2019

White paper series
Publicação 6

– CLASSIFICAÇÃO –
DE DADOS

OEA Mais direitos para mais pessoas

aws

— CLASSIFICAÇÃO —
DE DADOS

CRÉDITOS

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Equipe técnico OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Kadri Kaska
Elsa Neeme
Klaid Mägi
Lauri Luht

Equipe técnico AWS

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTEÚDO

1. **INTRODUÇÃO..... 5**

ESTRUTURA 6

2. **PRINCÍPIOS DE CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES..... 7**

3. **QUAIS SÃO OS MODELOS EXISTENTES DO SETOR PÚBLICO?..... 9**

ESTADOS UNIDOS DA AMÉRICA (EUA) 9
REINO UNIDO 11
ARGENTINA 12

4. **RECOMENDAÇÕES PARA ESTABELECER UM SISTEMA DE CLASSIFICAÇÃO DE DADOS.....13**

AUDITORIA 13
IMPLEMENTAÇÃO 14
MONITORAMENTO 15
REVISÃO 16

5. **RECURSOS RECOMENDADOS.....17**

6. **ANEXO I. CENÁRIOS DE RISCO.....19**

— CLASSIFICAÇÃO —
DE DADOS

Introdução

1

Organizações, pessoas, bilhões de dispositivos conectados geram, processam e consomem todo tipo de dados todos os dias. A cada dia são criados mais de 2,5 quintilhões de bytes de todo tipo de informação[1] nnova para ser analisada, processada e armazenada. Os tipos de dados também são diversos: de uns e zeros que provêm de dispositivos simples da Internet das coisas (IoT, por suas siglas em inglês) que indicam de quando se liga ou se desliga algum aparelho (por exemplo, um sensor de movimento) até o clima, o trânsito, as transações financeiras, a saúde e as redes sociais, entre outros. Além disso, os governos, que são o objetivo principal desse documento, geram, administram e armazenam petabytes de dados. A grande diversidade de dados demanda a análise de políticas públicas que governos adotam para classificar e armazenar os dados que possui. A resposta dos governos a esta demanda gerou o que se denomina política de Classificação de Dados, que reflete um conjunto de regras específicas para órgãos e organizações governamentais classificarem os diversos tipos de dados para que então possam ser protegidos, controlados, armazenados e processados em função dessa classificação.

A primeira pergunta que se faz frequentemente é "por que não protegemos todos os dados em nível mais alto e assim poupamos tempo?" Para os governos, isto não é viável financeiramente, muito menos é alinhado aos benefícios que a classificação e a rotulação adequadas dos diferentes tipos de dados podem proporcionar. Em primeiro lugar, os níveis mais altos de proteção de dados geram custos adicionais e, muitas vezes, essas despesas são superiores aos valores que os governos podem gastar. Outro aspecto é que, caso conferissem o mesmo tratamento a todos os dados governos poderiam enfrentar dificuldades para aplicar controles de acesso adequados, o que levaria a que as pessoas que não tenham uma razão oficial para ter acesso a dados confidenciais possam ter acesso a eles facilmente. E, finalmente, podem se obter bons resultados na gestão e na apresentação de relatórios sobre dados que estão organizados, agrupados, assegurados e rotulados adequadamente, dependendo da classificação.

A classificação de dados permite às organizações pensar em dados partindo da sensibilidade e do impacto comercial deles, o que ajuda a

1 Forbes: How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#49f394760ba9

organização a avaliar os riscos relacionados a diferentes tipos de dados. As organizações reconhecidas por seus padrões, tais como a Organização Internacional de Normalização (ISO, por suas siglas em inglês) e o Instituto Nacional de Padrões e Tecnologia (NIST, por suas siglas em inglês), aconselham a aplicação de esquemas de classificação de dados para que a informação possa ser administrada e assegurada de uma forma mais efetiva, de acordo com sua criticidade e com seu risco relativo e sua recomendação é prescindir das práticas que tratam todos os dados da mesma forma. Apesar do fato de cada organização processar e classificar os dados de acordo com suas respectivas necessidades, regulamentações e, até mesmo, capacidades, continua existindo a necessidade de se estabelecer uma linha base de controles de segurança que ofereça proteção adequada contra vulnerabilidades, ameaças e riscos relacionados com o nível de proteção atribuído, especialmente, no setor público.

Os benefícios de se possuir uma classificação efetiva de dados são inúmeros. Uma organização pode melhorar seu acesso e eficiência organizacional e uma classificação de dados efetiva também garante que a informação receba a proteção adequada dependendo de sua sensibilidade, valor e criticidade, bem como do tipo e das características dos riscos decorrentes de uma divulgação indevida, de um dano ou de sua destruição.

O objetivo deste whitepaper é dar orientações para o desenvolvimento de um sistema de classificação de dados para garantir o acesso e a proteção das informações geradas e processadas pelos governos. É importante salientar que uma política de classificação de dados é necessária, independentemente do tipo de infraestrutura utilizada por uma organização, seja nas instalações próprias, na nuvem ou dispositivo móvel. Uma política de classificação de dados dá às organizações diretrizes sobre o nível de segurança e sobre os processos associados para armazenar e administrar diferentes tipos de dados. Além disso, as recomendações constantes neste whitepaper podem ser utilizadas independentemente do tipo de organização, pois seu principal objetivo é mostrar às entidades governamentais que prestam serviços públicos os aspectos fundamentais a serem levados em conta nesse processo.

|Estrutura|

Este documento técnico visa fornecer orientações para o desenvolvimento de um sistema de classificação de dados, a fim de garantir o acesso e a proteção das informações geradas e processadas pelos governos. O whitepaper analisa os diversos tipos de classificação de dados existentes em níveis nacional e internacional, a fim de tornar essa classificação de dados uma ferramenta funcional para evitar riscos potenciais, como a classificação de informações excessivas ou insuficientes.

O documento está dividido em quatro seções: i. Princípios de classificação de dados e informações; ii. Quais são os modelos existentes do setor público? iii. Recomendações para o estabelecimento de um sistema de classificação de dados; e iv. Recursos recomendados, onde se oferece uma visão geral dos princípios de classificação de dados, bem como recomendações para o seu estabelecimento. Para ilustrar alguns dos modelos existentes no setor público, na Seção II, é analisada a experiência dos Estados Unidos, do Reino Unido e da Argentina em sua implementação, bem como as regulamentações gerais de classificação de dados. Os estudos de caso dos EUA e do Reino Unido são particularmente relevantes por seu nível de rigor e sofisticação. Já o caso argentino destaca a experiência de um país na região da América Latina. Mais importante ainda é que as recomendações deste whitepaper sejam aplicadas dependendo do contexto e das necessidades de sua própria organização quando você criar uma estratégia de classificação de dados.

Princípios de classificação de dados e informação

2

A implementação da gestão da informação em geral e a classificação de dados em particular varia de acordo com o tipo de organização e pode até ser diferente para cada organização. No entanto, existem certos princípios fundamentais comuns nos governos, nas organizações não governamentais e nas organizações comerciais. A seguir, mostrase uma síntese de seis princípios que constam nas fontes jurídicas nacionais (e regionais) e nos instrumentos das organizações internacionais para a gestão da informação. Os princípios devem ser utilizados como um guia e não como um ponto de referência único e permanente quando estiver sendo preparada a construção e/ou aperfeiçoamento de uma estratégia de gestão da informação e a classificação de dados.

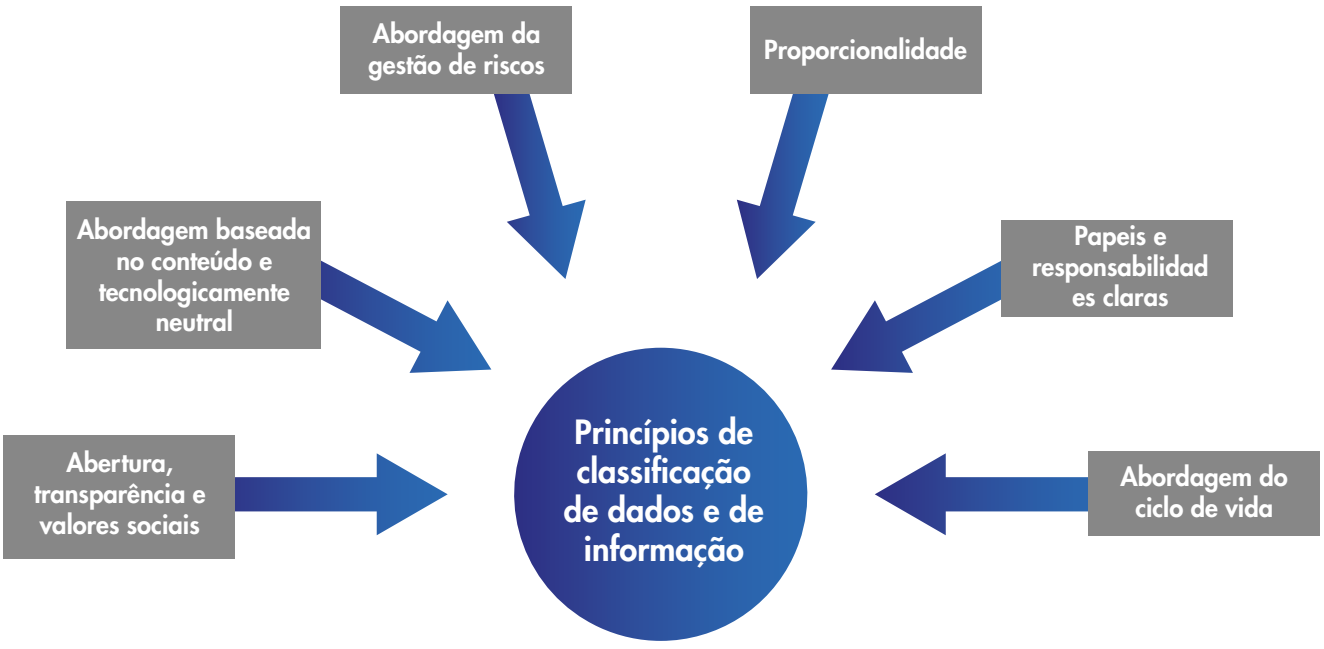

Figura 1- Princípios de classificação de dados e informação

1. **Abertura, transparência e valores sociais:** A classificação deve ser utilizada com cuidado e de acordo com a sensibilidade, o valor e a criticidade dos dados. As restrições de acesso só devem ser escolhidas nos casos em que a divulgação de informações seja prejudicial aos interesses legítimos e às obrigações legais da própria organização, do seu pessoal ou de terceiros. Nesses casos, os procedimentos especificados devem ser rigorosamente observados para garantir que as informações não sejam comprometidas, quer intencionalmente, quer inadvertidamente. O desafio será não classificar excessivamente por conveniência ou praticidade, o que prejudicaria a transparência e a confiança do público, privando assim as partes interessadas de tomarem suas próprias decisões na gestão de riscos.

2. **Abordagem baseada no conteúdo e tecnologicamente neutra:** As nformações devem ser classificadas de acordo com seu conteúdo e os riscos associados ao comprometimento do conteúdo, independentemente de seu formato, meios ou origem. Não deve haver discriminação com base no formato ou nos meios da informação, seja analógica (em papel) ou digital ou por ser armazenada em um sistema de informação, em meios de armazenamento, em dispositivos móveis ou na nuvem. Além disso, a decisão de classificar a informação deve depender do próprio conteúdo e não necessariamente vir automaticamente da fonte da informação na qual esteja localizada, à qual responde ou à qual faz referência. Por exemplo, confiar em fontes públicas não deve pressupor automaticamente que as informações agregadas devam ser divulgadas publicamente.

3. **Abordagem da gestão de riscos:** As informações devem ser protegidas de acordo com o nível de sensibilidade, valor e criticidade que elas tenham. A proteção é geralmente feita com uma abordagem progressiva, baseada nos níveis correspondentes ao valor e ao risco. Um nível de proteção abrange o conjunto de medidas para reduzir os riscos a um nível aceitável, ou seja, diminuir a possível gravidade e probabilidade de a informação ser comprometida. Para determinar o nível de sensibilidade e o valor da informação, é necessário levar em conta tanto o grau de dano potencial de comprometimento (divulgação não autorizada, alteração ou perda) quanto o valor potencial dos dados.

4. **Proporcionalidade:** As informações serão classificadas em um nível adequado que deverá ser o mais baixo possível, mas o mais elevado que seja necessário.

5. **Papéis e responsabilidades claras:** No que diz respeito à classificação de dados, devem ser estabelecidos a política e os processos para alcançar a segurança da informação dentro da organização e eles devem ser confirmados pelo compromisso e pela consciência da segurança da informação.

6. **Abordagem do ciclo da vida:** Como faz parte de um sistema de gestão da informação, o sistema de classificação deve tomar em consideração as informações ao longo de todo o seu ciclo de vida: da criação ou recepção, armazenamento, recuperação, modificação, transferência, cópia e transmissão até à destruição. Além disso, a política de gestão de informação/ processamento de dados de uma organização não deve ser escrita em pedra, mas sim deve ser avaliada regularmente para garantir que satisfaz as necessidades e expectativas da organização.

Quais são os modelos existentes no setor público?

3

A globalização tem marcado uma tendência de convergência na terminologia de classificação de dados. Esta convergência tem sido impulsionada, principalmente, pelo rigor dos padrões da indústria das TIC (por exemplo, a observância das definições ISO/IEC, NIST), pelos fatos políticos e jurídicos regionais consequentes (particularmente na União Europeia e nos seus estadosmembros), mas sobretudo pela interação e a interdependência entre domínios (por exemplo, uma crescente consideração à cibersegurança e à regulamentação da proteção de dados entre si). Por conseguinte, é aconselhável levar em conta estas melhores práticas quando forem feitas as definições nacionais.

Os Estados Unidos (EUA), o Reino Unido e a Argentina já estabeleceram esquemas de classificação de dados para os dados no setor público. Os governos dos EUA e do Reino Unido usam um esquema de classificação de três níveis, no qual a maioria dos dados do setor público é classificada nos dois níveis mais baixos. A Argentina foi incluída como um estudo de caso para apresentar um exemplo regional de implementação e os desafios que enfrentou. A cidade de Washington D.C. também poderia ser um bom modelo a ser destacado por ter sido aplicada a convergência de dados abertos com classificação de dados sem um componente de segurança nacional. Os sistemas de classificação de dados têm uma pequena lista de atributos e medidas ou critérios associados que ajudam as organizações a determinar o nível adequado de categorização.[2]

|Estados Unidos da América (EUA)|

O governo dos EUA utiliza um sistema de classificação em três níveis que foi atualizado pela Ordem Executiva 135261 e está fundamentado no potencial impacto sobre a segurança nacional caso essas informações fossem divulgadas (ou seja, questões de confidencialidade):

1.Confidencial— Informação cuja divulgação não autorizada possa causar danos à segurança nacional.

2.Secreta— Informação cuja divulgação não autorizada possa causar danos graves à segurança nacional.

2 AWS Data Classification – Secure Cloud Adoption (junho2018)

3.Alto secreto— Informação cuja divulgação não autorizada possa causar danos excepcionalmente graves à segurança nacional.

Embora esta não seja uma classificação real, nos EUA também é usado o termo "dados não classificados" para fazer referência a qualquer dado que não esteja incluído nos três níveis oficiais de classificação. Até mesmo em relação aos dados não classificados, existem alguns avisos para informações sensíveis, tais como "Apenas para uso oficial" (FOUO, por suas siglas em inglês) e "Informações controladas não classificadas" (CUI, por suas siglas em inglês) que restringem a sua divulgação ao público ou a pessoas não autorizadas. No entanto, aqui não estão sendo levadas em conta as diversas leis de proteção de dados baseadas em margens mais estreitas de tipos de dados, tais como dados fiscais privados, dados criminosos, dados de cartões de crédito, dados de atendimento médico e outros.

Devido à abordagem tão restrita do sistema de classificação dos EUA, que não inclui diretamente a integridade e a disponibilidade de dados entre seus níveis de classificação, que deveriam ser solicitados ao avaliar os requisitos de proteção da informação, o NIST criou um esquema de categorização em três níveis baseado no potencial impacto na confidencialidade, integridade e disponibilidade das informações e nos sistemas de informação aplicáveis à missão de uma organização. A maioria dos dados processados e armazenados pelas organizações do setor público pode ser classificada como se lista a seguir:

- **Baixo—** Efeito adverso limitado nas operações da organização, nos ativos da organização ou nas pessoas.

- **Moderado —** Efeito adverso grave nas operações da organização, nos ativos da organização ou nas pessoas.

- **Alto —** Efeito adverso severo ou catastrófico nas operações da organização, nos ativos da organização ou nas pessoas.

Classificação de dados	Classificação do sistema de segurança
Não classificado	De Baixo a alto
Confidencial	De Moderado a alto
Secreto	De Moderado a alto
Alto secreto	Alto

Tabela 1 — Alinhamento da classificação de dados com a categorização de segurança do sistema

Para muitos outros governos nacionais, provinciais, estaduais e municipais, este sistema duplo de classificação e categorização pode ser complexo e desnecessário para satisfazer as necessidades de segurança das informações. Nessas situações, uma opção mais simples pode ser juntar os dois conceitos em um único termo "classificação", que é abordar a segurança nacional (caso corresponder) e a importância dos três pilares da proteção da informação: confidencialidade, integridade e disponibilidade na missão e nos negócios da organização. Por esta razão, a palavra "classificação" será usada neste documento com uma abordagem holística da categorização para a confidencialidade, integridade e disponibilidade, em vez do alcance mais limitado do impacto na segurança nacional.

|Reino Unido|

O governo do Reino Unido recentemente simplificou seu esquema de classificação reduzindo os níveis de seis para três, que são os seguintes:

1.Oficial— Operações e serviços comerciais de rotina que poderiam ter consequências prejudiciais se fossem perdidos, roubados ou publicados nos meios de comunicação social, mas nenhum deles seria considerado como um perfil de ameaça elevada.

2.Secreto—Informações muito sensíveis que justificam a intensificação das medidas de proteção para se defender contra atores de ameaças muito decididos e altamente capazes (por exemplo, o comprometimento delas poderia prejudicar significativamente as capacidades militares, as relações internacionais ou a investigação de crimes graves e da delinquência organizada).

3.Alto secreto— As informações mais confidenciais que exigem os mais elevados níveis de proteção contra as ameaças mais graves (por exemplo, o compromisso poderia causar a perda generalizada de vidas ou por em risco a segurança ou o bemestar econômico do país ou das nações amigas).

O governo do Reino Unido classificou tradicionalmente cerca de 90% dos seus dados como "oficiais"[3]. O Reino Unido utiliza uma abordagem de classificação flexível e descentralizada, na qual as agências privadas definem quais os serviços de nuvem que são adequados para os dados "oficiais" com base na garantia de segurança de um fornecedor de serviços de nuvem (CSP, por suas siglas em inglês) e em 14 princípios de segurança da nuvem[4]. A maioria das agências governamentais do Reino Unido já determinou que é apropriado usar as CSPs de grande escala e de boa reputação ao executarem cargas de trabalho com dados "oficiais".

O governo do Reino Unido estabeleceu várias considerações para toda a segurança da informação quando armazenada na nuvem:

1.Oficial— Todas as informações e ativos que sejam classificados como "oficiais" são adequados para diferentes serviços do GCloud[4]. No entanto, todos os proprietários de dados devem entender completamente todo o processo de credenciamento do GCloud. Todos os serviços de tecnologias da informação e da comunicação (TIC) devem seguir o processo de gestão de riscos estabelecido nas Normas de Segurança Garantiada Informação do governo do Reino Unido, bem como cumprir com as abordagens arquitetônicas padronizadas que devem ser aplicadas no Reino Unido.

2.Secreto— Todos os serviços das TIC que tratam ou armazenam informação secreta deve ser credenciados segundo corresponder dependendo do modelo de ameaça secreta. Os padrões ou conselhos de design específicos devem provir da Autoridade Técnica Nacional para a proteção da informação (CESG, por suas siglas em inglês). Uma avaliação preliminar do risco e das implicações para habilitar a funcionalidade da troca de informação no nível secreto será altamente restrito e administrado, utilizando a capacidade credenciada compartilhada.

3. Altamente secreto:— Os sistemas das TIC projetados devem ser adequadamente acreditados a fim de poder conter materiais *Altomemte secretos*. Pode ser necessário contar com assessoramento arquitetônico personalizado.

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf

4 https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

5 O quadro G-Cloud é um acordo entre o governo do Reino Unido e os fornecedores que oferecem serviços baseados na nuvem.

|Argentina|

Em 2004, o governo argentino começou a estabelecer os requisitos para a formação e implementação de uma estratégia nacional de proteção de dados. Esta estratégia inicial incluiu a criação de um modelo de política de segurança, a formação de um comitê de segurança da informação, o estabelecimento de suas funções e a nomeação de um coordenador para a supervisão dos trabalhos desse comitê. A política foi formalizada em 2005, quando o Escritório Nacional de Tecnologias da Informação (ONTI por suas siglas em espanhol), a entidade argentina responsável da transformação e implementação de soluções tecnológicas no setor público, promulgou o Modelo de Política de Segurança da Informação, Decreto nº 378, que depois foi atualizado e modificado em 2014, com base em uma série de recomendações decorrentes de sua revisão de 2013 e passou a ser chamada Disposição 1/2015.[i]

Nessa política são estabelecidas as melhores práticas para a proteção e a administração de ativos como parte da sua gestão de riscos. Os proprietários dos dados e das informações são responsáveis por classificar a informação, dependendo do grau de sensibilidade, por documentar e atualizar a classificação da informação e por definir quais os usuáriosdevem ter acesso a essa informação dependendo de suas funções e papeis. No âmbito da classificação, a política deve se basear nos seguintes três fatores: confidencialidade, integridade e disponibilidade. Cada um desses três fatores tem uma escala de 0 a 3, que determina o grau de proteção que deve receber. A escala se divide da seguinte forma:

- **Baixa criticidade:** As informações são consideradas como públicas. As informações são normalmente conhecidas e utilizadas por qualquer pessoa ou funcionário. Uma modificação não autorizada pode ser facilmente resolvida e não compromete as operações da organização.

- **Criticidade média:** As informações são consideradas como reservadas para uso interno. As informações podem ser conhecidas ou utilizadas por alguns funcionários da organização e por algumas autoridades delegadas externas. Seu uso poderia causar leves riscos ou prejuízos para a agência, o setor público nacional ou terceiros. Uma modificação não autorizada poderia ser resolvida, embora possa causar pequenos prejuízos para a agência pública ou para terceiros associados. A perda de um dia ou de forma permanente poderia causar danos significativos nas operações da organização.

- **Alta criticidade:** As informações são consideradas como confidenciais ou secretas. Estas informações somente podem ser conhecidas por um grupo ou por um grupo muito pequeno de funcionários, geralmente os altos diretores da organização, e sua divulgação ou uso não autorizado poderia causar sérios prejuízos ao setor público ou a terceiros associados. A perda permanente poderia causar graves danos à organização.

i http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Recomendações para estabelecer um sistema de classificação de dados

4

Os sistemas de classificação de dados existentes reconhecem diferentes níveis de sensibilidade, valor e criticidade da informação, bem como diversos níveis de severidade e probabilidade de comprometimento. A menos que os níveis de segurança para certos dados sejam prescritos por lei (por exemplo, para informação de segurança nacional ou privacidade) e/ou precisem de alinhamento com compromissos regionais ou internacionais, a definição dos níveis de segurança depende da decisão da organização em particular. Isto não implica necessariamente que a observância dos requisitos legais exija uma série de categorias de classificação independentes. Quando o risco e as proteções necessárias são equivalentes, é bem possível que essas proteções pertençam a um mesmo nível de classificação.

A seção a seguir oferece um resumo das fases primárias do processo de classificação de dados. Não substitui a aplicação sistemática das normas de segurança da informação ou dos requisitos legais decorrentes de instrumentos específicos, mas pretende proporcionar uma visão geral das principais etapas necessárias para desenvolver e aplicar um sistema de classificação de dados. É dividido em quatro etapas principais:

|Auditoria|

•Inventário de ativos de dados
A primeira etapa envolvida na classificação de dados dentro de uma organização é a execu;áo de um inventário de dados ou uma "auditoria de dados". Esta atividade deve proporcionar uma compreensão ampla dos tipos de dados e informações processadas dentro da organização, seu valor, sensibilidade e criticidade.

Esta etapa também abrange a identificação dos requisitos legais aplicáveis, bem como uma auditoria das políticas e dos procedimentos organizacionais ou administrativos existentes para a gestão de dados, incluindo as funções e responsabilidades organizacionais existentes no processamento de dados.

• Avaliação de riscos
Após terem sido definidas as políticas de classificação de dados, o sistema de classificação de dados pode ser implementado. A etapa seguinte é fazer uma avaliação de riscos para os tipos de dados processados, identificando e quantificando os riscos de gravidade e de probabilidade, priorizando os riscos com base nos critérios de aceitação de riscos e objetivos relevantes para a

organização. O resultado deste exercício deve orientar e determinar a seleção de medidas técnicas e organizacionais adequadas, bem como as prioridades para a gestão de riscos. As avaliações de risco devem ser periódicas - reconhecendo que o ambiente tecnológico e de ameaças, bem como o das práticas de segurança, evoluem continuamente ao longo do tempo – e, de preferência, devem ser comparáveis.[6]

A avaliação de riscos é uma responsabilidade do controlador de dados, em alguns casos apoiado por requisitos legais, conforme discutido na seção anterior.[7] A legislação aplicável pode exigir que o controlador demonstre que o tratamento cumpre com os requisitos e com as restrições estabelecidas (por exemplo, o GDPR o faz em relação ao tratamento de dados pessoais). Veja no Anexo I algumas ideias sobre os fatores de risco que podem ser considerados na realização deste processo.

•Definição dos níveis de proteção e sua aplicação

Devem ser definidos os requisitos de proteção adequados, agrupados por categoria de classificação, para cada tipo de ativo de informação.

O número de níveis de classificação de dados deve ser exatos para as necessidades da organização. Uma abordagem muito ampla é difícil de aplicar e pode resultar em que os dados sejam protegidos de forma incoerente e com um risco maior, podendo confundir os controladores e os processadores de dados. Já um modelo excessivamente simplificado apresentaria o risco de ser uma classificação excessiva ou insuficiente. Uma abordagem em três níveis tende a satisfazer tanto aos padrões de segurança da informação (ISO, NIST, padrões nacionais) quanto, na maioria dos casos, às expectativas de conformidade legal.

•Determinação dos papeis na gestão de dados

A próxima etapa é definir os papéis e as responsabilidades da organização e do pessoal em relação à classificação e proteção da informação. Além dos papeis, devem ser definidas as obrigações de gestão de riscos adequadas para cada papel. O objetivo é "traduzir" o anterior em rotinas organizacionais através de políticas e procedimentos. Esta é também uma boa fase para revisar e atualizar os regulamentos internos existentes como parte deste processo.

Em última instância, a organização, como "controladora de dados", é responsável pelo conformidade e deve ser capaz de provar essa conformidade (através da prestação de contas).

|Implementação|

•Classificação

Dependendo da avaliação de risco, o nível de risco é atribuído considerando cada objetivo de segurança individualmente (confidencialidade, integridade e disponibilidade). Uma classificação geral é atribuída aos dados de acordo com o valor mais alto entre os três fatores.[8] Alguns sistemas também reconhecem um nível misto (alta confidencialidade, integridade moderada, baixa disponibilidade)[9].

6 ISO 27000:2018; ISO/IEC 27005 proporciona orientação sobre a gestão de riscos de segurança da informação, incluindo o assessoramento sobre a avaliação de riscos, tratamento de riscos, aceitação de riscos, relatórios de riscos, monitoramento de riscos e revisão de riscos. Também são incluídos os exemplos de metodologias de avaliação de riscos.

7 Vir, e.g., GDPR, prâmbulo seção 75

8 Data Classification: Secure Cloud Adoption'. AWS, junho 2018. https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf.

9 Por exemplo, IT Grundschutz da Alemanha https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html e o ISKE da Estônia, https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.

•Considerações para tecnologias emergentes: nuvem, dispositivo móvel e IoT

Deve ser adotada uma abordagem baseada no risco para todas as avaliações e implementações técnicas, quer se trate de equipamentos tradicionais em instalações, dispositivos móveis, na nuvem ou com dispositivos da Internet das coisas (IoT). As estratégias para adotar tecnologias emergentes devem ser influenciadas pela estratégia de risco organizacional, mas também devem fornecer feedback para atualizar a estratégia de risco da organização à medida que novas capacidades vão sendo disponibilizadas. Uma avaliação dos ativos de dados, dos níveis de risco e dos requisitos de confidencialidade, integridade e disponibilidade deve oferecer à organização o entendimento do seu nível de tolerância ao risco, bem como as combinações aceitáveis de implementação, modelos de serviço e as localizações que as tecnologias emergentes podem oferecer.

Por exemplo, uma das tecnologias emergentes mais incompreendidas atualmente é a "nuvem". Quando governos e organizações não possuem um programa de classificação de dados, processos de gestão de riscos e se concentram em controles técnicos herdados em vez de em objetivos de segurança de dados, isso leva a medo, incerteza e dúvida (FUD, por suas siglas em inglês). Esse FUD impede que a organização adote tecnologias emergentes e novos recursos e que perca desempenho e eficiência de custo.

Uma abordagem de "migração por etapas" pode ser útil no que diz respeito à adoção de tecnologias emergentes. Nesse caso, os ativos e os serviços são inicialmente atribuídos a "macrocategorias" (por exemplo, não sensíveis e não críticos, meio sensíveis e meio críticos, etc.) e uma classificação detalhada é atribuída a cada ativo e serviço à medida que ele migra para a nuvem[10].

|Monitoramento|

• Acompanhamento e garantia de qualidade
Deve ser designada uma entidade adequada para o acompanhamento, o assessoramento e a consultoria, bem como para a análise das decisões de classificação, por exemplo, Diretor de Informação (CIO, por suas siglas em inglês), Diretor de Dados (CDO, por suas siglas em inglês) ou Diretor de Segurança da Informação (CISO, por suas siglas em inglês) cuja responsabilidade específica é a classificação de dados, as decisões de risco dos dados e medidas de proteção necessárias. Essa entidade deve, igualmente, estar habilitada para demonstrar a garantia de qualidade na implementação dos controles de segurança, a idoneidade e a adequação dos controles existentes para cumprir com os objetivos de segurança desejados e com qualquer requisito de conformidade.

• Melhora contínua e monitoramento
Após os ativos de dados serem classificados, devem se aplicar os procedimentos de segurança a fim de fazer um monitoramento e uma avaliação constante para continuar cumprindo com os requisitos de conformidade e de gestão de risco. Para continuar cumprindo com os objetivos de segurança da política, é aconselhável desenvolver padrões de segurança e guias de implementação baseados nas atuais capacidades técnicas e não técnicas, que podem ser atualizadas para adotarem mais facilmente novas inovações sem ter que atualizar a política.

10 Security & Resilience in Governmental Clouds: Making an informed decision. ENISA 2011, https://www.enisa.europa.eu/publications/security-and-resilience...clouds/.../fullReport.

|Revisão|

•Revisão e ajuste periódico

Para além do monitoramento e da avaliação contínua, as revisões sistemáticas periódicas permitem fazer ajustes no acesso aos dados e na revisão de dados classificados. Uma metodologia de reclassificação e revisão pode garantir que sejam aplicadas não somente medidas de segurança adequadas à tecnologia atual e ao ambiente de ameaça/risco, mas também ao valor e à sensibilidade dos dados classificados que sempre podem ser alterados. As informações classificadas devem ser revisadas regularmente para evitar que as informações herdadas permaneçam vigentes, o que é caro para armazenar e administrar. É também aconselhável revisar periodicamente as políticas e os procedimentos de classificação.

Figura 2- Recomendações para estabelecer um sistema de classificação de dados

Recursos recomendados

5

Convênio do Conselho da Europa sobre acesso aos documentos públicos (2009)
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084826

Classificação de dados para a preparação da nuvem. Microsoft, abril de 2017.
https://gallery.technet.microsoft.com/Data-Classification-for-51252f03

Classificação de dados: adoção segura da nuvem. AWS, junho de 2018.
https://d1.awsstatic.com/Whitepapers/compliance/AWS_Data_Classification.pdf

Ordem Executiva 13526 sobre classificação e desclassificação de informação sobre segurança nacional (CT:IM-226; 10-31-2018). Escritório de origem: A/GIS/IPS https://fam.state.gov/fam/05fam/05fam0480.html; vide 5 FAM 482.5 para as categorias de classificação.

Guia de boas práticas para a implementação segura de nuvens governamentais. ENISA, 2013,
https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

Regulamento geral de proteção de dados. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e pelo que é revogado o Parecer 95/46/EC. OJ L 119, 4.5.2016, p. 1–88, http://data.europa.eu/eli/reg/2016/679/oj

olítica de proteção da informação da CPI, ICC/AI/2007/001. Boletim do Secretário Geral ST/SGB/2007/6 de 12 de fevereiro de 2007 sobre sensibilidade, classificação e tratamento,
https://www.icc-cpi.int/resource-library/Vademecum/ICC%20Information%20Protection%20Policy%20-%202007.pdf

IT Grundshutz. Escritório Federal de Segurança da Informação. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

Lei de informação pública, Estônia https://www.riigiteataja.ee/en/eli/529032019012/consolide

Uso seguro de serviços na nuvem no setor financeiro. Boas práticas e recomendações. ENISA, 2015 https://www.enisa.europa.eu/publications/cloud-in-finance

Lei de Secretos de Estado e Informação Classificada de Estados Estrangeiros, https://www.riigiteataja.ee/en/eli/501042019009/consolide

Publicação especial do NIST 800-60 Rev. 1 (Volume 1, Volume 2), Guia para atribuir tipos de informação e sistemas de informação a categorias de segurança.

Publicação 199 das Normas federais de processamento de informação do NIST: Normas para a categorização de segurança da informação federal e dos sistemas de informação https://nvlpubs.nist.gov/nistpubs/FIPS/NIST. FIPS.199.pdf

Quadro de gestão de riscos do NIST (RMF) https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

Classificações de segurança do governo do Reino Unido https://www.gov.uk/government/publications/government-security-classifications

Organização Internacional de Normalização (ISO) 27001, Requisitos para os sistemas de gestão de segurança da informação https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Associação de Auditoria e Controle de Sistemas de Informação (ISACA) Objetivos de controle para a Informação e a Tecnologia Relacionadas (COBIT) http://www.isaca.org/cobit/pages/default.aspx

Blogue da AWS sobre como abordar a residência de dados — https://aws.amazon.com/blogs/security/addressing-data- residency-with-aws/

Documentos técnicos da AWS — https://aws.amazon.com/Whitepapers/

A segurança física e o centro de dados da AWS — https://aws.amazon.com/compliance/data-center/data- centers/

Classificação de dados da AWS: adoção segura da nuvem em junho de 2018 https://d1.awsstatic.com/Whitepapers/compliance/AWS_Data_Classification.pdf

Anexo I. Cenários de risco

6

A categorização a seguir resume os cenários de risco comumente reconhecidos nos instrumentos incluídos nas seções anteriores deste whitepaper. Em vez de apresentar um catálogo prédeterminado de riscos, ele oferece orientações para o desenvolvimento de um sistema de classificação de dados, a fim de gerir os riscos decorrentes de violações à segurança da informação (ou seja, confidencialidade, integridade ou disponibilidade).

Riscos para a pessoa	- Efeito do comprometimento à segurança e à proteção física de uma pessoa, incluindo a ameaça direta ou indireta à vida ou à saúde, independentemente da relação do indivíduo com a organização (pessoal ou terceiros); - Efeito do comprometimento a direitos imateriais individuais (quando o resultado pode ser a perda ou a violação da privacidade, a discriminação, a deterioração da reputação ou outra desvantagem social significativa ou quando uma parte interessada possa ter privação de seus direitos e liberdades ou possa ser impedida de exercer o controle em relação a seus dados pessoais); - Efeito do comprometimento de direitos e interesses materiais individuais (quando o resultado possa ser, por exemplo, roubo ou fraude de identidade, um prejuízo financeiro ou outra desvantagem econômica significativa);
Riscos para as operações de uma organização	- Efeito do comprometimento à operação e à administração efetiva da organização e de seus processos; - Efeito do comprometimento ao processo de tomada de decisão interno livre e independente e às investigações (internas);

Riscos para os ativos ou para os interesses comerciais de uma organização	- Risco de prejuízo financeiro para a organização; efeito do comprometimento dos interesses financeiros da organização ou os de outras partes envolvidas; - Efeito do comprometimento dos sócios da organização, até mesmo da informação trocada com terceiros sob uma expectativa de confidencialidade; - Efeito do comprometimento da informação que abrange o privilégio legal; - Efeito do comprometimento da organização em negociações comerciais ou políticas; - Risco para a reputação, estabilidade ou segurança da organização;
Risco para a segurança nacional, a ordem pública ou as relações exteriores	- Efeito do comprometimento à segurança nacional e à capacidade de defesa (incluindo as questões tecnológicas e econômicas relacionadas com a segurança nacional) ou prejuízo às operações ou atividades de segurança; - Efeito do comprometimento ao exercício das relações exteriores (incluindo a informação de governos estrangeiros); - Efeito do comprometimento à ordem pública e ao funcionamento das autoridades de segurança. - Efeito do comprometimento à informação sobre vulnerabilidades ou capacidades de sistemas, instalações, infraestruturas, projetos, planos ou serviços de proteção relacionados com a segurança nacional; - Efeito do comprometimento à infraestrutura e à proteção da informação; - Efeito do comprometimento aos interesses administrativos ou jurídicos, incluindo uma investigação ou um julgamento; - Efeito do comprometimento à confiança pública da organização e de suas operações.

Fontes e exemplos:

RGPD, ISO/IEC, NIST, CPI, lei de segurança nacional

(Estados Unidos, Estônia e países da OTAN/UE)[11].

11 https://www.valisluureamet.ee/nsa/tables.html

— CLASSIFICAÇÃO —
DE DADOS

OEA | Mais direitos para mais pessoas

aws

– CLASSIFICAÇÃO –
DE DADOS

White paper series
Publicação 6

2019