



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

Consulta Prévia n.º

002/ASI/EPD/2020

CADERNO DE ENCARGOS

Plataforma SGSI-AR e SGPD-AR

Índice

1	Enquadramento.....	1
2	OBJETO	2
3	ESPECIFICAÇÃO DAS PRINCIPAIS FUNCIONALIDADES DO SGSI-AR	3
3.1	Módulo SGSI-AR.....	3
3.2	Módulo de Gestão Documental	3
3.3	Gestão de Incidentes	4
3.4	Gestão de Auditorias	5
3.5	Gestão do Risco	6
3.6	Gestão de inquéritos/questionários (SGSI-AR e SGPD-AR)	6
3.7	Awareness e E-Learning (SGSI-AR e SGPD-AR)	7
4	ESPECIFICAÇÃO DAS PRINCIPAIS FUNCIONALIDADES DO SGPD-AR	8
4.1	Gestão dos registos de atividades de tratamento.....	8
4.2	Data mapping (inventário e mapeamento de ativos/dados pessoais)	8
4.3	Avaliação de Impacto de Privacidade dos Dados (AIPD)	9
4.4	Violação de Dados Pessoais.....	9
4.5	Interação com autoridade de controlo.....	10
4.6	Exercício de Direitos pelos Titulares dos dados pessoais.....	10
4.7	Outras funcionalidades.....	10
5	ESPECIFICAÇÕES GERAIS DO SISTEMA	11
5.1	Breve caracterização do sistema informático da AR	11
5.2	Requisitos de instalação do sistema.....	11
5.3	Requisitos de configuração do sistema	12
5.4	Requisitos técnicos	12
5.5	Requisitos de monitorização	12
6	LOCAL DA PRESTAÇÃO DOS SERVIÇOS	12
7	PRAZO MÁXIMO DE IMPLEMENTAÇÃO DA SOLUÇÃO	12
8	PREÇO, CONDIÇÕES DE PAGAMENTO E FATURAÇÃO.....	13
9	CRITÉRIO DE ADJUDICAÇÃO	13
10	FORMAÇÃO	13
11	LICENCIAMENTO , DIREITOS DE AUTOR E PROPRIEDADE INTELECTUAL	14
12	MANUTENÇÃO	14
13	SIGILO	14
14	REQUISITOS DE PROTEÇÃO DE DADOS	15
15	REQUISITOS DE SEGURANÇA DA INFORMAÇÃO	16
16	PENALIDADES	18
17	GESTOR DO CONTRATO.....	19
18	CASOS FORTUITOS OU DE FORÇA MAIOR.....	19
19	PATENTES LICENÇAS E MARCAS	19
20	CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO	19
21	RESOLUÇÃO DO CONTRATO.....	20
22	GARANTIA.....	20
23	LEGISLAÇÃO APLICÁVEL.....	20

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

1 Enquadramento

Os processos de implementação do Sistema de Gestão da Segurança da Informação (SGSI) e do Sistema de Gestão da Proteção de Dados (SGPD) da Assembleia da República (AR) compreendem o desenvolvimento das seguintes atividades: Diagnóstico; Planeamento; Implementação e Operação; Monitorização e Avaliação; e Melhoria Contínua.

1.1. Implementação do SGSI-AR

A implementação do SGSI-AR, iniciada no segundo semestre de 2019, tem como objetivo estabelecer a sistematização de controlos de segurança da informação baseada na norma ISO/IEC 27001: 2013 e vai ser efetuada em duas fases:

FASE 1

- **DIAGNÓSTICO DA SITUAÇÃO ATUAL:** consiste na compreensão do negócio, na determinação do *gap* entre os requisitos standard e as práticas atuais;
- **PLANEAMENTO DO SISTEMA:** compreende a definição de políticas, objetivos, processos e procedimentos para a gestão de segurança da informação, bem como do *roadmap* para a implementação;

FASE 2

- **IMPLEMENTAÇÃO E OPERAÇÃO:** consiste em implementar e operacionalizar a política de segurança da informação através de controlos e medidas de segurança da informação, de processos e de procedimentos;
- **MONITORIZAÇÃO E AVALIAÇÃO:** inclui a realização de controlos e práticas necessárias para avaliar a eficiência e a eficácia do SGSI-AR, com o objetivo de melhorar o desempenho do sistema;
- **MANUTENÇÃO E MELHORIA:** compreende a execução de ações corretivas e preventivas com base nos resultados da avaliação, com o objetivo de assegurar a melhoria contínua do SGSI-AR.

1.2. Implementação do SGPD-AR

A implementação do SGPD-AR, iniciada no primeiro semestre de 2020 tem como objetivo adequar o tratamento de dados pessoais pela Assembleia da República à legislação aplicável, designadamente o RGPD, dotando-a dos mecanismos de controlo que garantam a conformidade e a respetiva demonstração (seguindo igualmente as Normas ISO, particularmente as 27701 e 29134), e também vai ser efetuado em duas fases:

FASE 1

- **DIAGNÓSTICO DA SITUAÇÃO ATUAL:** Compreende as tarefas de Preparação e Levantamento (auditoria à situação existente, procedendo-se ao inventário e mapeamento dos dados à guarda da Assembleia da República); Avaliação da conformidade (avaliação da maturidade das operações de tratamento com base no risco e apurar as desconformidades com o RGPD) e recomendações;



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- **PLANEAMENTO DO SISTEMA:** Compreende a definição do Plano de Implementação (modelo de organização do SGPD-AR - que contemple as funções, autoridades e responsabilidades, mas também as políticas, processos e procedimentos – e o planeamento das ações a adotar, bem como a definição de um Programa de Formação).

FASE 2

- **IMPLEMENTAÇÃO E OPERAÇÃO:** consiste na aplicação do plano aprovado na primeira fase, na parametrização e operacionalização do sistema de gestão para atividades de tratamento, garantir os direitos dos titulares e demonstrar evidências
- **MONITORIZAÇÃO E AVALIAÇÃO:** inclui a realização de auditorias, análise de indicadores dos processos, de riscos e de controlos de proteção de dados controlos e práticas necessárias para avaliar a eficiência e a eficácia do SGPD-AR
- **MANUTENÇÃO E MELHORIA:** compreende a execução de ações corretivas e preventivas com base nos resultados da avaliação, com o objetivo de assegurar a melhoria contínua do SGPD-AR.

2 OBJETO

Para melhorar a eficácia e a eficiência na gestão das áreas de Administração de Segurança da Informação e de Encarregado de Proteção de Dados da AR, foi considerada a necessidade de adquirir uma plataforma de software que permite a gestão de forma estruturada da Documentação (manuais, planos e políticas operacionais, procedimentos, processos, modelos, relatórios e a declaração de aplicabilidade); de Incidentes de Segurança da Informação; de Auditorias ISO 27001; do Risco; de Inquéritos, de Questionários, de *Awareness* e E-learning, que estão a ser desenvolvidos no âmbito da implementação do SGSI-AR e do SGPD-AR.

O presente Caderno de Encargos tem por objeto a aquisição de serviços de desenvolvimento de uma aplicação para a gestão integrada dos sistemas de Segurança da Informação e de Proteção de Dados da Assembleia da República. A plataforma a desenvolver deve satisfazer os requisitos que se seguem.

Requisitos a considerar no módulo SGSI-AR:

- a) Gestão do SGSI-AR propriamente dito
- b) Gestão Documental
- c) Gestão de Incidentes
- d) Gestão de Auditorias ISO 27001
- e) Gestão de Risco
- f) Gestão de inquéritos/questionários
- g) *Awareness* e *E-Learning* (SGSI-AR e SGPD-AR)

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

Requisitos a considerar no módulo SGPD-AR:

- a) Gestão dos registos de atividades de tratamento
- b) *Data mapping* (inventário e mapeamento de ativos/dados pessoais)
- c) Avaliação de Impacto de Privacidade dos Dados (AIPD)
- d) Violação de Dados Pessoais
- e) Interação com autoridade de controlo
- f) Exercício de Direitos pelos Titulares dos dados pessoais
- g) Outras funcionalidades (Gestão Documental e Gestão de Auditorias)

Especificações gerais do sistema

- a) Breve caracterização do sistema informático da AR
- b) Requisitos de configuração
- c) Requisitos técnicos
- d) Requisitos de monitorização

3 ESPECIFICAÇÃO DAS PRINCIPAIS FUNCIONALIDADES DO SGSI-AR

3.1 Módulo SGSI-AR

Este módulo abrange a avaliação do risco da segurança da informação e inclui a definição, implementação e avaliação da eficácia dos controlos para tratamento dos riscos. Deve integrar todos os ativos de sistemas e tecnologias de informação e comunicação relevantes para os processos de operação da organização dentro do âmbito do SGSI-AR.

O Fluxograma do Processo de Gestão de Segurança da Informação deve contemplar as seguintes atividades:

1. Realizar a avaliação de risco de segurança da informação;
2. Documentar os controlos de segurança da informação;
3. Aprovar os controlos de segurança da informação;
4. Implementar os controlos de segurança da informação;
5. Avaliar a eficácia dos controlos de segurança da informação;

3.2 Módulo de Gestão Documental

O módulo de Gestão Documental deve permitir a gestão centralizada de todo o repositório documental do SGSI-AR e deve disponibilizar as seguintes funcionalidades:

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- Criação de estrutura de arquivo com codificação específica para a gestão de documentos no âmbito da ISO 27001, tais como Manuais, Planos, Políticas Operacionais, Procedimentos, Processos, Modelos, Relatórios, SoA-Declaração de Aplicabilidade e Outros;
- *Workflows* personalizáveis com a possibilidade de gestão e parametrização do fluxo necessário para aprovação de documentos de acordo com as competências das Unidades Orgânicas da AR;
- Gestão e controlo de acessos e permissões de acesso;
- Classificação de documentos e registos;
- Possibilidade de publicação e distribuição de documentos depois de aprovados;
- Possibilidade de associar referência a um documento através de links;
- Controlo das etapas de elaboração de um documento até à sua aprovação final;
- Controlo do estado dos documentos em vigor, revogados e notificação das tarefas aos intervenientes;
- Possibilidade de gerar relatórios que permitem visualizar o mapa de controlo documental, com listagem de toda a documentação no âmbito do SGSI-AR.

3.3 Gestão de Incidentes

O módulo de Gestão de Incidentes deve permitir a gestão da informação recolhida no âmbito do Processo de Gestão de Incidentes de Segurança de Informação que consiste na deteção, reporte, avaliação, resposta e comunicação de ocorrências suscetíveis de serem classificadas como incidentes de segurança de informação. Deve disponibilizar as seguintes funcionalidades:

- Registo, tratamento e acompanhamento de incidentes, com a possibilidade de enviar notificações, de anexar evidências e todos os documentos necessários para tratamento de incidentes;
- Gestão e controlo de acessos e permissões de acesso aos registos e anexos;
- Análise de ocorrências em termos de avaliação de risco para a AR de forma a ter noção da sua criticidade ou oportunidade;
- Elaboração de relatório em formato Excel e PDF para análise ao mais alto nível, contendo toda a informação associada ao registo do incidente;
- O Fluxograma do Processo de Gestão de Incidentes deve contemplar as seguintes atividades:
 1. Registrar o incidente de segurança
 2. Analisar Incidente de Segurança da Informação
 3. Conter/resolver incidente de segurança da informação
 4. Efetuar a recolha e arquivo de evidências
 5. Erradicar o incidente e recuperar os ativos de informação afetados

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

6. Informar às partes interessadas e documentar lições aprendidas
7. Fechar incidente de segurança da informação
8. Validar o fecho do incidente de segurança da informação
9. Rever incidentes de segurança da informação

3.4 Gestão de Auditorias

O módulo de Gestão de Auditorias deve permitir o registo e gestão de informação sobre as auditorias planeadas e realizadas, de forma a assegurar a melhoria contínua do SGSI-AR. Deve disponibilizar as seguintes funcionalidades:

- Gestão da bolsa de auditores e referenciais normativos associados;
- Possibilidade de construção de *checklist* para realização de auditorias internas e externas;
- Elaboração e distribuição do relatório da auditoria com controlo de acessos;
- *Checklists* personalizáveis e à medida (ISO 27001, ISO 27701, RGPD, etc.);
- Registo do resultado da auditoria e constatações;
- Notificação dos intervenientes;
- Emissão de Relatórios e possibilidade de exportação para Excel dos programas de auditoria;
- Registo de ações para tratamento das constatações ou de qualquer tipo de ações que possam implicar um tratamento mais detalhado pela parte da AR;
- Efetuar o planeamento e acompanhamento de todos os planos de ações inerentes a qualquer atividade da AR, com controlo de acessos
- Notificação automática aos intervenientes nas várias fases do plano e conforme as Unidades Orgânicas intervenientes e prazos a cumprir;
- Anexar ficheiros com informação de suporte, pareceres, orçamentos, etc.;
- Acompanhamento e pontos de situação das ações: fase em que se encontra e respetivo responsável; taxa de execução por ação; taxa de execução global;
- Extrair Relatórios PDF com toda a informação associada às ações, designadamente análise de desvios de custos, desvios de tempos.

O Fluxograma do Processo de Gestão de Auditorias deve contemplar as seguintes atividades:

1. Preparar/atualizar Programa de Auditorias
2. Aprovar Programa de Auditorias
3. Publicar e comunicar Programa de Auditorias
4. Planear Auditoria

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

5. Realizar Reunião de Abertura
6. Realizar Auditoria
7. Preparar Relatório de Auditoria
8. Realizar Reunião de Fecho

3.5 Gestão do Risco

O módulo de Gestão do Risco deve permitir o registo e gestão de informação sobre a segurança da informação, definindo a periodicidade de realização da avaliação do risco, os critérios a considerar e as consequentes ações de tratamento.

Estão abrangidos todos os ativos de sistemas e tecnologias de informação e comunicação relevantes considerados como críticos para as atividades da AR, tais como a própria informação, a estrutura organizacional, o hardware, o software, as redes, as pessoas e as instalações físicas. Deve disponibilizar as seguintes funcionalidades:

- Parametrização da fórmula de cálculo do nível do risco ou potencial dos benefícios de uma oportunidade;
- Identificação das fontes de risco e oportunidades, seus efeitos potenciais;
- Identificação de tipo de causas e resposta ao respetivo risco/oportunidade;
- Aprovação e comunicação do nível do risco/potencial dos benefícios de uma oportunidade;
- Anexar ficheiros ao registo do risco/oportunidade com informação de suporte;
- Exportar a matriz de risco para Excel e elaborar relatórios em PDF.

O Fluxograma do Processo de Gestão do Risco deve contemplar as seguintes atividades:

1. Estabelecer o contexto
2. Identificar os riscos
3. Estimar os riscos
4. Definir o tratamento dos riscos
5. Aprovar formalmente o tratamento e aceitação dos riscos.

3.6 Gestão de inquéritos/questionários (SGSI-AR e SGPD-AR)

O módulo de Gestão de inquéritos/questionários deve permitir a criação de inquéritos e questionários online com total flexibilidade de configuração das questões e tratamento das respostas. Deve disponibilizar as seguintes funcionalidades:

- Criação de um número ilimitado de questionários em simultâneo;

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- Criação de questionários anónimos;
- Possibilidade de diversos tipos de questões disponíveis (resposta única, resposta múltipla, matriz, resposta aberta, texto descritivo, resposta percentagem, resposta data, etc.);
- Notificação aos participantes convidados a responder ao questionário;
- Consulta individual das respostas;
- Análise estatística dos resultados a qualquer momento;
- Permitir a exportação de resultados para Excel e PDF;
- Disponibilização de portal de acesso externo que permita o envio e preenchimento de questionários a utilizadores externos (fornecedores e parceiros).

3.7 *Awareness e E-Learning* (SGSI-AR e SGPD-AR)

O módulo de *Awareness e E-Learning* deve permitir avaliar o grau de maturidade dos utilizadores nas áreas de cibersegurança, *compliance* (RGPD, segurança da informação) e deve disponibilizar as seguintes funcionalidades:

- Permitir a criação de *Quizzes* pelo gestor da plataforma
- Associar *Quizzes* por perfil de utilizadores e da estrutura orgânica da AR
- Definir tempo limite para os desafios
- Ser possível fazer questões apelativas (com imagens, vídeos curtos, etc.).
- Agrupar questões por áreas de conhecimento, tais como:
 - cibersegurança - nível I - redes
 - cibersegurança - nível II - Engenharia Social
 - cibersegurança - nível III - *Phishing*
 - RGPD - Desafios de conformidade para parceiros
 - RGPD - Desafios de conformidade para colaboradores
- Ser possível gerar aleatoriamente questões para *Quizzes* nos seguintes tópicos de cibersegurança:
 - Segurança de dispositivos móveis
 - Recomendações para smartphones
 - Passwords
 - Navegação segura
 - Correio eletrónico
 - Guia de ciberhigiene informática
 - VPN
 - Boas praticas em viagem

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- Rede *Guest*
- Formatação de *pen-drives*
- Ter as avaliações por grupos e Unidades Orgânica da estrutura orgânica da AR
- Ter indicadores em forma gráfica

4 ESPECIFICAÇÃO DAS PRINCIPAIS FUNCIONALIDADES DO SGPD-AR

4.1 Gestão dos registos de atividades de tratamento

Este módulo deve permitir à AR manter o registo de todas as atividades de tratamento de dados pessoais sob sua responsabilidade, devendo disponibilizar as seguintes funcionalidades:

- Identificação do responsável pelo tratamento dos dados
- Finalidades do tratamento dos dados
- Categorias dos titulares dos dados
- Categorias de destinatários
- Transmissão de dados para países terceiros ou organizações internacionais,
- Medidas de salvaguarda no envio para países terceiros
- Prazos previstos para o apagamento
- Descrição geral das medidas técnicas
- Exportações em Excel e PDF
- *Dashboard* gráfico sobre os RATs

4.2 *Data mapping* (inventário e mapeamento de ativos/dados pessoais)

Este módulo deve permitir inventariar exaustivamente todas as categorias de dados pessoais tratados, descrevendo os respetivos fluxos, e registar o cumprimento dos requisitos legais dos tratamentos.

Deve disponibilizar as seguintes funcionalidades:

- Gestão de dados pessoais/categorias de dados
- Descrição de fluxos por ciclo de vida dos dados pessoais
- Base legal para o tratamento dos dados (art.º 6)
- Tratamento de categorias especiais de dados pessoais (art.º 9)
- Legítimo interesse para o tratamento de dados
- Avisos para o exercício dos direitos disponibilizados aos titulares de dados
- Decisões automatizadas (*Profiling*)
- Origem dos dados pessoais
- Anexar os ficheiros dos registos de consentimento
- Repositórios (físicos ou digitais) onde os dados se encontram armazenados
- Exportações em Excel e PDF

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- *Dashboard* gráfico dos inventários de dados pessoais

4.3 Avaliação de Impacto de Privacidade dos Dados (AIPD)

Este módulo deve permitir a preparação e realização de avaliações de impacto sobre a privacidade, nos termos do artigo 35.º do RGPD, devendo, para tanto, disponibilizar as seguintes funcionalidades:

- Realizar AIPD antes de iniciar o tratamento, durante ou em alterações ao tratamento e ciclo de vida do tratamento de dados pessoais
- Registrar a necessidade da AIPD
- Descrever o fluxo de informações (operações de tratamento previstas, finalidades, contexto, objetivos)
- Auscultação de partes interessadas
- Avaliar necessidade e proporcionalidade
- Identificar privacidade e riscos relacionados
- Identificar medidas para reduzir riscos
- Fecho e validação de resultados
- Integrar os resultados no plano do projeto
- Exportações em Excel e PDF
- *Dashboard* gráfico dos inventários de dados pessoais com níveis de risco

4.4 Violação de Dados Pessoais

Este módulo deve permitir gerir as situações em que ocorram violações de dados, desde que são reportadas até às notificações aos titulares e à entidade de controlo, devendo, para tanto, disponibilizar as seguintes funcionalidades:

- Registrar violações sobre dados pessoais
- Notificação à autoridade de controlo
- Auscultação de partes interessadas
- Pedidos de parecer
- Natureza da violação de dados pessoais
- Categoria e quantidade de titulares afetados
- Número aproximado de registos de dados pessoais em causa
- Identificação do DPO, (nome e contactos)
- Consequências prováveis (efeitos)
- Medidas adotadas ou propostas pelo responsável pelo tratamento e/ou medidas para atenuar os seus eventuais efeitos negativos
- Repositório de evidências (gravadas de forma encriptada) e com controlo de acessos.
- Exportações em Excel e PDF
- *Dashboard* gráfico

4.5 Interação com autoridade de controlo

Este módulo deve permitir registar e gerir todas as comunicações com a autoridade de controlo, devendo disponibilizar as seguintes funcionalidades:

- Registar todas as interações com as autoridades de controlo (nacionais e internacionais)
- Definir responsabilidades (entre o responsável pelo tratamento/ responsáveis conjuntos/eventuais subcontratantes)
- Finalidades
- Medidas e garantias previstas
- Informações necessárias/solicitadas pela autoridade de controlo
- Exportações em Excel e PDF
- *Dashboard* gráfico

4.6 Exercício de Direitos pelos Titulares dos dados pessoais

Este módulo deve permitir centralizar e gerir de forma integrada o exercício de direitos pelos titulares de dados, garantindo as evidências, e deve disponibilizar as seguintes funcionalidades:

- Centralizar toda a gestão dos exercícios de direitos pelos titulares registados internamente ou externamente (online)
- Análise e delegação automática aos responsáveis dos exercícios de direitos registados (Direito de Acesso, retificação, esquecimento, apagamento, limitação de tratamento, portabilidade, oposição e informação)
- Pesquisas e filtros por situação dos pedidos
- Exportações em Excel e PDF
- *Dashboard* gráfico

4.7 Outras funcionalidades

- a) O SGPD deve dispor de um módulo de Gestão Documental, para gestão centralizada de todo o repositório documental, com base no modelo previsto para o SGSI, mas com funcionalidades adaptadas aos processos de proteção de dados.
- b) O Módulo de Gestão de Auditoria, previsto para o SGSI, deve poder ser adaptado de modo a permitir o registo e gestão de informação sobre as auditorias planeadas e realizadas (tendo em atenção o RGPS e as normas ISO 27701 e 29134, de forma a assegurar a melhoria contínua do SGPD-AR.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

5 ESPECIFICAÇÕES GERAIS DO SISTEMA

5.1 Breve caracterização do sistema informático da AR

- a) A Assembleia da República (AR) dispõe atualmente de uma infraestrutura tecnológica de acordo com a caracterização que se segue:
- Uma rede informática TCP/IP V4, suportada por um sistema de cablagem estruturada (dependendo dos locais pode variar entre categoria 5, 5e e 6) com ligações aos postos de 100/1000Mbit;
 - Plataforma de virtualização VMware (VMware ESXi 6.7) que suporta toda a infraestrutura de servidores;
 - O Diretório de Autenticação da AR baseia-se em Microsoft Active Directory. As permissões de acesso dos utilizadores às aplicações são atribuídas de acordo com grupos de segurança definidos nesta Active Directory.
 - O Forest Level e o Domain Level do domínio é Windows Server 2012 R2. Os servidores de domínio são Windows 2016 64bit.
 - Sistemas operativos Windows Server 2012R2, 2016 e 2019 em 64bit e Linux CentoOS em inglês;
 - Sistema de correio eletrónico baseado em Microsoft Exchange 2013;
 - Motor de base dados SQL Server 2014 64bit, com redundância em Always-On e MariaDB 10.2;
 - Sites web baseados em IIS e Apache/PHP;
- b) A solução a implementar terá que se integrar nesta infraestrutura, utilizando servidores virtuais dedicados.
- c) A plataforma de virtualização utilizada na Assembleia da República é abrangente nos sistemas que suporta. No entanto, a solução proposta deverá integrar-se nos standards atuais do mercado, nomeadamente devendo tirar partido do cluster SQL Server em que foram consolidadas as bases de dados que a Assembleia da República utiliza.

5.2 Requisitos de instalação do sistema

- Sistema operativo do servidor;
- Sistema de Gestão de Base de Dados (SGBD);
- WebServer;
- Linguagem de programação;
- Requisitos para os postos clientes;
- Modalidades de licenciamento.

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

5.3 Requisitos de configuração do sistema

- Sistema de Autenticação deve integrar com a atual *Active Directory* (AD) e permitir a funcionalidade *single sign on*;
- Mapeamento dinâmico da estrutura organizacional da Assembleia da República e entidades associadas;
- Perfis por utilizadores e por grupos;
- Gestão de acessos.

5.4 Requisitos técnicos

- Solução assente em tecnologias WEB;
- Solução compatível e integrável com os sistemas/bases de dados da AR;
- Possibilidade de instalação local, “*on-premises*” e *as-a-service*;
- Possibilidade de exportação de listagens;
- Solução “chave na mão”;
- Licenciamento para aproximadamente 500 utilizadores.

5.5 Requisitos de monitorização

- Monitorização do estado do SGSI-AR;
- Monitorização do estado do SGPD-AR;
- Monitorização do estado da cibersegurança da AR;
- Notificação sobre potenciais riscos e ameaças;
- Alertas gráfico, visual e sonoro de anomalias e não conformidades.

6 LOCAL DA PRESTAÇÃO DOS SERVIÇOS

Os serviços serão executados presencialmente, nas instalações da Assembleia da República, sitas no Palácio de São Bento, 1249-068, Lisboa.

7 PRAZO MÁXIMO DE IMPLEMENTAÇÃO DA SOLUÇÃO

O prazo máximo de implementação não poderá ser superior a 12 semanas.

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

8 PREÇO, CONDIÇÕES DE PAGAMENTO E FATURAÇÃO

- a) Para a prestação dos serviços de desenvolvimento da plataforma de gestão da Segurança da Informação e Proteção de Dados, a Assembleia da República pagará o preço total constante da proposta que não deverá exceder os **25.000,00 € (vinte e cinco mil euros)**, acrescido de IVA à taxa legal em vigor.
- b) Considera-se incluído no valor do projeto todos os custos inerentes ao cumprimento integral dos requisitos descritos no caderno de encargos, bem como eventuais elementos adicionais incluídos na proposta do concorrente.
- c) A faturação e o pagamento serão realizados após a conclusão, entrega e aceitação de toda a solução, por parte da entidade adjudicante.
- d) O pagamento será realizado no prazo de 30 (trinta) dias após a apresentação da fatura correspondente pela entidade adjudicatária, desde que apresentada nos termos adequados à sua liquidação.

9 CRITÉRIO DE ADJUDICAÇÃO

Propõe-se que a adjudicação seja feita nos termos da alínea a) do nº1, do artigo 74º do Código dos Contratos Públicos, ou seja, de acordo com o critério da proposta economicamente mais vantajosa para a AR, determinada pela melhor relação qualidade-preço, mediante aplicação, por ordem decrescente de importância, dos seguintes fatores:

- a) Preço 50%
- b) Equipa de projeto constituída por consultores certificados com os seguintes perfis de competências: (30%)
 - Pelo menos dois consultores certificados em ISO/IEC 27001 (nível Lead Auditor);
 - Pelo menos dois consultores certificados em ISO/IEC 27001 (nível Implementer);
 - Pelo menos um consultor com certificação de Encarregado de Proteção de Dados.
- c) Prazo de desenvolvimento em semanas – 20%.

10 FORMAÇÃO

- a) Os concorrentes deverão considerar a possibilidade de elaborar um plano de formação, a ministrar aos diversos perfis de utilizadores da AR para transmissão do conhecimento técnico e funcional da plataforma, que deverá contemplar todos os aspetos de operação e administração da aplicação, de acordo com as especificações técnicas do SGSI-AR e SGPD-AR.
- b) Deverão ainda contemplar neste plano a disponibilização de manuais em suporte digital para explicação do sistema implementado, funcionalidades disponíveis e processos suportados.
- c) As ações de formação deverão ser desenvolvidas nas instalações da entidade adjudicante.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

11 LICENCIAMENTO , DIREITOS DE AUTOR E PROPRIEDADE INTELECTUAL

- a) A Assembleia da República será titular dos direitos de autor, bem como de outros direitos de propriedade intelectual, relativos aos serviços objeto do procedimento e produtos deles resultantes, desde que produzidos especificamente no âmbito do contrato: código fonte, planos, desenhos, documentação e elementos afins, bem como dos produtos consequentes a todas as ulteriores adaptações que se venham a revelar necessárias.
- b) O Adjudicatário entregará o software e as respetivas fontes e toda a documentação relativa aos trabalhos desenvolvidos no âmbito do Contrato.
- c) A Assembleia da República detém uma licença válida para a utilização de todos os programas adquiridos, no mínimo, enquanto se mantiverem em vigor os serviços de manutenção e de suporte.

12 MANUTENÇÃO

De modo a assegurar a atualização, manutenção e suporte da plataforma, os concorrentes deverão apresentar valores do custo adicional para a manutenção da aplicação em duas modalidades:

- a) Contrato anual de manutenção e suporte;
- b) Pacote de horas de manutenção e suporte.

13 SIGILO

- a) O adjudicatário obriga-se a observar o mais estrito sigilo sobre toda a informação e documentação, técnica e não técnica, relacionada com a atividade da AR ou qualquer outra entidade envolvida na execução do contrato.
- b) A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
- c) O adjudicatário compromete-se a respeitar a confidencialidade sobre todos os dados ou informações disponibilizadas pelo adjudicante, bem como pelas informações de carácter pessoal, funcional ou processual dos Sistemas de Informação da Assembleia da República, não os disponibilizando a quaisquer outras entidades, salvo autorização expressa do adjudicante.
- d) O adjudicatário assume, igualmente, o compromisso de remover e destruir, no final do contrato, todo e qualquer tipo de registo (digital ou em papel) relacionado com os dados analisados e que o adjudicante considere de acesso privilegiado.
- e) O adjudicatário garante que terceiros que envolva na execução dos serviços, respeitam as obrigações de sigilo e confidencialidade constantes nos números anteriores.

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- f) Caso o adjudicatário ou os seus representantes a quem tenha sido transmitida, no todo ou em parte, informação confidencial fiquem legalmente obrigados a revelar algum elemento constante da mesma, por força da lei, de processo judicial ou a pedido de entidade de regulação ou de fiscalização, compromete-se - e fará com que os seus representantes também se comprometam - a avisar de imediato a entidade adjudicante, previamente à divulgação da informação reservada, de modo a que sejam conjuntamente asseguradas quaisquer providências necessárias para manter, dentro do legalmente permitido, a confidencialidade da informação reservada.
- g) Nenhum aviso, comunicado à imprensa, relatório ou aviso público destinado a fins publicitários ou de referência ao objeto do contrato pode ser realizado pelo prestador de serviços sem aprovação escrita prévia da Assembleia da República.
- h) Para além das ações penais, civis e processos disciplinares que ao caso couber, o adjudicatário pagará à entidade adjudicante uma compensação pela divulgação, seja por que meio for, de factos relativos à Assembleia da República, aos Deputados, funcionários ou outros agentes vinculados à entidade pública contratante, num montante calculado pela seguinte fórmula: **C = RMMG x 50**, em que: C – Montante da compensação (em euros) e; RMMG – remuneração mínima mensal garantida em vigor.
- i) O disposto no número anterior não é aplicável em caso de imposição legal ou judicial de comunicação de factos sigilosos, desde que sejam cumpridos os estritos termos e objetivos inerentes à obrigação de comunicação.

14 REQUISITOS DE PROTEÇÃO DE DADOS

- a) Será celebrado um contrato de proteção de dados entre a Assembleia da República e adjudicatário que deverá conter as normas constantes das cláusulas seguintes.
- b) No caso de o Adjudicatário necessitar de aceder a dados pessoais, fá-lo-á exclusivamente na medida do estritamente necessário para integral e adequada prossecução dos fins constantes neste caderno de encargos, e por conta e de acordo com as instruções da Assembleia da República, nos termos da legislação aplicável à proteção de dados pessoais.
- c) O Adjudicatário não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem do contrato, comprometendo-se ainda ao seguinte:
 - i. Respeitar integralmente o disposto na legislação nacional e internacional em vigor relativa à proteção de dados pessoais, e em qualquer outra legislação que a substitua ou venha a ser aplicável a esta matéria, nomeadamente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), e a Lei n.º 58/2019, de 8 de agosto.
 - ii. Cumprir rigorosamente as instruções da Assembleia da República no que diz respeito ao acesso, registo, transmissão ou qualquer outra operação de tratamento de dados pessoais.

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- iii. Tratar os dados pessoais de forma lícita, utilizando-os exclusivamente para as finalidades a que se reporta o Contrato, não podendo ser posteriormente acedidos nem tratados de forma incompatível com tais finalidades.
 - iv. Implementar as medidas técnicas e organizativas para proteger os dados contra destruição acidental ou ilícita, perda acidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
 - v. Comunicar de imediato à Assembleia da República quaisquer reclamações ou questões colocadas pelos titulares dos dados pessoais.
 - vi. Apagar e destruir os dados pessoais tratados quando os mesmos deixarem de ser necessários para a execução do contrato, e sempre em prazo não superior a um ano após a cessação do contrato que esteve na base da licitude do seu tratamento.
 - vii. Sem prejuízo do disposto na alínea seguinte, o Adjudicatário obriga-se a manter os dados pessoais estritamente confidenciais, sendo responsável pela confidencialidade e utilização dos mesmos por parte dos respetivos trabalhadores, outros colaboradores ou subcontratados.
 - viii. Se quaisquer dados se perderem ou forem danificados no âmbito da execução do contrato, por causas imputáveis ao Adjudicatário, este compromete-se a adotar as medidas que forem necessárias com vista à recuperação dos dados, sem quaisquer custos adicionais para a Assembleia da República.
- d) O Adjudicatário obriga-se a ressarcir a Assembleia da República por todos os prejuízos em que este venha a incorrer em virtude da utilização ilegal e/ou ilícita dos dados referidos, nomeadamente por indemnizações e despesas em que tenha incorrido na sequência de reclamações ou processos propostos pelos titulares dos dados, bem como por taxas, coimas e multas que tenha de pagar.

15 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

No âmbito desta prestação de serviços, o adjudicatário obriga-se a cumprir os seguintes requisitos de segurança da informação:

- a) A descrição da informação a ser fornecida/acedida e os métodos para fornecer/aceder a informação;
- b) A classificação da informação fornecida/acedida tem de ser efetuada de acordo com os critérios de classificação de informação estabelecidos na AR;
- c) Os requisitos legais e regulamentares aplicáveis, incluindo a proteção de dados, os direitos de propriedade intelectual, os direitos de autor (copyright) e uma descrição de como vai ser garantido o seu cumprimento;
- d) A obrigação de cada parte contratual de implementar os controlos acordados, incluindo controlos de acesso, avaliação do desempenho, monitorização, gestão de incidentes, e realização de auditorias;

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- e) A lista de funcionários do fornecedor autorizados para aceder ou receber informação da AR ou, em alternativa, os procedimentos/condições estabelecidos para autorizar e remover os privilégios de acesso ou receção de informação da AR;
- f) As políticas operacionais de segurança da informação relevantes para o contrato em causa;
- g) Os requisitos do Processo de Gestão de Incidentes e Pedidos de Serviço da AR e do Processo de Gestão de Incidentes de Segurança da Informação, com destaque para as responsabilidades de notificação e colaboração durante a resolução de incidentes;
- h) Os requisitos de formação e sensibilização necessários para determinados procedimentos e requisitos de segurança da informação (por exemplo, resposta a incidentes ou procedimentos de autorização);
- i) Os regulamentos relevantes para a subcontratação, incluindo os controlos necessários a implementar;
- j) Os acordos com parceiros relevantes, incluindo a pessoa de contacto para questões relacionadas com segurança da informação;
- k) Os requisitos de rastreio, quando considerado necessário, dos funcionários dos fornecedores, tais como a verificação da sua identidade, a informação pessoal e o registo criminal. Estes requisitos incluem ainda as responsabilidades para conduzir os procedimentos de rastreio e notificação, no caso de o rastreio não ser concluído ou se os resultados levantarem dúvidas ou preocupações;
- l) O direito de auditar os processos e controlos do fornecedor;
- m) Os processos a seguir em caso de disputas contratuais;
- n) A obrigação do fornecedor em providenciar informação sobre incidentes de segurança da informação para revisão da AR;
- o) A obrigação do fornecedor em assegurar a monitorização e revisão dos aspetos de segurança da informação relativos às relações com os seus próprios fornecedores (quando aplicável);
- p) A obrigação do fornecedor em assegurar a continuidade de serviço adequada, através de planos de recuperação de desastres que assegurem os níveis de continuidade dos serviços acordados com a AR, no caso de ocorrência de falhas ou desastres;
- q) A obrigação do fornecedor em apresentar periodicamente relatórios sobre a eficiência dos controlos e as medidas estabelecidas para a correção atempada de questões relevantes suscitadas no relatório;
- r) A obrigação do fornecedor em cumprir com os requisitos de segurança da informação da AR (e.g. proteção contra software malicioso; salvaguarda de dados; procedimentos de recuperação de desastres; controlos criptográficos; gestão de vulnerabilidade; gestão de incidentes de segurança da informação; recolha, manutenção e proteção de evidências, incluindo logs e audit trails; autenticação e controlo de acessos).

16 PENALIDADES

- a) No caso de mora ou cumprimento defeituoso das prestações do contrato por parte do adjudicatário, poderá a Assembleia da República interpelar o adjudicatário para cumprir pontualmente as tarefas contratadas, quando tal ainda for possível e se mantenha o interesse na prestação, devendo nesse caso o adjudicatário dar-lhes cumprimento imediato, bem como suportar todos os danos que a Assembleia da República sofra na sequência de tais factos.
- b) Sem prejuízo do disposto no número anterior, e da obrigação de indemnizar por parte do adjudicatário, poderá a Assembleia, aplicar-lhe as seguintes penalidades:
 - i. Pelo atraso no cumprimento do prazo previsto na proposta para efeitos de prestação da totalidade dos serviços objeto do presente procedimento – 5% (por cem) do preço contratual por cada 10 dias de atraso;
 - ii. No caso de incumprimento pelo adjudicatário de outras obrigações decorrentes do presente CE, serão aplicadas as seguintes penalidades diárias por cada prestação em falta de acordo com a seguinte fórmula:

$$“P = V \times A / 500”$$

em que “P” corresponde à penalidade, “V” ao preço total do contrato e “A” o número de dias em atraso no cumprimento integral e satisfatório da prestação.

- c) A aplicação das sanções acima referidas será efetivada a critério da entidade adjudicante, designadamente por desconto no pagamento ou pagamentos subsequentes à verificação do facto que tenha dado origem à penalidade.
- d) As penalidades previstas na presente cláusula não afastam o direito da entidade adjudicante de ser indemnizada, nos termos gerais, quando se verificarem os fundamentos de facto e de direito para o efeito.
- e) O não cumprimento de cláusulas do contrato, quando a sua gravidade o justifique pelos prejuízos acusados à Assembleia da República, poderá constituir fundamento para resolução imediata do contrato, nos termos legalmente aplicáveis.
- f) Na determinação da gravidade do incumprimento a Assembleia da República tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do Adjudicatário e as consequências do incumprimento.
- g) O valor acumulado das sanções pecuniárias não pode exceder 20% do preço contratual, nos termos do nº 2 do artigo 329º, do C.C.P.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

17 GESTOR DO CONTRATO

O contraente público nos termos do artigo 290º-A do CCP designará um gestor do contrato, com a função de acompanhar permanentemente a execução deste.

18 CASOS FORTUITOS OU DE FORÇA MAIOR

- a) Nenhuma das partes pode ser responsável pelo incumprimento ou pelo cumprimento defeituoso das obrigações emergentes do contrato, na estrita medida em que se verifiquem em casos de força maior, sendo considerados casos de força maior as circunstâncias que impossibilitam o cumprimento das obrigações emergentes do contrato, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
- b) A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.
- c) Quando uma das partes não aceite por escrito que certa ocorrência invocada pela outra constitua força maior, cabe a esta fazer prova do mesmo.
- d) A verificação de uma situação de força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas, pelo período de tempo comprovadamente correspondente ao impedimento resultante de força maior.
- e) Caso a impossibilidade de execução do contrato, em resultado de força maior, se prolongue por um período contínuo superior a um mês, qualquer das partes pode proceder à respetiva resolução, mediante comunicação enviada à outra parte, com pelo menos 5 (cinco) dias de antecedência.

19 PATENTES LICENÇAS E MARCAS

- a) São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
- b) Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no ponto anterior, o adjudicatário indemniza-a de todas as despesas que, em consequência haja lugar e de todas as quantias que tenha que pagar, seja a que título for.

20 CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO

- a) O adjudicatário não pode ceder a terceiros, total ou parcialmente, a sua posição contratual, ou qualquer dos direitos e obrigações decorrentes do contrato, nomeadamente subcontratar, sem autorização prévia da entidade adjudicante.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO/ENCARREGADO DE PROTEÇÃO DE DADOS

- b) Para efeitos de obtenção da *supra* referida autorização, deverá o adjudicatário observar o previsto sobre esta matéria no artigo 318.º do Código dos Contratos Públicos.

21 RESOLUÇÃO DO CONTRATO

- a) A entidade adjudicante reserva-se ao direito de resolver o contrato em caso de incumprimento definitivo pelo adjudicatário das suas obrigações contratuais, nos termos do disposto na parte final do n.º 1 do artigo 325.º e ainda do disposto nos artigos 334.º, 335.º e 448.º do Código dos Contratos Públicos.
- b) Em tais circunstâncias a entidade adjudicante comunicará por escrito ao adjudicatário as deficiências do serviço, fixando um prazo para a sua regularização, findo o qual, se as anomalias não tiverem sido totalmente corrigidas, terá lugar a resolução do contrato que será comunicada ao adjudicatário mediante carta registada com aviso de receção, na qual serão indicadas as razões que a entidade adjudicante considera justificativas da resolução.
- c) Sem prejuízo da resolução do contrato nos termos previstos nos pontos anteriores, a entidade adjudicante mantém o direito ao pagamento das indemnizações e penalidades aplicáveis nos termos do presente caderno de encargos ou de qualquer disposição legal vigente.

22 GARANTIA

O adjudicatário garantirá, sem qualquer encargo para a entidade adjudicante, os bens e serviços fornecidos pelo prazo indicado na sua proposta, que não pode ser inferior a 2 (dois) anos a contar da data efetiva de entrega, contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos definidos na Secção II do Caderno de Encargos.

23 LEGISLAÇÃO APLICÁVEL

Em tudo o que o presente caderno de encargos for omissivo observar-se-á o disposto no C.C.P., aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual e demais legislação aplicável e, em qualquer caso, sempre a Lei portuguesa.