eProcess

Especificação da segurança entre organizações envolvidas no BPMN end2end

Link Consulting – Tecnologias de Informação, S.A.

v1

Janeiro 2025

COMPETE 2030 PORTUGAL 2030 Cofinanciado pela União Europeia

Índice

Índice de Figuras

Índice de Tabelas

1 Introdução

A crescente digitalização dos processos empresariais e administrativos impõe desafios significativos de interoperabilidade, segurança e conformidade regulatória. No contexto do projeto eProcess, a necessidade de garantir a execução segura e confiável de processos que envolvem múltiplas organizações e aplicações exige uma abordagem estruturada para a gestão de riscos.

Este documento apresenta a especificação da segurança entre organizações envolvidas em processos que se podem expressar em BPMN, com foco na identificação e mitigação de riscos associados à interoperabilidade, fiabilidade, segurança da informação e gestão de níveis de serviço (SLA). A utilização do EdocLink é considerada como plataforma de gestão documental e automação de processos. Os desafios exemplificados podem ser aplicados, ou servir de guia de aplicação, em cenários em que diferentes empresas operam em conjunto, seja utilizando a mesma tecnologia ou integrando soluções distintas.

A especificação ilustra a identificação dos principais riscos inerentes ao contexto de múltiplas organizações, descrevendo causas de riscos, impactos e medidas de mitigação. São exemplificadas implicações da conformidade com normativas como o Regulamento Geral sobre a Proteção de Dados (RGPD), garantindo que a segurança da informação seja abordada de forma abrangente e alinhada às melhores práticas.

Por meio deste estudo, pretende-se fornecer um modelo sólido para avaliação e mitigação de riscos em processos BPMN distribuídos envolvendo a tecnologia EdocLink, guiando para que organizações colaborem de forma eficiente, segura e em conformidade com os requisitos legais e operacionais.

2 Descrição Geral

A crescente digitalização e automação de processos envolvendo múltiplas organizações impõem desafios significativos de interoperabilidade, segurança e conformidade regulatória. O EdocLink surge como uma plataforma robusta para gestão documental e automação de workflows, sendo amplamente utilizada para facilitar a execução de processos que envolvem múltiplas empresas e aplicações. No entanto, quando o EdocLink é adotado em cenários onde diferentes organizações interagem, algumas utilizando exclusivamente esta plataforma e outras combinando-a com soluções distintas, podem surgir riscos específicos que precisam ser geridos de forma estruturada.

A principal questão que se coloca é: **quais são os riscos que emergem quando as atividades de um processo BPMN são executadas em diferentes aplicações, operadas por múltiplas empresas, e como mitigar esses riscos?**

Para responder a essa questão, é essencial compreender os desafios associados à interoperabilidade, segurança da informação, fiabilidade operacional e conformidade regulatória. Esses desafios tornam-se ainda mais críticos à medida que processos envolvendo múltiplas organizações dependem de infraestruturas distribuídas, integração de sistemas distintos e mecanismos de transferência segura de dados e documentos.

Neste contexto, a segurança e integridade da informação desempenham um papel central. Processos de negócio que envolvem troca de documentos e dados entre entidades precisam garantir a confidencialidade, autenticidade e rastreabilidade de cada transação. A falta de padronização, a existência de diferentes versões do EdocLink, ou a integração com outros produtos podem levar a inconsistências operacionais, falhas de segurança e dificuldades na conformidade com normas como o Regulamento Geral sobre a Proteção de Dados (RGPD).

Além disso, a gestão eficaz dos níveis de serviço (SLA) é um fator determinante para o sucesso da colaboração entre organizações. Empresas envolvidas em processos BPMN distribuídos podem ter diferentes requisitos de desempenho, disponibilidade e tempos de resposta, o que pode comprometer a fluidez do "workflow" e impactar a eficiência global do processo. Portanto, definir acordos claros de interoperabilidade, mecanismos de monitorização ativa e políticas comuns de gestão de incidentes é essencial para garantir um funcionamento contínuo e seguro.

A análise de riscos apresentada neste documento ilustra como as ameaças mais relevantes podem ser estruturadas, e como medidas concretas de mitigação podem ser decididas. Nesta ilustração são categorizados riscos de integração e interoperabilidade, riscos de fiabilidade e disponibilidade, riscos de segurança da informação e riscos na gestão de SLA e monitorização. São ainda abordados, por exemplo, problemas decorrentes da incompatibilidade entre versões do EdocLink, falhas na transmissão segura de documentos, acesso não autorizado a informações confidenciais, impacto de "downtime" na continuidade dos processos e desafios relacionados à conformidade com requisitos legais e regulatórios.

Ao compreender e antecipar esses riscos, a Link pode ponderar e propor às organizações estabelecer estratégias proativas para fortalecer a segurança e a confiabilidade dos seus processos. A implementação de boas práticas de governança digital, integração segura e monitorização contínua permite não apenas reduzir a exposição a ameaças, mas também otimizar a colaboração entre empresas, garantindo maior eficiência e conformidade nas operações.

Este documento serve assim como um guia de referência para a Link e organizações que utilizam o EdocLink em processos envolvendo outras organizações, ajudando a uma boa gestão de risco.

3 Análise de riscos

A utilização do EdocLink por várias empresas num processo de colaboração expresso em BPMN e partilhado traz desafios significativos de integração, segurança e governança. A estruturação dos riscos com causas, eventos, consequências e medidas de mitigação permite uma abordagem proativa para minimizar impactos operacionais e estratégicos. As dimensões da análise dependerão de cada cenário concreto, sendo o que segue ilustrativo para um cenário genérico.

3.1 Riscos de Integração e Interoperabilidade

- Risco 1.1 - Incompatibilidade entre versões do EdocLink
    - Causa: Empresas utilizam versões diferentes do EdocLink, com configurações distintas.
    - Evento: Problemas na partilha de documentos e "workflows" devido a diferenças de funcionalidade ou estrutura de dados.
    - Consequência: Processos bloqueados, necessidade de retrabalho, aumento do tempo de resposta.
    - Controlo ou Mitigação:
        - Definir normas de configuração comuns para todas as empresas.
        - Realizar testes de interoperabilidade antes da entrada em produção.
        - Monitorizar atualizações do EdocLink e avaliar impactos antes da implementação.
- Risco 1.2 - Integração falhada entre EdocLink e outros produtos
    - Causa: Algumas empresas utilizam EdocLink como sistema principal, enquanto outras o integram com aplicações externas.
    - Evento: Inconsistências na troca de informação entre EdocLink e outros sistemas.
    - Consequência: Dados corrompidos, falha de processos automatizados, perda de produtividade.
    - Controlo ou Mitigação:
        - Utilizar APIs padronizadas e bem documentadas do EdocLink.
        - Criar mecanismos de validação de dados antes da troca entre sistemas.
        - Definir regras claras para "workflows" intersistémicos.

3.2 Riscos de Fiabilidade e Disponibilidade

- Risco 2.1 - Falha no acesso ao EdocLink
  - Causa: Problemas técnicos na infraestrutura cloud ou on-premise onde o EdocLink está alojado.
  - Evento: Empresas não conseguem aceder ao sistema para consulta ou registo de documentos.
  - Consequência: Atraso na execução de processos, perda de informação em operações críticas.
  - Controlo ou Mitigação:
    - Definir SLA rigorosos com garantias de "uptime".
    - Implementar redundância e "failover" para ambientes críticos.
    - Realizar testes regulares de continuidade de negócio.
- Risco 2.2 - Desempenho degradado em processos de alto volume
  - Causa: Aumento do volume de documentos ou processamento inadequado da infraestrutura.
  - Evento: Lentidão no carregamento e recuperação de documentos, impacto no tempo de resposta dos "workflows".
  - Consequência: Diminuição da eficiência operacional, frustração dos utilizadores, incumprimento de prazos.
  - Controlo ou Mitigação:
    - Monitorização ativa do desempenho do sistema.
    - Dimensionamento correto da infraestrutura com capacidade de escalabilidade.
    - Implementação de arquivamento automático para reduzir carga sobre o sistema ativo.

3.3 Riscos de Segurança da Informação

- Risco 3.1 - Acesso não autorizado a documentos sensíveis
  - Causa: Configuração inadequada de permissões de acesso entre empresas diferentes.
  - Evento: Utilizadores não autorizados conseguem visualizar ou modificar documentos confidenciais.
  - Consequência: Violação de segurança, exposição de informação estratégica ou legalmente protegida.
  - Controlo ou Mitigação:
    - Implementar gestão de acessos baseada em funções.

- Usar autenticação multifator (MFA) para acessos a dados críticos.
- Auditar periodicamente os acessos e permissões.

- Risco 3.2 - Perda ou corrupção de dados
  - Causa: Falhas no sistema, ataques cibernéticos ou erro humano.
  - Evento: Documentos eliminados ou alterados sem possibilidade de recuperação.
  - Consequência: Risco legal, impacto financeiro e necessidade de retrabalho.
  - Controlo ou Mitigação:
    - Implementação de backups automáticos e testados regularmente.
    - Utilização de assinaturas digitais e "logs" de auditoria para rastreamento de alterações.
    - Encriptação de dados em repouso e em trânsito.
- Risco 3.3 - Conformidade legal insuficiente (ex.: RGPD)
  - Causa: Falta de alinhamento entre os processos das empresas e os requisitos legais.
  - Evento: Armazenamento indevido de documentos com dados pessoais.
  - Consequência: Multas regulatórias, perda de credibilidade e riscos jurídicos.
  - Controlo ou Mitigação:
    - Definir políticas de retenção e eliminação de dados alinhadas com o RGPD.
    - Implementar registos de auditoria acessíveis apenas a pessoal autorizado.
    - Assegurar que todas as integrações cumprem requisitos legais.

3.4 Riscos na Gestão de SLA e Monitorização

- Risco 4.1 - Diferentes empresas têm SLAs distintos
  - Causa: Algumas empresas podem utilizar o EdocLink na "cloud", outras "on-premise", e com diferentes contratos de suporte.
  - Evento: Variação no tempo de resposta entre empresas no mesmo processo BPMN.

- Consequência: Dificuldade em garantir um fluxo de trabalho consistente.
- Controlo ou Mitigação:
  - Definir SLAs comuns entre as empresas envolvidas no processo.
  - Criar ferramentas centralizadas de monitorização de desempenho.
- Realizar reuniões periódicas de alinhamento operacional.

- 5. Riscos de Governança e Responsabilidade
  - Risco 5.1 - Falta de clareza sobre responsabilidades
  - Causa: Diferentes partes do processo BPMN são geridas por diferentes empresas, cada uma com o seu sistema.
  - Evento: Quando ocorre um problema, não há clareza sobre qual entidade deve resolvê-lo.
  - Consequência: Atraso na resolução de incidentes, aumento do custo operacional.
  - Controlo ou Mitigação:
    - Criar uma matriz de responsabilidades (RACI) para cada fase do processo.
    - Definir um processo de escalonamento de incidentes entre empresas.
    - Formalizar acordos contratuais claros sobre obrigações e níveis de serviço.
- Risco 5.2 - Mudanças descoordenadas no EdocLink
  - Causa: Atualizações do EdocLink feitas por uma empresa sem aviso às outras.
  - Evento: Disrupção dos processos automatizados que dependem do sistema.
  - Consequência: Falha nos fluxos de trabalho e necessidade de ajustes emergenciais.
  - Controlo ou Mitigação:
    - Estabelecer um processo formal de homologação para novas versões do EdocLink.
    - Criar um ambiente de testes conjunto antes de implementar mudanças.
    - Garantir comunicação antecipada de atualizações entre todas as partes.

4 Exemplo – Processo Px

O cenário que, embora muito simples, pode ilustrar vários desafios de interoperabilidade, segurança da informação e conformidade legal devido à colaboração entre múltiplas empresas e aplicações. A implementação das ações de mitigação adequadas pode reduzir significativamente os riscos e garantir que o processo decorre de forma segura e eficiente:

Cenário:

- A **empresa E1** inicia o processo **Px** executando a tarefa **T1** na aplicação **App1**, que gera o **documento Doc1**.
- O **Doc1** é enviado para a aplicação **App2** da **empresa E2**, que é uma aplicação **EdocLink** e executa a tarefa **T2**, produzindo o **documento Doc2**.
- O **Doc2** é enviado para a aplicação **App3** da **empresa E3**, que gera o **documento Doc3**.
- O **Doc3** é enviado para a aplicação **App4** da **empresa E1**, que também é uma aplicação **EdocLink**.
- Todos os documentos contêm **informação confidencial e dados pessoais**, sendo necessário **garantir a privacidade e conformidade legal**.

4.1 Risco 1 - Interoperabilidade entre aplicações diferentes

- **Causa:** A empresa **E1** usa **App1 e App4**, sendo App4 uma aplicação **EdocLink**, mas a **App1** pode ter um formato de documento incompatível com o **App2 (EdocLink)** da empresa **E2**.
- **Evento:** O documento **Doc1** pode não ser corretamente interpretado ao entrar no **App2 (EdocLink)** da empresa **E2**.
- **Consequência:** Possível perda ou corrupção de dados no **Doc1**, podendo resultar em falhas na tarefa **T2** e impactar o restante processo.
- **Controlo ou Mitigação:**
  - Garantir que **App1** e **App2 (EdocLink)** suportam **formatos de ficheiro comuns** (ex.: PDF/A, XML, JSON).
  - Implementar **validação automática** no momento da receção do documento.
  - Criar **testes de interoperabilidade periódicos** para garantir que os formatos de documentos são compatíveis.

4.2 Risco 2 - Falha na transmissão segura dos documentos

- **Causa:** O **Doc1, Doc2 e Doc3** são trocados entre empresas via **redes externas** (internet, VPNs, APIs), podendo ser alvo de interceção ou modificação maliciosa.
- **Evento:** Um atacante pode capturar ou adulterar os documentos durante a transmissão entre empresas.
- **Consequência: Violação de confidencialidade e integridade dos documentos**, expondo dados sensíveis e resultando em **não conformidade com o RGPD**.
- **Controlo ou Mitigação:**
  - Usar **encriptação ponta a ponta** (ex.: TLS 1.3) para proteger os documentos em trânsito.
  - Implementar **assinaturas digitais** para garantir a integridade dos documentos.
  - Configurar **firewalls e IDS/IPS** para monitorizar o tráfego entre as aplicações.

4.3 Risco 3 - Acesso não autorizado a documentos armazenados

- **Causa:** Diferentes empresas utilizam **diferentes políticas de gestão de acessos**, podendo permitir que utilizadores não autorizados visualizem documentos sensíveis.
- **Evento:** Um utilizador da empresa **E2 ou E3** pode aceder a um documento sem permissão.
- **Consequência: Fuga de informação confidencial** e possíveis penalizações legais.
- **Controlo ou Mitigação:**
  - Definir **gestão de acessos baseada em funções (RBAC – Roll Based Access Control)** nas aplicações.
  - Implementar **autenticação multifator (MFA)** para todos os utilizadores com acesso aos documentos.
  - Monitorizar "**logs" de acesso e atividades suspeitas** nos sistemas.

4.4 Risco 4 - Perda ou corrupção de documentos

- **Causa:** Falhas técnicas nos servidores das empresas **E1, E2 ou E3**, ataques de "ransomware" ou erro humano.
- **Evento:** Um documento pode ser perdido ou corrompido antes de completar o ciclo **T1 → T2 → T3 → T4**.
- **Consequência: Interrupção do processo Px**, necessidade de refazer documentos, impacto na eficiência operacional.
- **Controlo ou Mitigação:**
  - Implementar **backups automáticos** e testá-los regularmente.
  - Usar **gestão de versões de documentos** para garantir que uma cópia anterior está disponível.
  - Criar em cada empresa um **plano de recuperação de desastres** para reposição rápida dos dados.

4.5 Risco 5 - Falta de conformidade com o RGPD

- **Causa:** Os documentos contêm **dados pessoais** e podem ser armazenados por períodos superiores ao permitido pelo **RGPD**.
- **Evento:** A empresa pode reter documentos além do tempo necessário ou não garantir a eliminação segura dos dados.
- **Consequência: Sanções regulatórias**, incluindo multas elevadas e danos reputacionais.
- **Controlo ou Mitigação:**
  - Definir em cada empresa as **políticas de retenção de dados** alinhadas com o RGPD.
  - Implementar **mecanismos automáticos de anonimização e eliminação segura de documentos**.
  - Garantir que todas as empresas assinam um **Acordo de Processamento de Dados (DPA)**.

4.6 Registo de riscos

Tabela 1: Plano de Mitigação para o processo Px

ID	Risco	Ação de Mitigação	Responsável	Prioridade
R1	Incompatibilidade entre aplicações	Padronizar formatos de documentos e validar compatibilidade	Equipas de engenharia de E1, E2 e E3	Alta
R2	Falha na transmissão segura	Implementar encriptação TLS 1.3 e assinaturas digitais	Equipas de segurança de E1, E2 e E3	Alta
R3	Acesso não autorizado	Aplicar gestão de acessos por função (RBAC) e autenticação multifator (MFA) em todas as aplicações	Responsáveis de segurança de cada empresa	Alta
R4	Perda ou corrupção de documentos	Criar backups automáticos e mecanismos de versionamento	Equipas de engenharia de E1, E2 e E3	Média
R5	Não conformidade com o RGPD	Definir políticas de retenção e eliminação segura	Responsável de conformidade (“Compliance Officer”) de cada empresa	Alta