Política de Segurança

Informação Geral

Controlo de documentos

Classificação	Público
Versão	3
Data de criação	29/04/2016
Data da última atualização	28/04/2026
Ficheiro	Política de Segurança

Estatuto formal

Preparado por:	Revisto por:	Aprovado por:
Gabinete de Segurança	Agente de Segurança	Comité de Segurança

Controlo de Versões

Versão	Descrição da mudança	Autor da alteração	Data da alteração
1.0	Criação de documentos	Gabinete de Segurança	29/04/2016
1.1	Crítica	Gabinete de Segurança	10/03/2017
2.0	Revisão dos papéis e das suas nomeações	Gabinete de Segurança	02/06/2017
2.1	Revisão dos papéis e separação de nomeações para o documento do Anexo.	Gabinete de Segurança	08/06/2017
2.2	É acrescentado o papel do Oficial de Revogação. A referência à AULOCE é substituída por ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.	Gabinete de Segurança	02/10/2020
2.3	Inclui o papel de Operador de Registo	Gabinete de Segurança	14/04/2023

2.4	Os detalhes das funções do Oficial de Segurança são revistos (ETSI EN 319 401 (v3.1.1))	Gabinete de Segurança	11/03/2025
2.5	A redação das funções do cargo de Auditor é revista e esclarecida	Gabinete de Segurança	28/03/2025
3	Adaptação à nova versão do ETSI EN 319 401, atualização de formato e inclusão do papel de Gestor de Desenvolvimento	Gabinete de Segurança	28/04/2026

Índice

1. Introdução

ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. com CIF A-50.878.842 e domiciliada na Calle Bari 39, C.P. 50.197 (Saragoça), registada no Registo Mercantil de Saragoça no volume 2.649, Fólio 215, página Z-28722, opera sob o nome comercial "**esFirma**" como prestadora de serviços de certificação.

A esFIRMA atua de acordo com as regulamentações nacionais e europeias que lhe são aplicadas, de modo a facilitar o cumprimento dos requisitos legais e o reconhecimento internacional dos seus serviços. Entre outros:

- Regulamento (UE) nº 910/2014 sobre identificação eletrónica e serviços de confiança para transações eletrónicas no mercado interno (Regulamento eIDAS).
- Normas técnicas ETSI aplicáveis à emissão e gestão de certificados qualificados, principalmente ETSI EN 319 411-1 e ETSI EN 319 411-2.
- Regulamentos nacionais sobre assinaturas eletrónicas.

A esFIRMA promoveu o desenvolvimento de uma política de segurança que serve de guia para a proteção dos sistemas e redes de informação que apoiam a prestação dos seus serviços de certificação. Esta política é adequada e complementar à estratégia e aos objetivos empresariais da esFirma, integrando a segurança como elemento fundamental para a continuidade e desenvolvimento do serviço.

A gestão da esFirma está comprometida em fornecer os recursos necessários para a implementação eficaz desta política, assegurando a disponibilidade de capital humano especializado, dotação financeira suficiente, bem como os processos, soluções tecnológicas e infraestruturas necessárias.

2. Âmbito

Esta política de segurança abrange todos os serviços de certificação prestados pela esFIRMA e é obrigatória para todo o pessoal da esFIRMA, bem como para terceiros que prestam ou utilizam serviços e transferem ou gerem informações pelas quais a esFirma é responsável (doravante, denominados conjuntamente "**pessoal**").

3. Princípios

Esta política será desenvolvida, em geral, de acordo com os seguintes princípios:

- **Princípio da confidencialidade.** Os ativos de TIC devem ser acessíveis apenas por pessoas ou processos autorizados.

- **Princípio de integridade e qualidade.** A integridade da informação deve ser mantida, assim como os processos de processamento.

- **Princípio da disponibilidade e continuidade.** Será garantido um elevado nível de disponibilidade de ativos TIC e serão fornecidos os planos e medidas necessários para garantir a continuidade dos serviços.

- **Princípio da rastreabilidade.** Serão implementadas medidas para garantir que, em todos os momentos, se possa determinar quem e quando uma ação foi desencadeada, de modo a ter capacidades de análise sobre incidentes de segurança detetados.

- **Princípio da autenticidade.** Devem ser articuladas medidas para garantir a fonte de informação de onde provêm os dados e que as entidades de onde os dados provêm são fiáveis.

- **Princípio de gestão de risco.** Os riscos serão analisados e serão estabelecidas as medidas de segurança necessárias para os minimizar.

- **Princípio da proporcionalidade no custo.** As medidas de segurança adotadas para mitigar os riscos serão implementadas numa perspetiva de proporcionalidade nos custos envolvidos.

- **Princípio de consciência e formação.** Todas as pessoas responsáveis pela gestão dos sistemas de informação serão formadas para que possam conhecer as suas obrigações relativamente ao tratamento seguro da informação que gerem.

- **Princípio da prevenção.** Serão realizadas iniciativas para a prevenção de incidentes de cibersegurança.

- **Princípio da melhoria contínua.** A esFirma manterá um compromisso explícito com a melhoria contínua da segurança das suas redes e sistemas de informação, rever periodicamente os seus controlos e adaptá-los a novas ameaças.

- **Princípio da segurança das TIC no ciclo de vida dos sistemas de informação**: Em todas as fases do ciclo de vida dos ativos, serão aplicadas as especificações de segurança e procedimentos de controlo correspondentes.

- **Princípio da segurança desde o design e por defeito**: a esFIRMA estabelecerá e aplicará regras para o desenvolvimento seguro de redes e sistemas de informação que abrangem todas as fases: especificação, design, desenvolvimento, implementação e testes.

- **Princípio da função diferenciada.** A responsabilidade pela segurança dos sistemas de informação será separada da responsabilidade pelo serviço.

4. Objetivos de segurança

A esFirma estabelece os seguintes objetivos estratégicos em termos de segurança de redes e sistemas de informação:

- **Proteger bens.** Proteger a confidencialidade das informações dos utilizadores e garantir a integridade absoluta dos processos de emissão, gestão e revogação de certificados.

- **Resiliência operacional.** Implementar mecanismos proativos de deteção e resposta, assegurando a continuidade do negócio através de planos de recuperação que garantam a resiliência dos serviços de confiança face a contingências.

- **Conformidade regulamentar.** Garantir o cumprimento total e contínuo do quadro legal aplicável à esFIRMA.

- **Geração de confiança:** Reforçar a reputação da esFIRMA junto dos seus stakeholders através de uma gestão de segurança transparente e da manutenção de elevados níveis de disponibilidade de serviços.

5. Organização de segurança

A organização da esFirma é articulada de acordo com os papéis descritos abaixo. As funções, responsabilidades e funções atribuídas serão revistas anualmente e quando ocorrerem incidentes significativos, alterações nas operações ou riscos.

5.1. Comité de Segurança

O Comité de Segurança será composto por três membros: o seu Presidente, o Oficial de Informação e Serviços e o Oficial de Segurança. O Comité de Segurança é responsável por:

a) Aprovação do nível de apetite pelo risco e do limiar de tolerância ao risco.
b) Aprovação da análise de risco e, quando apropriado, do plano de tratamento de risco.
c) Aprovação de novos documentos ou modificações relevantes ao quadro regulatório de segurança e documentação relevante da autoridade certificadora (plano de cessação, plano de continuidade, declaração de práticas de certificação, política de segurança...).

5.2. Gabinete de Segurança

O Gabinete de Segurança corresponde ao Departamento de Conformidade Regulamentar e é composto pelo Gestor de Segurança e pelo pessoal considerado necessário em todos os momentos para o desempenho das suas funções.

As suas funções incluem:

a) Realização da avaliação anual de risco e, quando apropriado, do plano de tratamento de risco, que deve ser aprovado pelo Comité de Segurança.
b) Preparação de propostas relativas à revisão do quadro regulatório de segurança e documentação relevante da autoridade de certificação (plano de cessação, plano de continuidade, declaração de práticas de certificação, política de segurança, etc.), que devem ser aprovadas pelo Comité de Segurança.
c) Pequenas modificações nos regulamentos, procedimentos, instruções e outros elementos dentro da estrutura regulatória de segurança.

d) Formação de pessoal em segurança da informação.
e) Reportar informações ao Comité de Segurança, através do Oficial de Segurança, sobre assuntos relacionados com a segurança das redes e sistemas de informação.

Para desempenhar as suas funções, o Gabinete de Segurança depende do Centro de Operações de Segurança (SOC) como unidade responsável pela vigilância ativa e manutenção do ambiente de segurança do esFirma (monitorização contínua, deteção e análise precoce de ameaças, resposta a incidentes, etc.).

5.3. Funções de confiança

As pessoas que desempenham cada uma das funções estão definidas no documento ANEXO. ESFIRMA – DEFINIÇÃO DE FUNÇÕES DE TRUST.

5.3.1. Papéis e Funções no âmbito da CA

- **Administrador de Sistemas**. Responsável pelo correto funcionamento do suporte de hardware e software da plataforma de certificação.

- **Administrador da Califórnia**. Responsável pelas ações a realizar com o material criptográfico, ou pelo desempenho de qualquer função que envolva a ativação das chaves privadas das autoridades certificadoras descritas neste documento, ou de qualquer um dos seus elementos.

- **Auditor**. Autorizado a visualizar ficheiros de registo e auditorias com o objetivo de auditar as operações do sistema segundo as políticas de segurança estabelecidas. As tarefas do Auditor são incompatíveis com a operação e administração dos sistemas.

- **Operador de ar condicionado**. Responsável pela custódia do material de ativação de chaves criptográficas em conjunto com o Administrador da CA, também responsável pelas operações de backup e manutenção da CA.

- **Gestor de Segurança**. Responsável por coordenar, controlar e aplicar as medidas de segurança definidas pelas políticas de segurança da esFIRMA. Responsável por aspetos

relacionados com a segurança da informação: lógico, físico, de redes, organizacional, etc., bem como reportando à gestão sénior através do Comité de Segurança.

- **Gestor de informação e serviço**. Define os requisitos de informação e serviços em termos de segurança. Este papel tem a responsabilidade última pela utilização da informação e dos serviços e, consequentemente, pelo seu nível de proteção.

- **Especialista em validação**. Responsável pela validação dos pedidos de certificados.

- **Oficial de Revogação**. Responsável pela operação de alteração do estado dos certificados.

- **Operador do registo.** Responsável pela aprovação dos pedidos de certificação pelo assinante.

- **Gestor de Desenvolvimento.** Assume as funções de implementação e controlo do ciclo de vida de desenvolvimento de sistemas de software e firmware PKI.

5.3.2. Papéis e funções no âmbito do sistema de assinatura remota (assinatura por PIN)

- **Gestor de Segurança**. Responsabilidade global pela gestão e implementação de práticas e políticas de segurança.

- **Administrador de Sistema L1**. Autorizado com quórum mínimo (3/5) a inicializar e atualizar SSCDs. Os SSCDs tornam-se imutáveis uma vez inicializados. São os detentores de uma parte da chave de ativação do sistema

- **Administrador de Sistema L2**. Autorizado a configurar e manter o sistema de assinatura de PIN com acesso controlado à informação de segurança. Eles podem ajustar a fonte do tempo. Eles podem criar credenciais de login para a SSA. Confirma essas credenciais.

- **Operador do sistema**. Responsável pela operação diária do sistema. Eles não podem, de qualquer forma, administrar ou configurar o sistema.

- **Auditor**. Autorizado a visualizar ficheiros de registo e auditorias com o objetivo de auditar as operações do sistema segundo as políticas de segurança estabelecidas. As tarefas do Auditor são incompatíveis com a operação e administração dos sistemas.

- **Gestor de Desenvolvimento.** Assume as funções de implementação e controlo do ciclo de vida de desenvolvimento do sistema de assinatura remota.

6. Estrutura regulatória de segurança

A política de segurança gera uma estrutura regulatória de segurança composta pela própria política, regulamentos e procedimentos de segurança, com níveis hierarquicamente relacionados, conforme descrito abaixo:

6.1.1. Primeiro nível: Política de segurança da informação.

A política de segurança é aprovada pelo Comité de Segurança. A política de segurança é comunicada e disponibilizada ao pessoal da esFirma e a terceiros interessados através de um link permanente no site da esfirma.

6.1.2. Segundo nível: Normas de segurança da informação

As normas de segurança surgem como um desenvolvimento de políticas numa determinada área da segurança da informação. Entre outros, vale a pena destacar:

- ✓ Regulamentos sobre a utilização de recursos e acesso a sistemas de informação
- ✓ Regulamentos de trabalho fora do local
- ✓ Regulamentos de classificação de informação
- ✓ Regulamentos para a utilização de Serviços Cloud
- ✓ Regulamentos para o uso do e-mail
- ✓ Regulamentos de gestão de media
- ✓ Regulamentos de gestão de incidentes cibernéticos
- ✓ Regulamentos de apagamento seguro de dados
- ✓ Política de Configuração de Palavras-passe

Os regulamentos de segurança são comunicados ao pessoal da EsFirma e estão disponíveis para consulta de forma permanente na Intranet da empresa.

6.1.3. Terceiro nível: Procedimentos de segurança da informação.

Os procedimentos indicam o fluxo de atividades relacionadas com os serviços ou ativos de informação realizados pela esFirma.

6.1.4. Quarto nível: Instruções Técnicas

Instruções técnicas são comandos que especificam como fazer o que está estipulado nos procedimentos.

7. Desenvolvimento Seguro de Redes e Sistemas

Antes de qualquer implementação de software, rede ou sistema de informação, o esFIRMA aplicará as seguintes diretrizes de segurança:

- Análise de requisitos: uma análise de segurança será realizada nas fases iniciais de especificação e design de qualquer projeto ou aquisição de produtos TIC.

- Engenharia segura: Serão aplicados princípios de engenharia de sistemas seguros e codificação segura, promovendo arquiteturas de "confiança zero".

- Ambientes controlados: Serão estabelecidos requisitos específicos para garantir a segurança dos ambientes de desenvolvimento, pré-produção e testes.

- Ciclo de teste: Os processos de teste de segurança serão implementados ao longo de todo o ciclo de vida do desenvolvimento.

- Gestão de dados de teste: os dados utilizados em ambientes de desenvolvimento e testes serão devidamente selecionados e protegidos; através da purificação de dados e anonimização.

- Desenvolvimento terceirizado: no caso de subcontratação, os fornecedores serão contratualmente obrigados a cumprir esses mesmos requisitos.

A esFIRMA possui processos para gestão de mudanças, aquisição de ativos de sistemas de informação, design e desenvolvimento seguro que complementam e desenvolvem as disposições desta Política.

8. Conformidade

8.1. Conformidade do pessoal

Todo o pessoal da esFirma é responsável por conhecer, compreender e cumprir rigorosamente esta política de segurança, bem como as regras e procedimentos derivados que afetam as suas funções específicas; cada pessoa é responsável pela correta utilização dos ativos de tecnologia da informação e comunicação que lhes são disponibilizados.

Da mesma forma, os colaboradores têm a obrigação de reportar imediatamente e sem demora excessiva qualquer incidente de segurança, através dos mecanismos disponibilizados pela esFIRMA.

Para garantir a eficácia deste compromisso, a esFirma implementa as seguintes ações:

- **Comunicação interna:** a política é comunicada e formalmente reconhecida por todos os colaboradores. Está permanentemente disponível para consulta no site da esFIRMA.

- **Sensibilização e formação:** são implementados programas regulares de formação em segurança da informação para garantir que o pessoal identifica riscos e age de acordo com os protocolos estabelecidos.

As respetivas sanções disciplinares serão aplicadas ao pessoal que violar esta política ou os regulamentos de segurança que a desenvolvem, de acordo com as disposições da legislação laboral aplicável.

8.2. Conformidade por terceiros

Terceiros que prestem serviços à esFIRMA ou tratem de informações sob a responsabilidade da esFIRMA devem cumprir as disposições desta Política e podem desenvolver os seus próprios procedimentos operacionais para a satisfazer.
Serão estabelecidos procedimentos específicos para reportar e resolver incidentes. Em particular, terceiros devem informar a esFIRMA de qualquer incidente de que tenham

conhecimento e que possa afetar um sistema de informação e/ou a informação em questão ou os serviços prestados.

O pessoal externo será incentivado a estar devidamente consciente da segurança e privacidade, pelo menos ao mesmo nível estabelecido nesta Política.

9. Gestão documental e conservação

A esFirma mantém um inventário da documentação do sistema de gestão de segurança da informação (políticas, regulamentos, instruções técnicas, etc.).

Toda a documentação, registos e dados dos serviços fiduciários serão mantidos de acordo com os prazos legais estabelecidos no Regulamento eIDAS e na Lei 6/2020, garantindo a sua disponibilidade por um período mínimo de 15 anos (ou conforme determinado pelos regulamentos em vigor em cada momento).

10. Monitorização e indicadores

Para supervisionar a implementação eficaz desta política e determinar o nível de maturidade do esFirma em termos de segurança de redes e sistemas de informação, é estabelecido um quadro de medição contínua, apoiado pela atividade do SOC (Centro de Operações de Segurança).

Esta estrutura utiliza os seguintes indicadores-chave:

- **Indicadores de Gestão de Incidentes:** monitorização da capacidade de resposta e do tratamento dos eventos de segurança detetados através do SOC, garantindo uma gestão eficaz das anomalias e mitigação de possíveis riscos operacionais.

- **Eficiência dos controlos:** Medição do nível de maturidade técnica através de varreduras periódicas de vulnerabilidades e testes de penetração.

- **Cultura de segurança:** Avaliação do nível de formação do pessoal através de indicadores de participação e sucesso em programas de formação e campanhas de sensibilização.

- **Disponibilidade e continuidade:** monitorizar os níveis de disponibilidade dos serviços de confiança e analisar os resultados obtidos em testes periódicos de planos de continuidade e recuperação de desastres.

11. Crítica

Esta política, bem como os regulamentos de segurança, estão sujeitos a revisão periódica para garantir que são adequados aos riscos e ao ambiente operacional do esFirma.

Esta revisão será realizada pelo menos anualmente e sempre que houver incidentes de segurança significativos ou alterações substanciais nas operações, nas tecnologias utilizadas ou na análise de risco.

O Gabinete de Segurança avaliará a validade do documento e propôs as atualizações necessárias quando apropriado. O Comité de Segurança é responsável pela aprovação formal desta política.

O resultado de cada revisão, independentemente de gerar ou não uma atualização de documento, deve ser devidamente documentado para garantir a rastreabilidade do processo de governação de segurança.