transferência de risco. Vamos aprofundar nosso conhecimento sobre o processo de classificação das informações e fornecer uma visão mais clara da abordagem para a classificação das informações.

3.1 O que é a classificação das informações?

A classificação das informações é o processo que uma organização segue para desenvolver um entendimento de seus ativos de informação, atribuir um valor a esses ativos e determinar o esforço e o custo necessários para proteger adequadamente os mais críticos desses ativos de informação. A classificação é um primeiro passo importante no estabelecimento de um programa de

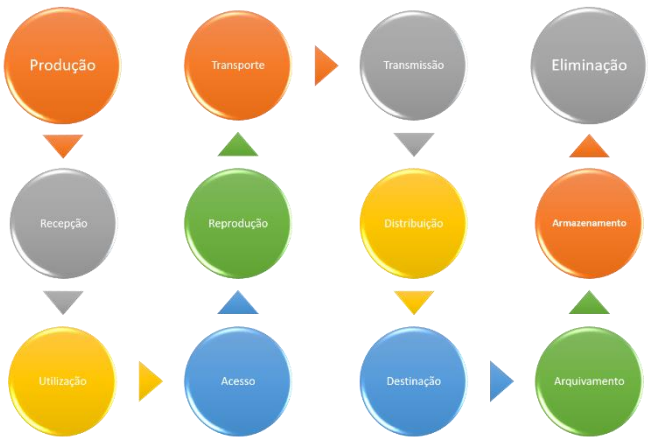
gerenciamento de Segurança da Informação, pois permite que a organização tome decisões gerenciais sobre a alocação de recursos para proteger suas informações. Partimos da premissa de que a organização já concluiu uma avaliação de risco e entende seus requisitos de privacidade e confidencialidade operacionais, regulatórios e contratuais.

Já sabemos que, para elaborar e colocar em prática os controles de Segurança da Informação listados e qualquer ação voltada às boas práticas e à política de segurança, deve-se fazer, antes, o inventário dos ativos das TICs da organização. Com o apoio desse inventário, as informações podem ser classificadas com base em seus usos, suas necessidades e particularidades. Para isso, é muito importante conhecer em detalhes cada um dos processos e das atividades do negócio.

3.2 Critérios, características e níveis

A classificação da informação ocorre de acordo com o tipo de negócio e das organizações, e também o grau de importância para as atividades e projetos dos quais toma parte. De acordo com a norma ISO/IEC 27002:2013, recomenda que, na classificação da informação, a organização leve em consideração seu valor, requisitos legais, sensibilidade e criticidade, bem como controles de proteção necessários à informação, além do compartilhamento ou restrição de acesso (ABNT, 2014).

Figura 1 – O ciclo de vida da informação



Fonte: ABNT NBR 16167.

Além da citada norma ISO, a ABNT editou em 2013 uma norma brasileira (NBR) voltada para a Segurança da Informação, mais especificamente para classificação, rotulação e tratamento da informação – a ABNT NBR 16167. Essa

norma define a classificação da informação como “a ação de definir o nível de sensibilidade da informação a fim de assegurar que a informação receba um nível adequado de proteção, conforme o seu valor, requisitos legais, sensibilidade e criticidade para a organização” (ABNT, 2014). Essa norma brasileira também aborda a rotulação e o tratamento da informação durante o seu ciclo de vida, da produção até a eliminação, como mostrado na Figura 1.

Essa norma também estabelece que a classificação deve ser feita pelo proprietário da informação o mais cedo possível, no momento em que é gerada ou obtida e passa a fazer parte dos processos da organização, ou assim que uma informação não classificada é identificada. Além disso propõe uma classificação da informação com base em quatro níveis, como mostrado no Quadro 2.

Tabela 1 – Níveis de classificação da informação de acordo com a NBR 16167

Níveis de classificação	**Características básicas**
Nível 1	Informações que podem ou devem ser divulgadas publicamente. Normalmente a divulgação deste tipo de informação é de responsabilidade de áreas específicas que fazem a interface com os públicos externos, como as áreas de comunicação e marketing, mas a responsabilidade pela classificação continua sendo do proprietário da informação. Exemplos deste nível são informações divulgadas para as mídias externas, ao mercado, à sociedade etc.
Nível 2	Informações internas a serem divulgadas a todos os colaboradores e prestadores de serviços, desde que estes estejam comprometidos com a confidencialidade das informações. Exemplos deste nível são as normas corporativas e campanhas internas da Organização.
Nível 3	Informações restritas, que devem ser divulgadas a determinados grupos, áreas ou cargos. Exemplos de informações deste nível são: informações de projetos, procedimentos específicos das áreas, relatórios de desempenho de processos, indicadores das áreas etc.
Nível 4	Informações que requerem um tratamento especial e cuja divulgação não autorizada ou acessos indevidos pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégias da Organização. Normalmente se encaixam neste nível informações privadas das pessoas, de clientes, de fornecedores e informações estratégicas da Organização.

Fonte: ABNT, 2014.

Esses níveis são somente sugeridos, e cada organização pode adequá-los às suas necessidades, inclusive com a criação de outros níveis ou a separação do público do nível 2 (pessoal próprio, terceiros etc.), por exemplo. A NBR 16167 também apresenta uma referência para a definição do tratamento adequado das

informações desses níveis em diversos cenários, os mais típicos em todas as etapas do ciclo de vida da informação nas organizações.

TEMA 4 – PADRÕES DE CLASSIFICAÇÃO DA INFORMAÇÃO

Verificamos que a classificação de dados é o processo que uma organização segue para desenvolver um entendimento de seus ativos de informação, atribuir um valor a esses ativos e determinar o esforço e o custo necessários para proteger adequadamente os mais críticos desses ativos de informação. Também já consideramos que os sistemas de negócios atuais e a natureza das empresas conectadas geram uma enorme quantidade de informações. Embora essas informações tenham valor organizacional, é importante reconhecer que nem todas têm o mesmo valor. Assim, nem todas precisam ser protegidas da mesma maneira. A realização de uma classificação de informações permite determinar os diferentes tipos de informações da organização e fornecer detalhes dos requisitos de proteção para cada tipo.

Os controles da ISO 27001 que apresentamos descrevem as melhores práticas para mitigar os riscos de Segurança da Informação. Embora não haja exigência de usar os controles, quaisquer outros controles usados devem ser comparados com aqueles. O objetivo de controle do Anexo A, A.8.2, afirma que a informação deve receber “um nível apropriado de proteção de acordo com sua importância para a organização”. Isso é alcançado por “classificação”, “rotulagem” e “manipulação”.

4.1 O que é um padrão de classificação?

Um padrão de classificação de informações é um modelo que estabelece um conjunto padronizado de descrições que podem ser aplicadas a todos os ativos de informação. Os termos que a organização usa são inteiramente uma questão de preferência e estão abertos à personalização, mas podem ser tão simples quanto um sistema de numeração ou rótulos descritivos como “Confidencial”, “Restrito”, e assim por diante. Qualquer esquema que a organização use deve ser apropriado para suas necessidades. Seja qual for a escolha para descrever seus ativos de informação, a organização deve ter um registro de ativos de informações completo e abrangente, que formalize a existência de ativos e permita avaliar seu valor rapidamente.

4.2 Estruturando a classificação da informação

Um padrão – ou esquema – de classificação de informações ideal deve limitar o número de classificações possíveis e, por sua vez, o número de processos necessários para manter essa classificação. Para a maioria das organizações não é necessário haver mais do que três ou quatro. Um exemplo simples de níveis de classificação pode ser algo como:

- **Não classificadas**: as informações não são particularmente valiosas, nem a organização é obrigada a protegê-las. Podem ser acessadas por qualquer pessoa para qualquer finalidade, incluindo a distribuição para o público ou clientes. Pode incluir os comunicados de imprensa, vagas de emprego, entre outras.
- **Apenas interna**: a informação tem valor internamente e pode ter algum valor para os concorrentes. Pode ser distribuída gratuitamente para qualquer pessoa dentro da organização. Pode incluir notas internas, dados de emprego, informações de contratos, e assim por diante.
- **Confidencial**: a informação tem um valor significativo e pode haver requisitos legais para sua proteção. O acesso é limitado a funções ou camadas designadas dentro da organização. Pode incluir propriedade intelectual, detalhes de pagamento do cliente, planejamento estratégico de longo prazo e outras.

Cada um desses níveis de classificação pode servir de premissa para que outros controles sejam usados para garantir que as informações sejam adequadamente protegidas contra acesso, modificação, distribuição e destruição não autorizados.

4.3 Implementando a classificação da informação

Existem vários fatores críticos na implementação de um esquema eficaz de classificação de informações: rotulagem, controles de acesso e conscientização do pessoal. Vamos analisar cada um desses fatores:

- Os **rótulos** são usados para identificar o valor dos dados e exibir sua classificação. A forma como a rotulagem é tratada deve estar de acordo com as necessidades da organização, mas deve ser relevante para o modo como a informação é usada. Por exemplo, cópias de arquivos, mídias

removíveis e assim por diante devem ter um rótulo físico; o conteúdo digital deve incluir o rótulo no nome do arquivo, o próprio documento e os metadados.

- Os **controles de acesso** podem ser usados na etiquetagem, nos metadados ou na estrutura de arquivos, para permitir ou negar acesso a informações com base nos direitos de acesso do usuário. Para cópias impressas, isso pode envolver o arquivamento de informações em locais específicos, que podem ser bloqueados, ou armazenar os documentos em local externo para controlar o acesso. O conteúdo digital pode empregar controles de rede para garantir que os usuários tenham acesso apenas às informações a que têm direito.
- A **conscientização do pessoal** é essencial para que qualquer esquema de classificação seja eficaz, assim como assegurar que seja simples o bastante para navegar – não deve haver muitas classificações; as regras para lidar com informações devem ser claras; a equipe deve classificar com segurança quaisquer informações novas ou ainda não classificadas. Todo o pessoal deve ser adequadamente treinado na classificação e tratamento de informações.

Embora não seja um sistema completo de Segurança da Informação, a classificação de informações é uma das ferramentas mais efetivas que as organizações devem considerar desde o início, construindo a base de sua abordagem de segurança em camadas. Ao identificar o valor dos dados que criam e compartilham, as organizações podem tomar decisões sobre como proteger dados mais valiosos ou confidenciais fundamentadas em critérios confiáveis. Ao contrário de muitas outras soluções de Segurança da Informação, a classificação de informações se espalha por pessoas, processos e tecnologias, fornecendo um grau de redundância e confiabilidade naturais. Mesmo que a organização não esteja buscando a certificação de acordo com a ISO 27001, o uso de um padrão de classificação de informações é a melhor prática e um processo que pode ser concluído sem um investimento proibitivo de tempo ou recursos.

TEMA 5 – PROCESSO DE CLASSIFICAÇÃO

Em um ambiente de negócios globalizado e conectado, os sistemas, as pessoas e as empresas produzem e utilizam uma enorme quantidade de

informações e de dados. Embora tenham valor organizacional, é importante reconhecer que nem todas as informações e dados têm o mesmo valor e, em função disso, não precisam ser protegidos da mesma maneira. A classificação de dados permite determinar os diferentes tipos de informações da organização e adequar os requisitos de proteção para cada tipo de informação e de dados.

O processo de classificação de informações é um ciclo contínuo com base no PDCA (Plan – Do – Check – Act), pois o universo das informações de uma organização está em constante evolução e mudança, assim como as TICs que suportam e permitem o acesso e a troca de informações com o ambiente no qual a organização opera. Desse modo, é necessário que esse processo esteja vinculado aos planos estratégicos, táticos e operacionais da organização, permeando todas as atividades que produzam informações e que delas dependam para a entrega de seus resultados.

5.1 As quatro atividades essenciais

Existem quatro atividades essenciais que um esforço bem-sucedido de classificação de informações incluirá:

- **Identificar**: identificar as informações produzidas ou utilizadas pela organização no desempenho das atividades.
- **Localizar**: identificar em que lugar as informações são produzidas ou utilizadas nos processos da organização, e por quem.
- **Classificar**: categorizar e determinar quais informações precisam de monitoramento e proteção, em quais momentos e qual a forma mais adequada de proteção.
- **Valorizar**: atribuir um valor às informações, de modo que possa ser calculada a perda de valor e o limite de investimento em sua proteção.

5.1.1 Identificar

Parece simples identificar as informações. No entanto, identificar sistematicamente as informações da organização pode ser bastante desafiador. Essa não é uma atividade que se pode delegar ao administrador do banco de dados. Ela precisa ser multifuncional, organizada em torno dos processos de negócios e orientada pelos proprietários dos processos. Geralmente vemos esses itens concluídos como orientações de cada processo de negócios – rastreando os

fluxos de dados com os proprietários do processo para identificar as informações. É comum serem necessárias várias perguntas importantes para identificar os tipos de dados mantidos pela sua organização, como, por exemplo:

- Quais dados a organização coleta de ou sobre clientes, fornecedores, parceiros comerciais?
- Quais dados a organização gera sobre essas partes interessadas durante o curso dos negócios?
- Quais dados proprietários a organização cria no desenvolvimento, fabricação, marketing e vendas de produtos?
- Quais dados transacionais a organização obtém ou gera no curso dos negócios?
- De todos esses dados coletados e gerados, o que é público, o que é privado e o que é confidencial?

Identificar e catalogar esses dados é o primeiro passo no processo de classificação. Ele servirá de base para todas as outras atividades de classificação.

5.1.2 Localizar

Indo além da identificação inicial, é importante identificar em seguida todos os lugares nos quais as informações são armazenadas, principalmente aquelas em formato digital. É desejável que o administrador de banco de dados ou arquiteto corporativo de informações ofereça suporte e ajude a concluir o processo de identificação de local. As ferramentas de prevenção de perda de dados podem até ser usadas como parte dessa etapa para ajudar na varredura de redes, procurando determinados tipos de informações.

Os sistemas de negócios atuais são tão integrados que as informações geralmente são distribuídas, interconectadas ou compartilhadas entre sistemas. Isso significa que podem residir em vários sistemas, e não apenas no sistema em que foram originalmente criadas ou inseridas. Lembre-se também de pensar nos sistemas de relatórios e nos *data warehouses*. Muitas vezes, dados transacionais podem ser arquivados nesses sistemas. Também é importante considerar sistemas com imagens de documentos e fotocopiadoras, nos quais as cópias eletrônicas de dados físicos já residem.

Um último sistema a considerar ao identificar o lugar no qual os dados são

armazenados é o sistema de *backup* real. Quase todas as organizações mantêm cópias de *backup* de dados. Não é incomum que as organizações mantenham várias cópias dos dados do sistema para suportar os requisitos de retenção de registros. No entanto, é quase tão comum que as organizações retenham esses registros além do requisito de negócios. Identificar em que lugar os dados são retidos excessivamente para que possam ser adequadamente eliminados é um resultado importante de um processo de classificação de dados.

5.1.3 Classificar

Neste ponto, teremos uma compreensão sólida do tipo de informações e de dados que a organização mantém, do lugar em que estão armazenados e sob a responsabilidade de quem. Os tipos de dados devem estar prontamente aparentes agora e, provavelmente, poderão ser separados em poucas categorias principais, dentre as quais:

- Dados de clientes.
- Dados pessoais.
- Informação da relação de trabalho ou da saúde, protegidas por lei.
- Dados de cartão de crédito.
- Dados competitivos/segredos comerciais.
- Dados disponíveis publicamente.

É importante que os gestores da organização determinem as classificações relevantes para a organização e o que proteger. A lista que apresentamos é apenas bom começo, e certamente pode haver mais itens de classificação para a organização. O objetivo principal é ter um índice para os diferentes tipos de informações na organização.

Uma boa regra é resistir ao desejo de fazer uma grande lista, muito detalhada, que vai ficar muito granular. Mais de dez tipos de dados de negócios na classificação? É um bom sinal de que essa lista ficou muito granular. Uma classificação demasiadamente granular tende a ser menos gerenciável ao longo do tempo. Cinco a oito categorias de classificação são razoáveis.

5.1.4 Valorizar

Atribuir um valor às informações classificadas é uma etapa essencial, pois permite a tomada de decisões com base no quanto se gasta para proteger essas informações. Vários fatores contribuem para o valor geral de um conjunto de informações. As organizações precisam considerar as penalidades associadas a uma perda ou violação de informações. Compreendendo os possíveis custos de *hardware* e *software* associados a um incidente que prejudique um determinado conjunto de informações, a organização pode definir expectativas realistas para o custo de proteção desse conjunto. Vamos considerar estes exemplos:

- Dados médicos ou da saúde: Quais multas podem ser cobradas por cada registro ilegalmente divulgado?
- Dados de portadores de cartão de crédito: Como um aumento nos custos de transação com cartões de crédito afetaria a receita líquida? Ou pior, causaria a perda da capacidade de aceitar cartões de crédito?
- Dados pessoais: A quais penalidades civis a organização pode estar sujeita pela divulgação inadvertida de informações pessoais? Quanto precisaria pagar para fornecer serviços de monitoramento de crédito a seus clientes?
- Segredos comerciais: Como uma perda de vantagem competitiva afetaria a receita?

5.1.5 Manter

Tendo concluído essas quatro etapas para classificar as informações, a organização pode tomar decisões sobre a forma mais adequada para gerenciá-las e protegê-las. Os resultados dessa classificação devem ser usados no programa geral de gerenciamento da Segurança da Informação. Ao entender em que lugar as informações estão e dimensionar o valor organizacional dessas informações, a organização pode implementar os controles de Segurança da Informação mais eficazes e econômicos, com base no risco de negócios associado a cada tipo de informação produzida, utilizada e mantida pela organização.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **Coletânea de Normas Técnicas – Segurança da Informação**. Rio de Janeiro: ABNT, 2014.

ISO/IEC. **ISO/IEC 27005:2011** – **Information technology** – **Security Techniques** – **Information Security Risk Management**. [S.l.], 2011.