

## Requisitos de Segurança de Informação para Fornecedores

### 1. Segurança no Acesso às Instalações

- (a) É estritamente proibido utilizar cartões de identificação ou credenciais de acesso de terceiros para entrar em zonas nas quais não se tem acesso autorizado;
- (b) Em todas as áreas que o acesso é controlado por cartão e/ou biometria, este deve ser efetuado a título individual, ou seja, não são permitidas entradas à “boleia”;
- (c) O cartão de identificação deve estar visível a todo o tempo enquanto o adjudicatário estiver dentro das instalações da INCM, principalmente nas zonas de segurança e zona de alta segurança;
- (d) O adjudicatário tem de estar acompanhado pelo trabalhador ou trabalhadora gestor do serviço durante toda a sua permanência nas instalações da INCM;
- (e) Em caso de perda ou roubo do cartão de identificação, o incidente deve ser relatado imediatamente à equipa de segurança interna para que as medidas adequadas sejam tomadas;
- (f) É estritamente proibida a entrada na zona de segurança e na zona alta de segurança com ativos de Informação ou equipamentos de suporte.

### 2. Requisitos Gerais de Segurança de Informação

- (a) O adjudicatário deve ter um procedimento para responder a incidentes de segurança da informação, incluindo a comunicação de eventos e vulnerabilidades de segurança que possam impactar, direta ou indiretamente, a INCM;
- (b) A INCM avalia periodicamente o adjudicatário e comunica a sua avaliação;
- (c) Sempre que se verificar um risco ou que ocorra um incidente de segurança da informação nos ativos da INCM, e se confirme que a causa resulta do incumprimento por parte do adjudicatário de um ou mais compromissos enumerados na presente política, a INCM reserva-se ao direito de propor alterações ou aplicar a resolução do contrato/acordo, conforme o impacto;
- (d) Quando o fornecimento é de produtos ou serviços essenciais para o funcionamento da INCM, deve ser evidenciado pelo adjudicatário um Plano de Continuidade de Negócio (PCN) que assegure a continuidade operacional. Um Plano de Recuperação da Infraestrutura Tecnológica deve ser evidenciado igualmente para serviços tecnológicos essenciais ao normal funcionamento da infraestrutura da INCM, podendo estar integrado no PCN;
- (e) A INCM reserva-se ao direito de auditar, monitorizar e rever os controlos e processos de segurança da informação relacionados aos serviços/produtos fornecidos, incluindo:
  - a. Verificar se os serviços estão em conformidade com os requisitos de segurança estabelecidos no contrato;

- b. Controlar o acesso dos trabalhadores e trabalhadoras do adjudicatário aos ativos da INCM;
  - c. Solicitar anualmente ao adjudicatário, sempre que a falta nos fornecimentos de bens ou serviços deste possam comprometer os SLA da INCM, o relatório dos testes efetuados ao PCN para garantir níveis adequados em caso de acidente ou catástrofe;
  - d. Avaliar anualmente a resposta adequada aos requisitos contratuais através de auditorias ou análise de relatórios de serviço, incidentes de segurança, além de verificar certificações em segurança da informação.
- (f) As constatações identificadas pela Direção de Auditoria da INCM, no decurso da auditoria ao adjudicatário, devem ser acompanhadas pelo adjudicatário para verificar a implementação das correções necessárias. A falta de resposta às constatações mais relevantes identificadas pode conduzir à resolução do contrato/acordo;
- (g) O transporte ou transferência das informações da INCM devem ser efetuadas de forma segura e cifrada;
- (h) O adjudicatário não deve divulgar nem utilizar informações da INCM para outros fins que não os contratualmente definidos ou devidamente autorizado;
- (i) O adjudicatário deve informar a INCM sobre mudanças de pessoal-chave em tempo útil;
- (j) O adjudicatário tem o dever de manter de “sigilo profissional” durante e após a execução do contrato, conforme o dever de confidencialidade acordado contratualmente;
- (k) Para assegurar a proteção e o uso apropriado das informações e recursos da INCM, o adjudicatário tem de obter uma autorização prévia do gestor do contrato da INCM para qualquer transmissão ou eliminação de informações relacionadas com o presente contrato. Além disso, o adjudicatário está restrito ao uso dos recursos de informação da INCM, devendo limitar a sua utilização estritamente aos fins comerciais previamente acordados e estabelecidos no contrato;
- (l) O adjudicatário, ao manter a custódia de informação da INCM, deve implementar:
- a. Controlos de acesso físico nas suas instalações;
  - b. Controlos para impedir o acesso não autorizado a suportes de dados.
- (m) A INCM pode solicitar relatórios de serviço que evidenciem o compromisso com a segurança da informação e que forneçam a garantia de que apenas pessoas autorizadas tenham acesso à informação da INCM;
- (n) Todas as exceções às regras descritas nesta política têm de ser devidamente autorizadas pelo responsável da UO impactada pela ação a desenvolver;
- (o) Quando aplicável, após a cessação da relação contratual entre o adjudicatário e a INCM, o adjudicatário compromete-se a:
- a. Efetuar a devolução de todos os ativos de informação associado ao contrato;
  - b. Efetuar a portabilidade da informação;
  - c. Proceder à devolução, destruição ou eliminação das informações da INCM de acordo com o estabelecido em contrato/CE.

### 3. Segurança no Desenvolvimento de Software

- (a) Deve ser evidenciada a identificação de riscos de segurança de informação e propostos os respetivos controlos de mitigação para novos desenvolvimentos e/ou alterações com impactos considerados relevantes para a INCM;
- (b) Na ausência de disposições contratuais específicas quanto ao licenciamento, titularidade do código e direitos de propriedade intelectual relativos aos conteúdos a serem desenvolvidos, presume-se que a propriedade pertença à INCM. Quando tais disposições existem, os termos contratuais devem estabelecer as condições relacionadas ao licenciamento, titularidade do código e direitos de propriedade intelectual associados aos conteúdos a serem desenvolvidos;
- (c) Deve ser evidenciado o levantamento dos requisitos de segurança da informação para assegurar a Confidencialidade, Integridade e Disponibilidade. A execução dos testes correspondentes a esses requisitos deve estar documentada, tendo como referência o Top 10 do OWASP;
- (d) Deve ser evidenciada anualmente a prática periódica de testes de intrusão, acompanhada pelas ações de mitigação de quaisquer ameaças identificadas;
- (e) Deve ser evidenciada a realização de testes de aceitação relativamente à qualidade dos entregáveis;
- (f) O adjudicatário deve fornecer à INCM toda a documentação relacionada ao projeto, conforme estabelecido nos termos contratuais ou no Caderno de Encargos (CE). Esta documentação inclui, mas não se limita a: manuais do utilizador, manuais de instalação, manuais técnicos e desenhos técnicos;
- (g) O Adjudicatário tem o dever de cumprir com os requisitos de segurança especificados em contrato/CE e de estar em conformidade com as boas práticas recomendadas de desenvolvimento seguro de software;
- (h) O Adjudicatário deve utilizar um sistema de controlo de versão do código fonte (VCS) com controlo de acesso e recuperação em caso de falhas;
- (i) O Adjudicatário deve assegurar os princípios de proteção de dados “*by design and by default*” em todo o âmbito do ciclo de vida do desenvolvimento dos sistemas de informação (desde a fase de conceção até à fase implementação);
- (j) O Adjudicatário deve implementar controlos para impedir que, na transmissão da informação objeto do contrato, bem como no transporte dos ativos de suporte da informação, esta possa ser lida, copiada, alterada ou eliminada de forma não autorizada;
- (k) A INCM detém o direito de realizar auditorias no processo de desenvolvimento, incluindo seus controlos, ou monitorizar as atividades vinculadas ao desenvolvimento contratado. Além disso pode também requisitar periodicamente um relatório que demonstre a eficácia dos controlos de segurança implementados em conformidade com os requisitos de segurança;

- (l) Sempre que possível e conforme os requisitos do sistema, devem ser considerados a autenticação integrada com *Single Sign-On* (SSO). Quando a integração da autenticação nos sistemas não for possível, o Adjudicatário deve garantir que as *passwords* atendam à qualidade e complexidade necessárias, incluindo um mínimo de 12 caracteres de tamanho e pelo menos 4 dos seguintes conjuntos de caracteres (letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # \$ % ^ & \* ( ) \_ + | ` - = \ { } [ ] : " ; ' < > ? , . /));
- (m) Deve-se contemplar a implementação do multi-fator de autenticação (MFA) sempre que seja possível a sua aplicação;
- (n) Se houver necessidade de integrar componentes de terceiros nos serviços ou produtos abrangidos pelo contrato, é responsabilidade do adjudicatário:
  - a. Obter consentimento formal da INCM antes de proceder à integração;
  - b. Validar o atendimento dos requisitos de segurança desses componentes em conformidade com as disposições estabelecidas no presente contrato.
- (o) O Adjudicatário deve implementar controlos apropriados para garantir a segurança da informação contra destruição acidental ou ilícita, perda acidental, alteração, divulgação ou acesso não autorizado, especialmente quando o tratamento envolver a transmissão por redes;
- (p) Os dados de teste, sempre que possível, devem ser criados de forma genérica, sem qualquer relação com dados reais da INCM;
- (q) O adjudicatário deve assegurar a Segregação entre Ambientes de Desenvolvimento, de forma a evitar a necessidade de acesso dos programadores ao ambiente de produção, e caso se verifique a necessidade de acesso dos programadores ao ambiente de produção, ou qualquer ambiente da infraestrutura da INCM, este acesso deve ser previamente autorizado e monitorizado. Deve igualmente ser acompanhado por um elemento da INCM, caso não seja possível, a sessão deve ser gravada com ferramentas próprias, previamente a este acesso, devem ser acautelados pontos de *restore*, que permitam reverter o que for efetuado diretamente em produtivo;
- (r) Para os sistemas que fiquem expostos ao público, o adjudicatário deve implementar um mecanismo que permita identificar a legitimidade e integridade desses sistemas e assegurar que a informação e os recursos de processamento da informação estão protegidos contra código malicioso;
- (s) Qualquer alteração em ambiente de produção deve ser comunicada previamente à INCM;
- (t) Quando a infraestrutura não está na INCM:
  - a. O adjudicatário deve garantir as atualizações de segurança dos sistemas, a fim de assegurar a correção ou atenuação das vulnerabilidades passíveis de serem exploradas em tempo útil;

- b. Assegurar cópias de segurança de forma a garantir que os dados possam ser restaurados em caso de perda, corrupção ou indisponibilidade. Estas cópias devem ser regulares e testadas conforme o PCN e realizado periodicamente;
  - c. Devem ser mantidas as versões anteriores do software desenvolvido, que sejam consideradas necessárias para garantir a recuperação em caso de necessidade de reposição, como medida de contingência.
- (u) O sistema a desenvolver deve prever a implementação de mecanismos de auditoria:
  - a. Para deteção de uso não autorizado;
  - b. Apoio a investigações de incidentes de segurança.
- (v) Registo Obrigatório de *Logs*:
  - a. *Login/Logout*: Identificação do utilizador e data/hora;
  - b. Tentativas de Acesso Falhadas;
  - c. Adições e Alterações: Em contas e permissões de utilizador;
  - d. Configurações de Auditoria e Eventos de Log: Alterações e exclusões;
  - e. Conforme a natureza da aplicação, devem ser identificados os registos de *logs* específicos.
- (w) A INCM pode cancelar ligações de rede caso os requisitos de segurança adequados não sejam implementados, ou for identificada a possibilidade de ataque aos sistemas da INCM através da rede do adjudicatário.
- (x) O adjudicatário deve apresentar evidências de que os seus sistemas possuem controlos de segurança adequados antes de obterem acesso à rede da INCM;
- (y) Garantir que apenas código executável aprovado e não código de desenvolvimento ou compiladores seja instalado nos sistemas operativos;
- (z) A instalação de aplicações e de software do sistema operativo só deve ser aplicada após testes de segurança intensivos e bem-sucedidos, comunicados à INCM previamente à implementação destes:
  - a. Devem ser evitadas configurações *default* e/ou redundantes, sendo que qualquer exceção requer uma aprovação formal da INCM;
  - b. Quaisquer programas ou software provenientes de fontes desconhecidas ou cuja proveniência é duvidosa, não devem ser executados e deverão ser eliminados de imediato. Além disso, as funções, portas, protocolos e serviços do sistema de informação considerados desnecessários e/ou não seguros devem ser desativados;
  - c. O *software* instalado nos sistemas que ligam à rede da INCM deve ser restringido ao que é necessário para a execução das funções de trabalho, os privilégios devem ser concedidos com base nas funções dos trabalhadores e trabalhadoras da INCM envolvidos;
  - d. O adjudicatário deve assegurar o menor tempo possível para a inatividade de sessões relativas aos acessos;

- e. Devem ser desativadas as contas de utilizador da INCM que não se autenticam há mais de 90 dias (caso não seja possível a integração com os sistemas de autenticação da INCM).

#### 4. Segurança em Serviços Fornecidos na Nuvem

Para os serviços em que a infraestrutura está na nuvem:

- (a) O adjudicatário implementa processos controlados de gestão de alterações nos componentes tecnológicos que suportam o serviço *Cloud* prestado à INCM;
- (b) Os serviços prestados pelo adjudicatário devem ser disponibilizados através de instalações e *Data Centers* localizados na União Europeia;
- (c) O adjudicatário assegura que os dados da INCM são apenas replicados por forma a cumprir os requisitos de disponibilidade e respetivos SLAs, acordados com a INCM;
- (d) O adjudicatário garante que os canais utilizados para transmitir os dados da INCM (e.g. ligação entre o *Data Center* da INCM e o adjudicatário de serviços *Cloud*, ligação à camada de apresentação de aplicações SaaS, ligação interna entre componentes da infraestrutura que suportam o serviço *Cloud*) são cifrados, utilizando uma cifra segura e que não são conhecidas vulnerabilidades;
- (e) O adjudicatário garante que os dados da INCM armazenados nos componentes da infraestrutura que suportam o SaaS são cifrados, utilizando uma cifra segura e que não são conhecidas vulnerabilidades;
- (f) O adjudicatário garante que os componentes tecnológicos que suportam o serviço *Cloud* prestado à INCM têm a capacidade de sincronizar o relógio com um servidor de tempo reconhecido (NTP);
- (g) O adjudicatário deve implementar processos de monitorização de segurança de modo permanente sobre os componentes tecnológicos que suportam o serviço *Cloud* à INCM, para projetos que tenham esse nível de exigência;
- (h) O adjudicatário deve assegurar mecanismos de monitorização para deteção de incidentes de cibersegurança;
- (i) O adjudicatário deve notificar a INCM sobre incidentes ocorridos com impacto direto ou indireto nos ativos da INCM, com o prazo de notificação de 24 (vinte e quatro) horas;
- (j) O adjudicatário informa de imediato a INCM sobre quaisquer vulnerabilidades conhecidas nos seus sistemas, que possam representar um risco para os dados da INCM;
- (k) O adjudicatário deve ter definido e implementados processos que assegurem a instalação atempada de atualizações de segurança nos componentes tecnológicos que suportam o serviço *Cloud* prestado à INCM;
- (l) O adjudicatário deve disponibilizar 1 (uma) vez por ano ou sempre que solicitado, informações relativas à capacidade de carga máxima de computação e memória dos componentes da infraestrutura que suporta o serviço *Cloud*;

- (m) O adjudicatário garante que os componentes tecnológicos que suportam o serviço *Cloud* estão configurados de acordo com as boas práticas de segurança;
- (n) O adjudicatário assegura que a infraestrutura virtual de cada cliente é segregada logicamente da infraestrutura virtual dos restantes clientes;
- (o) O adjudicatário assegura que os dados de cada cliente estão segregados logicamente dos restantes clientes;
- (p) O adjudicatário deve implementar várias camadas de segurança de rede, seguindo o princípio da defesa em profundidade para proteção contra ataques de rede;
- (q) O adjudicatário disponibiliza mecanismos de redundância que suportam a ligação dos seus clientes à infraestrutura que suporta o serviço *Cloud*;
- (r) O adjudicatário de serviço *Cloud* disponibiliza uma arquitetura de rede que suporta o tráfego de rede necessário à prestação do serviço *Cloud*, de forma a garantir a manutenção dos objetivos de serviço nos níveis contratualizados com a INCM;
- (s) Caso seja âmbito do projeto, o adjudicatário deve disponibilizar mecanismos de interoperabilidade, como interfaces aplicacionais (*APIs*), que permitem a comunicação com outros recursos através de meios programáticos e que asseguram a confidencialidade, integridade e disponibilidade dos dados em trânsito;
- (t) O adjudicatário implementa processos controlados de gestão do ciclo de vida das chaves criptográficas e certificados digitais;
- (u) O adjudicatário garante que os equipamentos críticos para a continuidade do fornecimento do serviço *Cloud* têm o nível de redundância necessário de forma a evitar interrupções dos serviços *Cloud* prestados aos seus clientes;
- (v) O adjudicatário deve realizar periodicamente testes ao Plano de Recuperação da Infraestrutura Tecnológica e ao Plano de Continuidade de Negócio e comunicar os resultados à INCM.

## 5. Segurança no acesso aos sistemas e redes da INCM

- (a) A INCM pode conceder aos colaboradores do adjudicatário contas de acesso que permitem o uso de ativos/sistemas de informação pertencentes à INCM;
- (b) As referidas contas de acesso são fornecidas exclusivamente para que os colaboradores externos possam fornecer o produto/serviço contratado pela INCM;
- (c) A conta de acesso é de uso único e exclusivo do utilizador ao qual foi fornecido, sendo intransferível. Desta forma, o utilizador é integralmente responsável pela sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outra entidade na posse da sua conta de acesso;
- (d) Os utilizadores deverão adotar as medidas de prevenção para garantir o acesso seguro aos ativos e serviços de informação, incluindo:
  - a. Não utilizar a sua conta, ou tentar utilizar qualquer outra conta, para violar controlos de segurança estabelecidos pela INCM;
  - b. Não partilhar as credenciais de acesso com terceiros;

- c. Informar imediatamente o gestor do contrato caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos/sistemas da INCM.
- (e) Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais de acesso a ativos/serviços de informação será considerada como um incidente de segurança da informação, podendo resultar na resolução do contrato.

## 6. Requisitos de Privacidade e Proteção de Dados

- (a) Quando o adjudicatário tratar dados pessoais por conta da INCM, será considerado como subcontratante, na aceção do disposto no artigo 4º, ponto 8) do RGPD- Regulamento Geral sobre a Proteção de Dados (adiante RGPD).
- (b) A subcontratante deve respeitar os direitos de proteção de dados previstos no **Regulamento Geral de Proteção de Dados (RGPD)** e disponibilizar à INCM todas as informações necessárias para demonstrar o cumprimento das obrigações decorrentes da legislação e/ou do presente Acordo;
- (c) No desenvolvimento de software que envolva o tratamento de dados pessoais, devem ser implementadas as medidas adequadas para cumprir os requisitos previstos no (RGPD), em conformidade com a legislação atualmente em vigor relativamente aos requisitos técnicos mínimos das redes e sistemas de informação.
- (d) O tratamento de dados em regime de subcontratação efetuado pelo subcontratante em nome da INCM é regulado por acordo próprio, nos termos previstos pelo artigo 28º do RGPD, o qual faz parte integrante do contrato principal celebrado com o Adjudicatário e a ele será anexado.

### Controlo de alterações/revisões:

Revisão n.º	Data	Motivo
0	31/10/2024	Criação do documento
1	25/11/2024	Inserção de inputs da DCS para alteração da ordem dos requisitos e correção de gralhas