jornadas FCCN

Identidade Digital e o Futuro da Autenticação Federada

Esmeralda Pires

epires@fccn.pt

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Agenda

jornadas FCCN

01	eduGAIN · Governação & Estratégia
02	REFEDS Baseline Expectations
03	Novos requisitos eduGAIN em curso
04	Preparação e Conformidade
05	Shibboleth IdP 5.2.1 Playbook

01 · eduGAIN Governação & Estratégia

jornadas FCCN

Reforma aprovada 2023 · Em vigor desde janeiro 2024

O QUE MUDOU NA GOVERNAÇÃO

ANTES

Steering Group (eSG)

- Um representante de cada federação, todos no mesmo grupo
- Decisões lentas, responsabilidade diluída, difícil de gerir
- Boas intenções, mas sem capacidade real de agir

AGORA

Assembleia + Steering Commitee

Representantes de cada federação + 6 membros eleitos

- Dois níveis distintos de governação
- Com poder e legitimidade para fazer cumprir as regras

Da reforma à ação: sete objetivos para concretizar a mudança

01 · eduGAIN Governação & Estratégia

jornadas FCCN

SETE OBJECTIVOS ESTRATÉGICOS 2025 - 2030

1 Consistência e fiabilidade

Melhorar a consistência e fiabilidade da informação sobre as federações de identidade

2 Melhorar a interoperabilidade

Melhorar a interoperabilidade entre e dentro das federações de identidade (ex.: incluir novos perfis tecnológicos como OIDC).

3 Elevar padrões de segurança

Melhorar os standards de segurança, proteção de dados e assurance em todas as entidades no eduGAIN (ex.: Aplicar as REFEDS Baseline Expectations)

4 Reduzir entidades não conformes

Reduzir o número de entidades não conformes e agir sobre os incumprimentos

5 Maior transparência

Maior transparência sobre o nível de assurance e conformidade esperados.

6 Sustentabilidade operacional a longo prazo

Garantir que as operações core do eduGAIN são mantidas, financiadas e operam de forma resiliente

7 Políticas adequadas e aplicadas

Garantir que as políticas e processos do eduGAIN são adequados e aplicados.
As regras já existiam. O Steering Commitee tem agora poder real para rever políticas, exigir cumprimento e suspender quem não cumpra.

Fonte: edugain.org/edugain-strategy-2025-2030/

02 · REFEDS Baseline Expectations

Os requisitos de confiança que sustentam a participação no eduGAIN

02 ·REFEDS BE Papéis e Responsabilidades

Papéis distintos e complementares na cadeia de confiança das federações de identidade

QUEM DEFINE **REFEDS**	QUEM IMPLEMENTA **eduGAIN**	QUEM APLICA **Federações Membro**
Research and Education FEDerations Comunidade global das federações académicas, coordenada pela GÉANT, que define as normas e boas práticas de identidade federada ***Define os requisitos*** Principais normas e perfis publicados: **Baseline Expectations**, Assurance Framework, MFA Profile, Sirtfi e Entity Categories (ex: R&S)	***Implementa e exige*** Adotou as REFEDS BE · verifica a conformidade nos metadados e atua sobre os incumprimentos	***Aplicam localmente*** Garantem que IdPs e SPs cumprem os requisitos antes de exportar para o eduGAIN

REFEDS diz o que é necessário · **eduGAIN** implementa e exige (técnico + operacional) · **Federações** aplicam localmente

02 ·REFEDS Baseline Expectations

Requisitos mínimos de confiança, segurança e qualidade de metadados que **todos os participantes do eduGAIN** devem cumprir (Federação, IdPs e SPs)

Independente da tecnologia

- As *BE* aplicam-se a qualquer organização, independentemente do protocolo ou software utilizado (SAML, OIDC ou outro).
- A conformidade assenta nos comportamentos operacionais da organização: como gere, protege e mantém o seu IdP ou SP.

Responsabilidade institucional

- *Mesmo que o IdP ou SP seja operado por terceiros , a responsabilidade pelo cumprimento das BE é sempre da organização cujo nome e autoridade são representados na federação.*

Conformidade em Evolução Permanente

- *São um compromisso contínuo, o nível de exigência cresce à medida que a comunidade evolui e as ameaças aumentam.*
- O que hoje é recomendado, amanhã pode ser obrigatório.

Documento oficial: **Baseline Expectations for Trust in Federation** · https://refeds.org/baseline-expectations

02 ·REFEDS BE = Requisitos mínimos obrigatórios

jornadas FCCN

Operadores de IdP [IPO]

- **IPO1** Responsabilidade legal e operacional pelo IdP
- **IPO2** IdP confiável para aceder aos sistemas internos da organização
- **IPO3** Contactos publicados, resposta atempada
- **IPO4** Práticas de segurança, proteção de dados e resposta a incidentes
- **IPO5** Metadata completa, precisa e atualizada

Operadores de SP [SPO]

- **SPO1** Controlos de privacidade do utilizador no serviço
- **SPO2** Não partilha de dados sem notificação; retenção mínima
- **SPO3** Contactos publicados, resposta atempada
- **SPO4** Segurança: proteção de dados, integridade e resposta a incidentes
- **SPO5** Metadata completa, precisa e atualizada
- **SPO6** Atributos requeridos publicados, respeitando a privacidade

Operadores de Federação / Interfederação [FO] — transversal a IdPs e SPs

- FO1 Confiabilidade da Federação como objetivo primário e transparência
- FO2 Contactos publicados e resposta atempada
- FO3 Práticas de segurança e resposta a incidentes
- FO4 Metadata autêntica, precisa e interoperável
- FO5 Implementar frameworks (R&S, SIRTFI, CoCo)
- FO6 Colaborar na promoção das BE

02 ·REFEDS BE da teoria à prática

jornadas FCCN

As Baseline Expectations **traduzem-se em requisitos técnicos** concretos na operação e na publicação de metadados SAML dos IdPs e SPs.

eduGAIN · Tradução Técnica

1 Práticas Operacionais

As BE operacionalizam-se nos processos internos dos IdPs e SPs (ex.: responsabilidade operacionais bem definidas, boas práticas de segurança, etc.)

2 SAML Metadata Profile do eduGAIN

Materializam-se na metadata SAML que circula entre federações

Garantido a Confiança e Interoperabilidade → em evidências técnicas e operacionais → **Verificáveis de forma automática**

02 · BE IdP Operators = Requisitos mínimos obrigatórios

jornadas FCCN

✓ Em vigor

IPO1 Responsabilidade Institucional do IdP

O Identity Provider (IdP) é operado sob autoridade formal da instituição garantindo que a organização assume plena responsabilidade legal e operacional pelo seu funcionamento.

IPO2 Confiável para sistemas internos

Identity Provider é suficientemente confiável para ser utilizado no acesso aos sistemas da sua própria organização

eduGAIN · Tradução Técnica

✓ MRPS - Metadata Registration Practice Statement

Cada federação participante no eduGAIN deve publicar e aplicar um **MRPS**.

- O MRPS define quem pode registar e operar IdPs
- O operador da federação valida e aprova entidades
- Apenas entidades aprovadas entram no metadata aggregate

Federação → Validação no processo de Onboarding → Instituição assina Protocolo

02 · BE IdP Operators = Requisitos mínimos obrigatórios

✓ Em vigor

IPO3 Contactos Operacionais do IdP

Publicas informação de contacto do teu Identity Provider e respondes de forma atempada a questões operacionais

eduGAIN · Tradução Técnica

✓ Requisitos obrigatórios no SAML Metadata

Os metadados SAML das entidades devem incluir contactos operacionais:

- **Contacto Técnico** *(técnico ou suporte, pelo menos um)*
- **Contacto de Suporte** *(alternativa válida ao técnico)*
- **Contacto Administrativo** *(opcional, fica ao critério da federação)*
- **Contacto de Segurança** *(obrigatório se a entidade afirma SIRTFI, testados periodicamente em exercícios formais)*

Emails devem ser de role/função (não pessoais).

eduGAIN não verifica se os contactos funcionam → responsabilidade da Instituição e da Federação

02 · BE IdP Operators = Requisitos mínimos obrigatórios

jornadas FCCN

✓ Em vigor

IPO4 Boas práticas de segurança

Aplicas práticas de segurança para proteger a informação dos utilizadores, garantir a integridade das transações e assegurar uma resposta atempada a incidentes.

eduGAIN · Tradução Técnica

✓ Proteção de Dados do Utilizador

- Todos os endpoints SAML devem usar HTTPS com TLS 1.2 ou superior
- Proibição de protocolos inseguros (TLS 1.0/1.1, SSLv3)
- Certificados TLS devem ser válidos e emitidos por CA de confiança

✓ Integridade das transações

- SAML Assertions devem ser assinadas digitalmente (XML Signature)
- Metadados das entidades é assinada pela federação

✓ Níveis de Confiabilidade de Identidade

- REFEDS Assurance Framework
- REFEDS MFA Profile

Adoção recomendada

✓ Resposta a Incidentes

- Framework **Sirtfi (REFEDS)**

Adoção recomendada

02 · BE IdP Operators = Requisitos mínimos obrigatórios

jornadas FCCN

✓ Em vigor

IPO5 Metadata completa e correcta

Assegura que os metadados registados na federação são completos, precisos e atualizados

eduGAIN · Tradução Técnica

✓ Qualidade e Actualização dos Metadados

- Registo completo de todos os elementos obrigatórios no metadata SAML (ex: endpoints, certificados, contactos)
- Precisão dos dados publicados, garantindo consistência entre configuração real e Metadata
- Atualização regular dos metadados, especialmente após alterações técnicas (certificados, URLs)
- Gestão da validade de certificados e dados críticos, prevenindo expiração ou inconsistências

Assegurados por validação técnica automática
+
Responsabilidade distribuída (federações e instituições)

→ **A não conformidade motivo de rejeição ou perda de interoperabilidade**

03·Novos requisitos eduGAIN em curso

O nível de exigência cresce à medida que a comunidade evolui e as ameaças aumentam.

O que hoje é recomendado, amanhã pode ser obrigatório.

03 · Novos Requisitos eduGAIN em curso

Roadmap em 4 Fases

Calendário proposto

1

CONCLUÍDA
31 Dez 2025

Federações

- Contactos de segurança obrigatórios
- Compromisso de resposta a incidentes
- Aplica-se a todas as federações membro

2

PROPOSTA
31 Dez 2026

Entidades & IdPs

- Contactos de segurança em todas as entidades
- Privacy notice + mdui:PrivacyStatementURL
- *Adoção RAF para todos os Identity Providers*

3

PROPOSTA
31 Dez 2027

Sirtfi & Unicidade

- Sirtfi obrigatório para todas as entidades
- Identificadores únicos: assurance/ID/unique

4

EM ANÁLISE
TBD

Nível mínimo RAF

- Estabelecer nível mínimo de assurance
- Base provável: IAP/low
- Em discussão na comunidade

⚠ Notas Fase 2 (2026)
O requisito de expressão de informação RAF (REFEDS Assurance Framework) para IdPs na Fase 2 está ainda em discussão dentro do eSC. Poderá ser movido para 2027 (Q1 ou Q4) dependendo da decisão final do Steering Committee.
O **PrivacyStatementURL** e os **contactos de segurança para TODAS as entidades** são os requisitos mais consolidados para 31 Dez 2026.

03 · Novos Requisitos eduGAIN em curso

Como cumprir a Fase 2

Deadline 31 Dezembro 2026

IdP + SP

Contacto de segurança formal

O contacto de segurança obrigatório, é usado pelo eduGAIN Security Team para notificação de incidentes.

Evidência:

Metadata: <ContactPerson contactType="other" remd:contactType="security"> com GivenName + EmailAddress

IdP + SP

PrivacyStatementURL obrigatório

Reforça que todas as entidades publicadas no eduGAIN (incluindo SPs) devem ter este campo, alinhando com requisitos de proteção de dados (RGPD)

Evidência:

Metadata: <mdui:PrivacyStatementURL xml:lang="pt">https://...</mdui:PrivacyStatementURL>

03 · Novos Requisitos eduGAIN em curso

Como cumprir a Fase 3

Deadline 31 Dezembro 2027

IdP + SP

SIRTFI obrigatório para todas as entidades

O SIRTFI fornece uma plataforma de confiança para comunicar, gerir e responder a incidentes de segurança federados, facilitando a colaboração entre instituições e serviços membros.

SIRTFI formalmente obrigatório para TODAS as entidades.

A instituição deve avaliar a documentação SIRTIFI e declarar conformidade e indicar contacto de segurança segundo as regras SIRTIFI.

Evidencias

- Entity attribute SIRTFI no metadata
- Contacto de segurança publicado
- Política de resposta a incidentes documentada

IdP

Assurance Framework
Unicidade de identificador declarada

A instituição deve avaliar os perfis de confiabilidade da sua federação e realizar uma auditoria de conformidade.

O IdP deve suportar os níveis de confiabilidade de identidade através do atributo **eduPersonAssurance** e declarar que identificadores de utilizador são persistentes, únicos e não reutilizados.

Evidência:

- Presença do atributo **eduPersonAssurance** na asserção SAML
- Valores REFEDS válidos
- Configuração do IdP para enviar esse atributo

04·Preparação e Conformidade

04 · Preparação e Conformidade

O que a RCTSaai já disponibiliza

Base para a preparação

Categorias Suportadas

Atributo SAML que sinaliza que a entidade cumpre os requisitos da categoria, agilizando a libertação automática do conjunto mínimo de atributos.

3 categorias recomendadas

- **R&S** · Research & Scholarship (REFEDS) — colaboração investigação/ensino; eppn, mail, displayName
- **CoCo** · GÉANT Data Protection Code of Conduct — conformidade RGPD na partilha de atributos
- **ESI** · European Student Identifier — mobilidade Erasmus+, transcrições e alianças universitárias

→ Página Atributos por Categoria no espaço RCTSaai

SIRTFI

Plataforma de confiança para resposta coordenada a incidentes de segurança entre instituições da federação.

4 áreas de auto-avaliação

- **OS** · segurança operacional (patching, deteção, equipa de resposta)
- **IR** · resposta a incidentes (contactos, colaboração, TLP)
- **TR** · rastreabilidade (logs, timestamps, identificadores)
- **PR** · responsabilidade dos participantes (PUA aceite pelos utilizadores)

Adesão: auto-avaliação → email para noc@fccn.pt → metadados atualizados pela equipa RCTSaai.

→ Página SIRTFI no espaço RCTSaai

Perfis de Confiabilidade

4 perfis que validam a qualidade da identidade digital, alinhados com REFEDS Assurance Framework, REFEDS SFA/MFA

- **RCTS P0** · identificador único; atributos por auto-asserção
- **RCTS P1** · identidade verificada pela instituição; atributos sob responsabilidade do membro
- **RCTS P2** · P1 + MFA obrigatória; auditoria com a Operação da Federação
- **RCTS P3** · identidade confirmada + MFA; auditoria reforçada

→ Página Perfis de Confiabilidade no espaço RCTSaai

04 · Preparação e Conformidade

Onde estamos hoje?

O que já cumprimos · Gaps abertos · Já em vigor (Baseline atual)

JÁ CUMPRIDO

Fase 1 — Federação

- Contactos de segurança da FCCN registados na federação
- Compromisso formal de resposta a incidentes (Sirtfi nível federação)
- Aplicável às federações-membro do eduGAIN — concluído a 31 Dez 2025

GAPS ABERTOS

O que falta nas entidades

- IP03 — muitos IdPs com contactos desatualizados
- IP04 — IdPs em versões sem suporte; baixa adesão a Sirtfi/Assurance
- IP05 — certificados expirados e key-rollover incompleto em IdPs/SPs

04 · Preparação e Conformidade

Marcos para chegar a Dez 2026 (Fase 2) e Dez 2027 (Fase 3) em conformidade

AGORA → Q2 2026

Estabilizar baseline

- Auditoria a IdPs/SPs: certificados válidos, endpoints e URLs corretos
- Renovar certificados expirados; concluir key-rollover pendente
- Atualizar IdPs com versões em fim de vida (Shibboleth/SimpleSAML)

Q3 → Dez 2026 · arranque RAF

Fase 2 eduGAIN + arranque RAF

- Adicionar contactos de segurança em todos os IdPs e SPs
- Publicar mdui:PrivacyStatementURL em IdPs e SPs
- Avaliar unicidade de identificadores e mapeamento RCTSaai
- Arrancar processo Sirtfi/RAF com Federação e IdPs: auditoria interna e desenho operacional

RAF em curso

2027

Fase 3 eduGAIN Consolidação

- Sirtfi em produção: declaração formal + processo de resposta a incidentes testado
- RAF implementado: IdPs libertam eduPersonAssurance conforme Perfil de Confiabilidade auditado
- Validação pela Federação e publicação em metadata

04 · Preparação e Conformidade

Começa já hoje a verificar o que tens de actualizar

eduGAIN Metadata Validator

https://technical.edugain.org/validator

Valida a metadata contra o perfil eduGAIN — campos em falta, erros de formato, warnings

Compliance Audit

technical.edugain.org/compliance_audit

Estado de compliance da federação RCTSaai face ao perfil SAML do eduGAIN

Attribute Release Check

release-check.edugain.org

Verifica se o IdP liberta os atributos corretos para SPs no contexto eduGAIN

Qualys SSL Labs

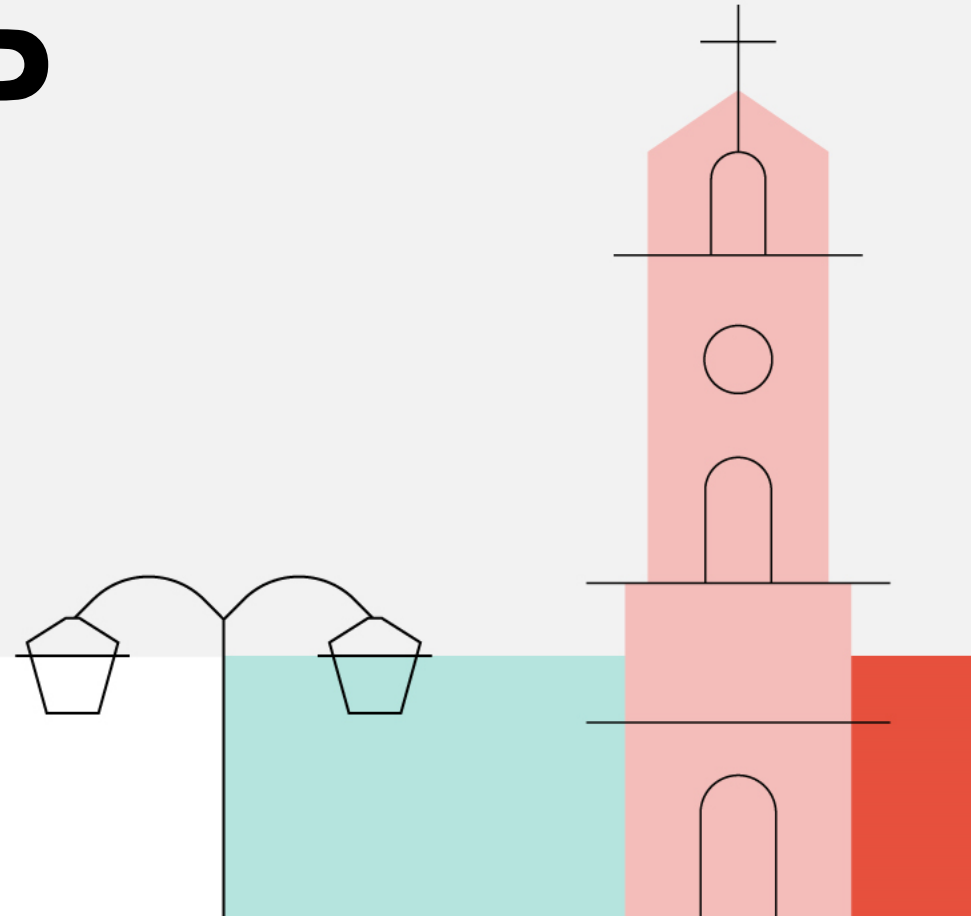
ssllabs.com/ssltest

Testa configuração TLS de um endpoint — deve obter rating A ou superior

jornadas FCCN

Atualização do IdP Shibboleth

v5.2.1 · novo playbook Ansible para Debian 13



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

05 · Shibboleth IdP 5.2.1 Playbook - o que há de novo

FCCN serviços digitais fct

RCTSaai eduGAIN Participantes Serviços Área Técnica Contactos FAQ

Shibboleth IdP 5.2.1 para Debian 13 - Integração com Active Directory

Nesta página vamos explicar como instalar um IDP Shibboleth 5.2.1 em Debian 13 integrado com uma Active Directory. Para esta instalação é utilizado um Playbook Ansible que automatiza a instalação e configuração do Apache2, Java 17.0.18, Tomcat 11.0.6, PostgreSQL e Shibboleth IDP 5.2.1 Este playbook permite fazer vários tipos de configuração. Permite:

- Instalar e configurar um IDP para ser possível fazer uma autenticação com a AD.
- Configurar um layout de acordo com a instituição.
- Instalar ou remover o plugin de autenticaçãoGov e configurá-lo para um ambiente de testes.
- Atualizar um IDP existente para a versão 5.2.1.

Estes métodos de instalação do playbook serão explicados em melhor detalhe na secção 2.1.

Playbook
Pode transferir o playbook através do link seguinte: Shibboleth IdP 5.2.1 para Debian 13 - Integração com AD.

1. Pré-requisitos
2. Configuração do playbook
   Descrição dos parâmetros a definir
   3.Tipos de instalação
4.Plugin Autenticacao.Gov
   Pré-requisitos
   Funcionamento do plug-in

1. Pré-requisitos

O primeiro passo a efectuar é instalar o pacote ansible e unzip.

```
shell> apt install ansible unzip
```

Crie a pasta Shibboleth_IDP_5.2.1, entre na nova diretoria e descomprima o código para dentro da mesma:

```
shell> mv shibboleth-idp-5-2-1-debian-ORG.zip Shibboleth_IDP_5.2.1
```

- Versão atual: Shibboleth IdP 5.2.1
- Playbook Ansible publicado no espaço técnico RCTSaai

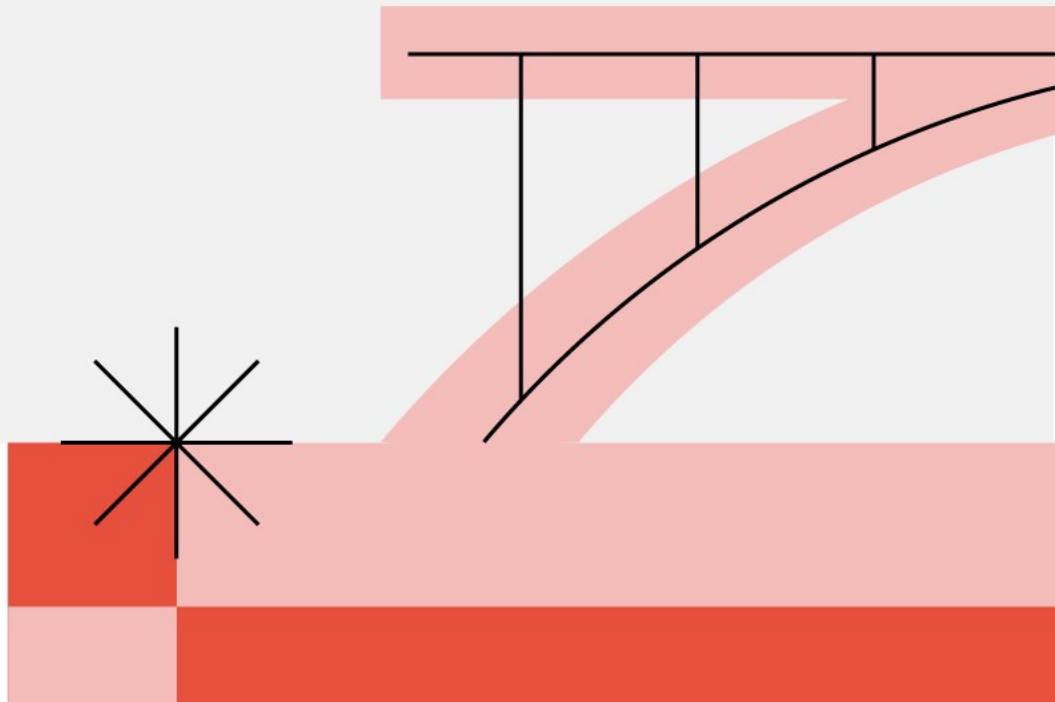
Novidades

- **Plugin Autenticação.GOV** compatível com 5.2.1
- **Certificados HTTPS** renovados automaticamente via ACME
- **SubjectID e Pairwise ID** prontos incluídos
- **Novos Filtros para Entity categories** pré-configuradas:
  - R&S
  - CoCo V2
  - Anonymous
  - Pseudonymous
  - Personalized

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO