

PROJETO DE RESOLUÇÃO N.º 1498/XIII/3.^a

Política geral de segurança da informação da Assembleia da República

A Assembleia da República reconhece que, independentemente do suporte, a informação é um ativo indispensável à sua atividade, sendo fundamental a criação das condições necessárias à sua proteção, com vista a garantir os meios adequados ao cumprimento eficiente das competências do Parlamento.

Entende-se por informação qualquer elemento de conhecimento, oral ou escrito, registado, independentemente do meio e do autor. Por sua vez, um documento é qualquer informação registada, independentemente da sua forma física ou das suas características.

A Assembleia da República, enquanto órgão de soberania, produz informação necessária à prossecução da sua atividade legislativa e fiscalizadora, a qual, na sua maioria, é dotada de interesse histórico, pelo que a respetiva segurança se deve manter durante todo o seu ciclo de vida.

Devem, assim, ser adotadas regras e procedimentos específicos para a conservação da informação em qualquer suporte, tendo também de ser adotadas medidas referentes ao seu manuseamento, tratamento, armazenamento, acesso e divulgação.

O constante aumento do volume de informação implica que se mantenha a sua integridade e autenticidade, através de um sistema de gestão documental adequado ainda a garantir a sua disponibilidade. O número dos sistemas de gestão da informação incrementa a complexidade e as vulnerabilidades em matéria de segurança, o que implica que, para além dos princípios desenvolvidos nesta Política Geral de Segurança da Informação, sejam definidas e implementadas políticas e procedimentos específicos que desenvolvam e detalhem cada uma das suas vertentes.

Assim, a Assembleia da República resolve, nos termos do n.º 5 do artigo 166.º da Constituição da República Portuguesa, o seguinte:

Artigo 1.º

Objeto

A presente resolução regula a política geral de segurança de informação da Assembleia da República.

Artigo 2.º

Objetivos da política de segurança de informação

1. A segurança da informação tem como principais objetivos garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento do órgão de soberania.
2. A integridade consiste na capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados.
3. A autenticidade consiste na manutenção da fiabilidade da informação desde o momento da sua produção e ao longo de todo o seu ciclo de vida.
4. A disponibilidade refere-se à possibilidade de acesso aos dados, quando necessário.
5. A confidencialidade refere-se à capacidade de proteger os dados daqueles que não estão autorizados a consultá-los, não impedindo o acesso aos mesmos, em tempo útil, de pessoas autorizadas.

6. Para o cumprimento destes objetivos, a Assembleia da República, em conformidade com a legislação e normativos em vigor em matéria de segurança da informação, compromete-se a adotar as melhores práticas nacionais e internacionais.

Artigo 3.º

Âmbito da política de segurança da informação

1. A política de segurança da informação aplica-se a todas as entidades individuais e coletivas que interagem com a informação sob a responsabilidade da Assembleia da República, designadamente Deputados, dirigentes e funcionários parlamentares, pessoal que desempenha funções nos Gabinetes e nos Grupos Parlamentares, bem como prestadores de serviços externos e entidades que utilizam as instalações e meios da Assembleia da República, doravante designados “utilizadores”.
2. A presente política aplica-se a toda a informação sob a responsabilidade da Assembleia da República, independentemente do suporte de registo: eletrónico, papel, audiovisual ou outros.
3. Além do acesso adequado à informação necessária para o desempenho das suas funções, todos os utilizadores devem ter conhecimento desta política, sendo-lhes exigido o respeito pelos controlos de segurança implementados.

Artigo 4.º

Conteúdos da política de segurança da informação

1. A política de segurança da informação da Assembleia da República consiste na proteção da informação produzida, armazenada, processada ou transmitida contra a perda de integridade, autenticidade, disponibilidade e confidencialidade.
2. A Assembleia da República compromete-se a desenvolver políticas e procedimentos específicos que respeitem as normas internacionais de referência, auditáveis, que definem os requisitos para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), abrangendo, nomeadamente as áreas previstas nas normas ISO 27001, ISO 27002 e ainda no Regulamento Geral de Proteção de Dados Pessoais, no que respeita a:
 - a) Recursos Humanos: **i.** Assegurar que todos os utilizadores conhecem, entendem e cumprem as responsabilidades na área da segurança da informação em conformidade com as suas funções. **ii.** Assegurar que os interesses da Assembleia da República e dos utilizadores são protegidos como parte do processo de início, mudança ou cessação de funções.
 - b) Gestão da Informação: **i.** Identificar a informação da Assembleia da República e definir as responsabilidades pela sua proteção. **ii.** Definir a política de classificação de segurança, assegurando que a informação receba um nível adequado de proteção de acordo com o seu valor, sensibilidade, criticidade, requisitos legais e riscos a que possa estar sujeita. **iii.** Definir a política de uso aceitável que deve conter regras para a utilização dos recursos da Assembleia da República, ficando o uso destes condicionado à concordância expressa por parte de cada utilizador. **iv.** Definir os procedimentos para a gestão dos suportes de armazenamento e salvaguarda da informação. **v.** Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação.

- c) **Gestão de Acessos:** **i.** Assegurar a gestão e o controlo dos acessos às instalações da Assembleia da República, ao sistema informático e à informação, responsabilizando os utilizadores pela proteção das suas credenciais de acesso e assegurando a intransferibilidade dos direitos atribuídos. **ii.** Gerir a divulgação da informação.
- d) **Segurança Física e Ambiental:** **i.** Proteger as informações, equipamentos e instalações físicas da Assembleia da República de acesso não autorizado, dano, interferência, perda, furto ou roubo. **ii.** Monitorizar e controlar o ambiente das instalações. **iii.** Definir procedimentos que assegurem a salvaguarda dos suportes físicos.
- e) **Gestão do Sistema Informático:** **i.** Garantir a operação e proteção, segura e correta, dos recursos de processamento da informação. **ii.** Registrar e monitorizar eventos e gerar evidências. **iii.** Analisar, controlar, mitigar e eliminar as vulnerabilidades. **iv.** Criar mecanismos que permitam controlar e auditar a conformidade das operações com as políticas de segurança da informação. **v.** Garantir a segurança da informação transmitida dentro da organização e com quaisquer entidades externas. **vi.** Assegurar o uso efetivo e adequado da criptografia para proteger a integridade, autenticidade e integridade da informação.
- f) **Gestão dos Incidentes de Segurança:** Definir as responsabilidades e os procedimentos a adotar para reagir de forma apropriada perante as fragilidades e incidentes que coloquem em risco a segurança da informação, garantindo o seu registo e prevendo um processo de melhoria contínua e revisão periódica dos processos de gestão de incidentes.

- g) **Gestão da Continuidade de Negócio:** **i.** Garantir que, após a ocorrência de desastres ou falhas de segurança (resultantes por exemplo de desastres naturais, acidentes, falhas de equipamentos ou ações intencionais), seja possível manter um nível de funcionamento aceitável até se retornar à situação normal. **ii.** Prever e implementar um plano de continuidade de negócio.
- h) **Conformidade Legal:** Assegurar o cumprimento das obrigações legais, estatutárias, regulamentares e contratuais, bem como de quaisquer requisitos de segurança.
- i) **Proteção de Dados Pessoais:** **i.** Identificar e localizar a informação que contem dados pessoais, o seu propósito, risco e valor. **ii.** Garantir que os procedimentos a estabelecer sejam adequados às obrigações de proteção de dados pessoais decorrentes, nomeadamente, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção de dados pessoais, e legislação nacional aplicável.

Artigo 5.º

Princípios aplicáveis

As políticas de segurança da informação da Assembleia da República, quer na sua definição, quer na sua concretização diária, devem orientar-se pelos seguintes princípios:

- a) Garantia de proteção - a informação é um recurso crítico para o eficaz desenvolvimento de todas as atividades da Assembleia da República, sendo assim fundamental garantir a sua adequada proteção, nas vertentes de integridade, autenticidade, disponibilidade e confidencialidade;

- b) Sujeição à lei – tanto a política como as tarefas executadas no seu âmbito estão sujeitas à legislação aplicável, bem como às normas e regulamentos internos aprovados pelas entidades competentes;
- c) Necessidade de acesso - o acesso à informação deve restringir-se, exclusivamente, às pessoas que tenham necessidade de a conhecer para cumprimento das suas funções e tarefas;
- d) Transparência - deve assegurar-se a transparência, conjugando o dever de informar com a fixação, de forma clara, das regras e procedimentos a adotar para a segurança da informação sob a responsabilidade deste órgão de soberania.
- e) Proporcionalidade - as atividades impostas pela segurança da informação devem ser proporcionais aos riscos a mitigar e limitadas ao necessário, minimizando a entropia no regular funcionamento da Assembleia da República;
- f) Obrigatoriedade de cumprimento - as políticas e procedimentos de segurança definidos devem ser integrados nos processos de trabalho e a execução das tarefas diárias deve ser pautada pelo seu cumprimento;
- g) Responsabilidades - as responsabilidades e o papel das entidades intervenientes na segurança da informação deverão ser definidas de forma clara e ser alvo de monitorização e auditoria periódicas;
- h) Informação - todas as políticas e procedimentos específicos devem ser publicitados e comunicados a todos os utilizadores que deles necessitem para o desempenho das suas funções e tarefas;

- i) Formação - deve ser planeado, aprovado e executado um plano de formação e de divulgação que incida sobre o domínio da segurança da informação e sobre as políticas e procedimentos específicos adotados neste âmbito;
- j) Avaliação do risco - deve ponderar-se a necessidade de proteção da informação em função da sua relevância e das ameaças que sob ela incidem. A avaliação do risco deve identificar, controlar e eliminar os diversos tipos de ameaças a que a informação se encontra sujeita. Os níveis de segurança, custo, medidas, práticas e procedimentos devem ser apropriados e proporcionais ao valor e ao nível de confiança da informação;
- k) Comunicação, registo e ponto de contacto único - todos os incidentes de segurança, bem como as fragilidades, têm de ser objeto de comunicação imediata e registo de forma a proporcionar uma resposta célere aos problemas. O processo de registo deve prever a identificação de um ponto único de contacto para onde devem ser canalizados todos os relatos;
- l) Sanções - a não observância das disposições de segurança da informação que se encontrem em vigor, será considerada como infração às normas e regulamentos internos e, como tal, será sujeita a medidas corretivas apropriadas de acordo com a legislação e normativos aplicáveis, ou que venham a ser estabelecidos para o efeito.

Artigo 6.º

Atribuição de responsabilidades

1. Todos os utilizadores estão obrigados a cumprir e a fazer cumprir a presente política de segurança da informação e têm o dever de zelar pela sua proteção e de proceder à comunicação de qualquer evento que provoque, ou possa provocar, uma quebra de segurança da informação.

2. O Presidente da Assembleia da República é o primeiro responsável pela implementação e controlo do Sistema de Gestão da Segurança da Informação da Assembleia da República, competindo-lhe aprovar os documentos “Política de Classificação da Informação”, “Política de Proteção de Dados Pessoais” e outras Políticas estabelecidas na sequência da Resolução aprovada pela Assembleia da República sobre a “Política Geral de Segurança da Informação”, ouvindo previamente o Conselho de Administração e a Conferência de Líderes.
3. O Presidente da Assembleia da República deve também garantir que sejam atribuídas as autoridades e responsabilidades para as funções da gestão da informação e para o cumprimento das obrigações legais aplicáveis.
4. O Secretário-Geral valida e submete à aprovação superior as propostas relacionadas com a segurança da informação, promove a disponibilização dos meios humanos, financeiros e materiais necessários à gestão da segurança da informação.
5. Os Deputados devem cumprir e fazer cumprir as políticas, regulamentos e procedimentos relativos à segurança da informação.
6. Os dirigentes dos serviços, ou equiparados, devem colaborar com o Administrador de Segurança na definição, implementação e controlo de aplicação das políticas e procedimentos de segurança que vierem a ser definidos para a sua área de competência e são responsáveis por garantir o seu cumprimento por parte dos recursos humanos e materiais sob sua responsabilidade.
7. Os funcionários parlamentares e o pessoal que desempenha funções nos Grupos Parlamentares devem cumprir e fazer cumprir as políticas, regulamentos e procedimentos relativos à segurança da informação.
8. Os colaboradores de terceiras entidades que prestam serviço na Assembleia da República, ou que utilizam as suas instalações e meios, ou ainda os trabalhadores ou empresas contratadas pela Assembleia da República, devem cumprir os normativos e procedimentos estipulados na política de segurança da informação da Assembleia da República.

9. O Administrador de Segurança é responsável pelas tarefas de implementação, manutenção e operação do sistema, devendo assegurar, designadamente, a gestão de incidentes de segurança, a execução periódica do processo de avaliação dos riscos de segurança, a elaboração dos planos de formação relativos à segurança da informação e a prestação de apoio às equipas técnicas das especialidades integradas nos processos abrangidos pelo sistema.
10. O Encarregado da Proteção de Dados é responsável pela aplicação e controlo da legislação relativa à proteção de dados pessoais, nomeadamente nos termos do já referido Regulamento Europeu de Proteção de Dados Pessoais, sendo designado com base nos seus conhecimentos especializados no domínio do Direito e das práticas de proteção de dados, bem como na capacidade para desempenhar as funções exigidas pelo Regulamento.

Artigo 7.º

Implementação

1. Devem ser implementadas as alterações necessárias às políticas específicas para garantir o cumprimento integral da Política definida, exceto quando forem identificadas razões técnicas ou de negócio que inviabilizem a implementação das alterações referidas. Estas exceções devem ser documentadas e acompanhadas de proposta de medidas que possam, entretanto, mitigar os riscos em causa.
2. De igual modo, sempre que uma ação de renovação tecnológica não conduza ao cumprimento integral da Política, deve ser mantida a identificação deste sistema como uma exceção documentada, com a salvaguarda de que nenhuma alteração deve conduzir a uma situação de risco acrescido comparativamente à situação anterior.

Artigo 8.º
Entrada em vigor e revisão

A presente política geral de segurança da informação entra em vigor na data da sua publicação e será revista sempre que seja considerado necessário.

Palácio de São Bento, 12 de abril de 2018

O PRESIDENTE DA ASSEMBLEIA DA REPÚBLICA

(Eduardo Ferro Rodrigues)