Política de Segurança da Cadeia de Abastecimento

Informação Geral

Controlo de documentos

Classificação	Público
Versão	1
Data de criação	28/04/2026
Data da última atualização	28/04/2026
Ficheiro	Política de Segurança da Cadeia de Abastecimento

Estatuto formal

Preparado por:	Revisto por:	Aprovado por:
Gabinete de Segurança	Conformidade Regulamentar	Comité de Segurança

Controlo de Versões

Versão	Descrição da mudança	Autor da alteração	Data da alteração
1.0	Criação de documentos	Gabinete de Segurança	28/04/2026

Índice

1. Introdução

Esta política estabelece o quadro de controlo para a gestão dos riscos de segurança associados à cadeia de abastecimento da ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. (doravante, "**esFIRMA"),** enquanto prestador de serviços fiduciários.

A esFIRMA reconhece que a segurança dos seus serviços depende da integridade e resiliência dos seus fornecedores e prestadores de serviços. Assim, na sua relação com a cadeia de abastecimento, a esFIRMA assume a responsabilidade por:

1. Identifique os requisitos de segurança necessários para cada serviço.
2. Comunique claramente estes requisitos aos seus fornecedores diretos.
3. Monitorizar o cumprimento contínuo dos níveis de serviço acordados.

Portanto, o objetivo desta política é definir os controlos para mitigar os riscos identificados para a segurança das redes e sistemas de informação, garantindo que os ativos e serviços de TIC de terceiros respondam aos mesmos níveis de procura que os seus próprios.

2. Âmbito

Esta política é obrigatória (i) para todo o pessoal da esFIRMA envolvido na aquisição de produtos ou serviços de TIC e (ii) para todos os fornecedores e prestadores de serviços que tenham acesso à informação ou infraestruturas da esFIRMA.

3. Critérios de seleção e contratação

De acordo com as disposições do procedimento PS-06 Seleção de fornecedores e PS-07-b Aquisição de ativos de sistemas de informação, a seleção de um determinado fornecedor, produto ou serviço de TIC basear-se-á no seguinte:

- A esFIRMA irá especificar os requisitos mínimos de segurança e avaliar os critérios de cibersegurança que o prestador deve cumprir, de acordo com a criticidade do ativo:

Critérios	Descrição
Práticas de Cibersegurança	Avaliação dos seus procedimentos de desenvolvimento seguro e gestão de vulnerabilidades.
Capacidade Técnica	Capacidade de cumprir especificações, gerir riscos e manter níveis de classificação de segurança.
Resiliência do Produto TIC	Medidas de qualidade e gestão de risco integradas nos produtos TIC fornecidos.
Diversificação	Estratégia para limitar a dependência de um único fornecedor e garantir a continuidade do serviço.
Certificações	Serão valorizadas certificações nas normas ISO 27001, ENS ou certificações específicas de produtos.

- O fornecedor deve garantir: (i) a disponibilidade de atualizações de segurança ao longo da vida útil esperada do ativo e (ii) o compromisso de suporte técnico ou, na falta disso, um plano de substituição/transição antes do final do período de manutenção.

- Para ativos complexos, o fornecedor será solicitado a fornecer informações descritivas dos componentes de hardware e software, declaração das funções de cibersegurança implementadas e orientações de configuração para operação segura.

4. Gestão de Risco de Fornecedores

A esFIRMA irá definir processos para gerir os riscos associados à utilização de produtos ou serviços de terceiros:

- **Avaliação inicial:** antes do contrato, a esFIRMA verificará a conformidade com o produto/serviço em termos de riscos, segurança, proteção de dados e condições contratuais e requisitos ambientais (quando aplicável). Em particular, o produto será avaliado com base nas conclusões da análise de risco, bem como nas necessidades técnicas, de formação e de financiamento.

  Para a avaliação inicial, serão tidos em conta critérios como: qualidade do produto ou serviço fornecido, experiência do fornecedor, relação histórica com ele, preço, reputação, certificações do produto ou da empresa. Em particular, o risco do fornecedor do ponto de vista da segurança da informação deve ser analisado e, dependendo desse risco, serão necessárias as salvaguardas adequadas.

  Além disso, se o produto ou serviço fornecido pelo fornecedor for suscetível de ter um impacto ambiental significativo, esta avaliação inicial terá em conta quaisquer certificações ambientais ou salvaguardas que o fornecedor possua.

- **Avaliação periódica:** os fornecedores estão sujeitos a avaliação periódica (anualmente) e quando há qualquer modificação significativa nos produtos ou serviços fornecidos.

5. Requisitos contratuais obrigatórios

Os contratos com fornecedores e os acordos de nível de serviço (SLAs) devem especificar:

- Requisitos técnicos específicos para a aquisição de serviços ou produtos.
- Obrigação de educação e formação em segurança para o pessoal do fornecedor.
- Requisitos de elegibilidade para funcionários fornecedores que acedam a sistemas críticos.
- Obrigação de informar a esFIRMA, sem demora indevida, de qualquer incidente que afete a segurança da rede ou a informação da esFIRMA.
- Faculdade da esFIRMA para realizar auditorias ou receber relatórios de auditoria de terceiros.
- Compromisso em gerir vulnerabilidades que representam um risco para a esFIRMA.
- Normas para subcontratação, exigindo o cumprimento dos mesmos requisitos de segurança.
- Protocolos para a recuperação e eliminação segura da informação no final da relação.

6. Supervisão e controlo

Para garantir a eficácia desta política, é a ASSINATURA:

- Irá rever periodicamente os relatórios de conformidade com acordos de nível de serviço (SLA).
- Irá analisar incidentes relacionados com produtos de TIC fornecidos por terceiros.
- Avaliar a necessidade de revisões adicionais com base no nível de risco detetado.
- Manterá um acompanhamento constante do desempenho dos fornecedores aceites, através da sua avaliação contínua.

7. Revisão e atualização

Esta política será revista pelo menos anualmente e sempre que houver alterações nas práticas de cibersegurança dos fornecedores e prestadores de serviços, ou alterações significativas nas operações de abastecimento ou incidentes de segurança relevantes que afetem a cadeia de abastecimento.