POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Automatização da Segurança em Sistemas SAP

Uma Abordagem Baseada em Análise de Vulnerabilidades e Mitigação de Riscos

Rúben da Costa Mendes

Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança & Informática Forense

Leiria, Julho 2026

Página intencionalmente deixada em branco.

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Automatização da Segurança em Sistemas SAP

Uma Abordagem Baseada em Análise de Vulnerabilidades e Mitigação de Riscos

Rúben da Costa Mendes

Supervisor: Dulce Gonçalves
Assistant Professor, Polytechnic University of Leiria

Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança & Informática Forense

Projeto

Leiria, Julho 2026

Página intencionalmente deixada em branco.

Automatização da Segurança em Sistemas SAP

O presente trabalho beneficiou da utilização do modelo *IPLeiria-Thesis*.

Página intencionalmente deixada em branco.

Agradecimentos

Na secção de agradecimentos, expresso a minha sincera gratidão a todos aqueles que, de alguma forma, contribuíram para a realização deste projeto.

Em primeiro lugar, agradeço à minha família, em especial aos meus pais e à minha irmã, pelo apoio incondicional ao longo de todo o percurso, tanto a nível pessoal como académico e profissional.

Agradeço também a todos os professores do curso pelos conhecimentos transmitidos ao longo do mestrado, com um reconhecimento especial à orientadora, Professora Dulce Gonçalves, pela orientação, disponibilidade e acompanhamento ao longo deste trabalho.

Aos meus colegas de mestrado, deixo igualmente um agradecimento pelo constante incentivo, motivação e espírito de entreajuda, fundamentais para a concretização deste projeto.

Aos meus amigos fora do contexto académico, agradeço o apoio e encorajamento, mesmo não estando diretamente ligados à área de estudo.

Um agradecimento especial ao meu amigo e colega Bruno Pereira, pela sua disponibilidade contínua para ajudar em temas relacionados com SAP Basis, e ao meu amigo Mickaël Santos, pelo apoio prestado nas questões ligadas à programação.

Por fim, mas não menos importante, agradeço ao Grupo Rolear por ter acolhido este projeto e por disponibilizar os seus sistemas para a realização dos testes, tornando possível a concretização prática deste projeto.

Página intencionalmente deixada em branco.

Resumo

A segurança dos sistemas SAP assume um papel crítico na proteção da informação empresarial, uma vez que estes sistemas suportam processos de negócio fundamentais em muitas organizações. No entanto, a análise de configurações de segurança em ambientes SAP continua frequentemente a ser realizada de forma manual, exigindo elevado conhecimento técnico e um investimento significativo de tempo por parte das equipas de administração e auditoria, através de ferramentas SAP que são complexas de configurar ou por ferramentas privadas bastante dispendiosas.

O presente projeto propõe o desenvolvimento de uma aplicação *web* destinada à automatização da análise de segurança em sistemas SAP, com os objetivos de identificar vulnerabilidades, avaliar o nível de conformidade das configurações e apoiar a mitigação de riscos operacionais. A solução desenvolvida integra um *backend* implementado em *Java*, responsável pela execução das verificações de segurança e comunicação com os sistemas SAP através de ligações RFC e com o *frontend* desenvolvido em React/-Next.js que permite a configuração de auditorias, visualização de resultados e gestão de relatórios.

A aplicação implementa um conjunto de verificações automáticas com base em recomendações de segurança documentadas pela própria SAP, incluindo análise de contas padrão, parâmetros de autenticação, configurações de RFC, permissões críticas e exposição de serviços *web*. Os resultados obtidos durante os testes demonstram que a solução é capaz de identificar vulnerabilidades reais em sistemas SAP e reduzir significativamente o tempo necessário para realizar auditorias de segurança.

Desta forma, o trabalho contribui para a melhoria dos processos de auditoria em ambientes SAP, promovendo uma abordagem mais eficiente, sistemática e alinhada com as boas práticas de segurança.

Palavras-Chave: SAP, Cibersegurança, Auditoria de Segurança, Automatização, Sistemas ERP.

Página intencionalmente deixada em branco.

Abstract

The security of SAP systems plays a critical role in protecting enterprise information, as these systems support core business processes in many organisations. However, the analysis of security configurations in SAP environments is still frequently performed manually, requiring specialised technical knowledge and significant effort from system administrators and auditors.

This project proposes the development of a web application designed to automate security analysis in SAP systems, with the objective of identifying vulnerabilities, assessing configuration compliance and supporting risk mitigation. The developed solution integrates a Java-based backend responsible for executing security checks and communicating with SAP systems through RFC connections, as well as a React/Next.js frontend that enables audit configuration, result visualisation and report management.

The application implements a set of automated checks based on security recommendations documented by SAP, including the analysis of default accounts, authentication parameters, RFC configurations, critical authorisations and exposed web services. The results obtained during testing demonstrate that the solution is capable of identifying real vulnerabilities in SAP systems and significantly reducing the time required to perform security audits.

Overall, this work contributes to improving security auditing processes in SAP environments by providing a more efficient, systematic and scalable approach aligned with recognised security best practices.

Keywords: SAP, Cybersecurity, Security Auditing, Automation, ERP Systems.

Página intencionalmente deixada em branco.

Declaração sobre o Uso de Inteligência Artificial

Durante a elaboração deste projeto foram utilizadas ferramentas de Inteligência Artificial como apoio auxiliar em diferentes fases do trabalho. A utilização destas ferramentas teve como objetivo melhorar a eficiência do processo de investigação, desenvolvimento e redação do documento, mantendo sempre a responsabilidade intelectual do autor sobre o conteúdo final.

Em primeiro lugar, ferramentas com base em Inteligência Artificial foram utilizadas como apoio à pesquisa de bibliografia e clarificação de conceitos técnicos relacionados com cibersegurança, sistemas ERP e arquitetura dos sistemas SAP, o que contribuiu para identificar fontes relevantes e aprofundar a compreensão de determinados tópicos abordados no trabalho.

Adicionalmente, estas ferramentas foram utilizadas para apoio à melhoria da qualidade linguística do texto, nomeadamente ao nível do vocabulário, clareza de expressão e correção gramatical, permitindo refinar a redação académica sem alterar o conteúdo científico produzido pelo autor.

Por fim, ferramentas de Inteligência Artificial foram também utilizadas de forma pontual como apoio ao desenvolvimento técnico da aplicação, nomeadamente para sugerir melhorias em fragmentos de código desenvolvidos em *Java* e *React*, bem como para auxiliar na análise de problemas de implementação durante o desenvolvimento do *backend* e do *frontend*.

Importa ainda salientar que todas as decisões técnicas, científicas e metodológicas apresentadas neste trabalho são da responsabilidade exclusiva do autor, tendo as ferramentas de Inteligência Artificial sido utilizadas apenas como apoio complementar.

Conteúdo

Página intencionalmente deixada em branco.

Lista de Figuras

Página intencionalmente deixada em branco.

Lista de Tabelas

Página intencionalmente deixada em branco.

Siglas

ABAP Advanced Business Application Programming. (*p. 20, 23, 27, 71, 74, 75*)
ACL Access Control List. (*p. 24, 25, 32, 38, 68*)
AES Advanced Encryption Standard. (*p. xiii, 34, 47, 49*)
API Application Programming Interface. (*p. 40, 43–45, 51, 54, 75*)
AS Application Server. (*p. 26*)
AWS Amazon Web Services. (*p. 16*)

CISA Cybersecurity and Infrastructure Security Agency. (*p. 26*)
CO Controlling Obejcts. (*p. 66*)
CORS Cross-Origin Resource Sharing. (*p. 44*)
CRM Customer Relationship Management. (*p. 9, 12*)
CVE Common Vulnerabilities and Exposures. (*p. 27, 28*)

DES Development System. (*p. 66*)
DTO Data Transfer Object. (*p. 44*)

ERP Enterprise Resource Planning. (*p. xiii, 4–15, 17–20*)

FI Financial Accounting. (*p. 66*)

GCM Galois/Counter Mode. (*p. xiii, 34, 47, 49, 55*)

HR Human Resources. (*p. 66*)
HTTP Hypertext Transfer Protocol. (*p. 44, 47, 54, 68*)

IA Inteligência Artificial. (*p. 13*)
ICF Internet Communication Framework. (*p. 24, 25*)
IDES Internet Demonstration and Evaluation System. (*p. 2, 65, 66*)

JCo SAP Java Connector. (*p. 38, 43, 44, 46*)
JPA Java Persistence API. (*p. 44, 47, 49, 52*)
JSON JavaScript Object Notation. (*p. 45, 47, 54*)
JWT JSON Web Token. (*p. xiii, 44, 45, 47, 48, 50, 51, 54*)

MM Materials Management. (*p. 66*)
MRP Material Requirements Planning. (*p. 7*)

PDF Portable Document Format. (*p. 35, 52, 55*)

QAS Quality Assurance System. (*p. 66*)

REST Representational State Transfer. (*p. 40, 43, 44, 51, 54*)
RFC Remote Function Call. (*p. 2, 3, 20, 22–25, 29, 32, 38, 39, 41, 43–46, 66–70, 73–75*)
RGPD Regulamento Geral sobre a Proteção de Dados. (*p. 6*)

SAP Systems, Applications and Products in Data Processing. (*p. xv, 1–4, 10, 13–16, 19–24, 26–29, 31–35, 37–47, 49–57, 59–63, 65–71, 73–76*)
SCM Supply Chain Management. (*p. 9*)
SD Sales and Distribution. (*p. 66*)
SHA Secure Hash Algorithm. (*p. 49*)
SOAP Simple Object Access Protocol. (*p. 38, 54, 68*)
SoD Segregation of Duties. (*p. 12, 18, 24, 75*)
SQL Structured Query Language. (*p. 41, 44*)

TI Tecnologias da Informação. (*p. 5, 9, 31*)

URL Uniform Resource Locator. (*p. 24, 50*)

Página intencionalmente deixada em branco.

1

Introdução

A segurança da informação assume, atualmente, um papel central na proteção dos processos de negócio das organizações, sendo determinante para a preservação da integridade, confidencialidade e disponibilidade dos dados. No contexto das médias e grandes empresas, os sistemas SAP destacam-se como plataformas críticas de gestão empresarial, integrando vários módulos que suportam processos como finanças, recursos humanos, produção, logística, compras e gestão de acessos. A sua abrangência e complexidade tornam-nos essenciais para o funcionamento interno das organizações, mas, simultaneamente, expõem um vetor de risco significativo caso as configurações de segurança não sejam corretamente implementadas e monitorizadas.

As análises realizadas durante este projeto são tradicionalmente realizadas de forma manual, envolvendo auditorias a parâmetros internos, perfis de utilizadores e políticas de autorizações e *passwords*. Contudo, este processo apresenta limitações relevantes: requer elevado conhecimento técnico especializado, é demorado, depende da interpretação humana e está sujeito a erros, o que frequentemente resulta em vulnerabilidades não mitigadas.

Tendo em conta estes desafios, este projeto apresenta o desenvolvimento de uma aplicação *web* destinada à automatização da análise de segurança em sistemas SAP, com capacidade para identificar vulnerabilidades, avaliar níveis de *compliance* (de acordo com as normas SAP) e propor ações de mitigação. A aplicação recorre a um *backend* desenvolvido em Java e a um *frontend* construído em Next.js, permitindo interação intuitiva e geração de visualizações gráficas para facilitar a interpretação dos resultados obtidos.

Este trabalho enquadra-se na área da cibersegurança no âmbito do mestrado em Cibersegurança e Informática Forense, contribuindo para a redução de esforço manual em processos de auditoria, para o reforço da maturidade de segurança das organizações e para a mitigação dos riscos operacionais associados à exploração de vulnerabilidades em SAP.

1.1 Motivação

O desenvolvimento deste projeto resulta da experiência profissional do autor na área de SAP BASIS, exercida enquanto consultor externo no Grupo Rolear. A manutenção e segurança de sistemas SAP constituem responsabilidades centrais. Ao longo da prática diária, torna se evidente que a segurança dos ambientes SAP continua a ser um dos pilares essenciais para garantir a continuidade operacional, a integridade dos dados e a conformidade com requisitos internos e externos das organizações

A repetição constante de verificações como a análise de contas padrão, revisão de parâmetros críticos, avaliação de Remote Function Calls (RFCs) e validação de autorizações torna-se não só dispendiosa, mas também arriscada, sobretudo quando não existe uma abordagem sistemática e automatizada.

Assim, a motivação para este projeto nasce da necessidade de criar uma solução que responda a estas limitações, proporcionando uma ferramenta que permita automatizar, padronizar e centralizar a análise de segurança em sistemas SAP. A partir da observação de problemas reais em diferentes ambientes, desde sistemas de desenvolvimento e teste até sistemas completos como o Internet Demonstration and Evaluation System (IDES) e sistemas de Produção, tornou-se claro que a existência de uma aplicação capaz de identificar vulnerabilidades de forma contínua e estruturada representa um valor significativo para equipas de BASIS e de auditoria.

Além disto, a motivação é reforçada pela oportunidade de contribuir para a evolução das práticas de segurança SAP, demonstrando que é possível combinar *frameworks* modernas (Next.js e Spring Boot) com tecnologias SAP tradicionais (RFCs) para criar soluções inovadoras que respondam a desafios reais do mercado. Acredita-se que uma ferramenta com estas características pode, não apenas melhorar a eficiência operacional, mas também elevar significativamente o nível de segurança dos sistemas SAP.

Após a implementação e validação, a aplicação passou a ser utilizada no contexto das atividades de administração SAP desenvolvidas pelo autor no Grupo Rolear, apoiando a execução das análises de segurança e reduzindo o esforço associado às auditorias manuais.

Em suma, este projeto procura dar resposta a uma necessidade identificada no contexto profissional e pretende constituir um contributo relevante para a área de administração e segurança SAP, oferecendo uma abordagem moderna, automatizada e tecnicamente robusta para lidar com vulnerabilidades que, de outra forma, poderiam passar despercebidas.

1.2 Objetivos

O objetivo geral deste projeto consiste em desenvolver uma aplicação capaz de automatizar a análise de vulnerabilidades e mitigar possíveis problemas de segurança nos sistemas SAP através das recomendações disponibilizadas no relatório da auditoria. Para alcançar este propósito, definem-se os seguintes objetivos específicos:

- Identificar parâmetros, perfis, *webservices*, RFCs, mandantes[1] e configurações SAP suscetíveis de originar problemas de segurança;
- Implementar mecanismos de avaliação automática de vulnerabilidades, classificando resultados segundo níveis de *compliance* da documentação SAP;
- Sugerir a correção manual de configurações consideradas inseguras, relatadas e documentadas no relatório;
- Integrar visualização gráfica para apoiar a interpretação e priorização das ações de mitigação no menu principal do utilizador;
- Centralização de relatórios de modo a permitir ao utilizador ter um histórico de versões e informações dos sistemas analisados.
- Garantir a conformidade com políticas de segurança internas e documentação oficial SAP.

1.3 Caracterização da Entidade Recetora do Projeto

O Grupo Rolear, fundado em 1979, destaca-se como um dos principais fornecedores de soluções energéticas e tecnológicas em Portugal. Com sede no Algarve e filiais distribuídas pelo território nacional, o grupo opera em áreas como climatização, energia renovável, automação, canalização e instalações elétricas. Com uma infraestrutura robusta e um forte compromisso com inovação e sustentabilidade, a Rolear atende clientes em diferentes tipos de mercado, disponibilizando produtos de alta qualidade e soluções personalizadas.

1.3.1 Acolhimento na Entidade Recetora

O ambiente de desenvolvimento fornecido pelo Grupo Rolear para o projeto caracteriza-se por uma infraestrutura atualizada e bem organizada, com destaque para a implementação de sistemas SAP que suportam as operações críticas e toda a lógica de negócio da empresa. Este cenário proporciona um ambiente ideal para a criação e integração de soluções tecnológicas. Durante o desenvolvimento da aplicação, foi disponibilizado acesso aos recursos necessários, bem como ao suporte técnico das equipas especializadas da empresa, promovendo uma colaboração eficiente e produtiva.

1.3.2 Projeto no Contexto do Grupo Rolear

O projeto consiste no desenvolvimento de uma aplicação com o objetivo de integrar com os sistemas SAP utilizados pelo Grupo Rolear, o que contribui diretamente para a melhoria dos processos internos de análise e resolução de incidentes de segurança. A solução desenvolvida permite ainda aumentar a eficiência operacional, reduzir o tempo de resposta a problemas e minimizar o esforço manual associado a estas tarefas, o que se traduz numa utilização mais eficaz dos recursos da organização e no reforço

[1] Mandantes no SAP são unidades lógicas independentes dentro do sistema, cada uma com os seus próprios dados, configurações e utilizadores, permitindo existir diferente informação no mesmo sistema

da fiabilidade dos sistemas. A aplicação foi testada em todo os *landscape* SAP do Grupo Rolear, garantindo que esteja alinhada com os fluxos de trabalho existentes e com as necessidades específicas da organização.

Ao longo do projeto, foram realizadas análises detalhadas da infraestrutura da empresa, incluindo a arquitetura dos sistemas SAP, os requisitos funcionais e o nível de segurança dos sistemas SAP. Este trabalho colaborativo permitiu que a aplicação responda aos padrões de qualidade e segurança necessários para o suporte às operações da Rolear de forma confiável e escalável.

1.4 Estrutura do Documento

O presente documento encontra-se organizado em nove capítulos que abordam de forma progressiva o enquadramento do problema, o desenvolvimento da solução proposta, a apresentação dos resultados e as respetivas conclusões.

O Capítulo 1 introduz o tema do trabalho, contextualizando o problema, definindo os objetivos da investigação e descrevendo a metodologia adotada.

No Capítulo 2 são apresentados os conceitos fundamentais associados aos sistemas ERP, incluindo a sua evolução, características principais e o papel que desempenham nas organizações.

O Capítulo 3 centra-se na plataforma SAP, descrevendo a sua arquitetura, os principais componentes do ecossistema e os aspetos mais relevantes do ponto de vista da segurança.

De seguida, o Capítulo 4 reúne o enquadramento teórico e o trabalho relacionado, analisando normas, recomendações e abordagens existentes para a análise de segurança em sistemas SAP.

A análise e especificação do sistema proposto são apresentadas no Capítulo 5, onde se descrevem os requisitos identificados, a arquitetura da solução e as tecnologias utilizadas.

O Capítulo 6 detalha o processo de desenvolvimento da aplicação, incluindo os principais componentes implementados e as decisões técnicas tomadas durante a implementação.

Posteriormente, o Capítulo 7 descreve os mecanismos de visualização e exploração dos resultados das auditorias realizadas pela aplicação.

No Capítulo 8 são apresentados os resultados obtidos e a respetiva avaliação da solução, incluindo os testes efetuados e a análise do desempenho do sistema.

Por fim, o Capítulo 9 reúne as principais conclusões do trabalho desenvolvido e identifica possíveis direções para trabalho futuro.

2

Caracterização de Sistemas ERP

Num cenário empresarial cada vez mais competitivo, as organizações enfrentam uma necessidade crescente de aceder a informação quase em tempo real, não apenas sobre os seus concorrentes, mas, acima de tudo, acerca do desempenho das suas operações. Para responder a esta exigência, muitas empresas têm optado pela adoção de sistemas que ajudam estes processos, como os *Enterprise Resource Planning* (ERP).

Nos anos 90, assistiu-se a uma mudança significativa na estratégia das empresas no que respeita às Tecnologias da Informação (TI). Em vez de desenvolverem internamente o seu *software*, as organizações começaram a adquirir aplicações de gestão desenvolvidas por fornecedores externos, entre as quais os sistemas ERP.

Os sistemas ERP são sistemas de informação configuráveis capazes de integrar dados e processos de negócio em todas as áreas funcionais de uma organização (Kumar et al., 2000). Estas soluções distinguem-se pela utilização de uma base de dados única, associada a uma aplicação integrada e a uma interface simples e uniforme.

São também desenvolvidos para facilitar as operações empresariais, proporcionando integração, planeamento em tempo real e resposta eficiente às necessidades dos utilizadores. Adicionalmente, incorporam melhores práticas de gestão, desenvolvidas a partir da análise de processos bem-sucedidos em organizações semelhantes (O'Leary, 2000).

Contudo, a implementação destes sistemas requer cautela, de modo a evitar alterações excessivas que possam comprometer o desempenho, dificultar futuras atualizações ou aumentar os custos de manutenção.

Frequentemente, os ERPs são escolhidos por empresas cujos processos de negócio já estão bem definidos. Contudo, nem sempre estes sistemas oferecem funcionalidades capazes de acomodar diretamente esses processos e, em muitos casos, é necessário personalizar o ERP para suportar as operações existentes, o que pode resultar em limitações como maior complexidade na manutenção ou menor alinhamento com as melhores práticas. Alternativamente, a empresa pode optar por ajustar os seus processos internos de forma a refletirem os fluxos padrão do sistema implementado (Davenport, 1998).

Apesar de abrangentes, os ERPs não são soluções universais para todos os desafios empresariais. Embora integrem os processos mais comuns, nem sempre conseguem responder plenamente às especificidades e necessidades de cada organização, sendo necessário um esforço de adaptação e alinhamento com todas as equipas de modo a que o ERP fique encaixado com toda a dinâmica da empresa.

2.1 Estrutura e Funcionalidades

Os sistemas ERP são compostos por uma arquitetura modular, onde cada módulo representa uma área funcional do negócio, tais como:

- **Gestão Financeira:** Inclui contabilidade geral, controlo de custos e gestão de tesouraria.
- **Recursos Humanos:** Abrange funções de recrutamento, formação, gestão de salários e benefícios.
- **Produção e Logística:** Envolve planeamento de produção, gestão de inventário, cadeia de abastecimento e distribuição.
- **Vendas e Marketing:** Foca-se na gestão de encomendas, faturação e análise de mercado.

A integração destas áreas permite que os dados fluam entre os diferentes departamentos, garantindo que a informação esteja sempre atualizada e acessível em tempo real.

2.2 Benefícios dos ERP

A implementação de um ERP proporciona diversos benefícios que vão além da simples automatização de processos. Entre os principais destacam-se (Chang, 2025):

- **Integração de Dados:** Centraliza todas as informações numa única base de dados, reduzindo erros e redundâncias.
- **Eficiência Operacional:** Automatiza tarefas repetitivas e melhora a produtividade dos colaboradores.
- **Transparência e Rastreabilidade:** Facilita a monitorização de processos e a identificação de gargalos operacionais.
- **Tomada de Decisões Informadas:** Proporciona acesso a dados em tempo real, permitindo decisões mais rápidas e fundamentadas.
- **Adaptação a Normas:** A adaptação a normas constitui uma das principais vantagens dos sistemas ERP, uma vez que estes suportam a conformidade com regulamentos como o Regulamento Geral sobre a Proteção de Dados (RGPD), através de mecanismos de controlo interno integrados e auditorias contínuas.

2.3 Desafios e Limitações

Apesar dos inúmeros benefícios, a implementação de um ERP não é isenta de desafios:

- **Custo Elevado:** Inclui investimento inicial, custos de licenciamento, consultoria e formação.
- **Complexidade de Implementação:** Requer uma análise detalhada dos processos existentes e planeamento rigoroso.
- **Resistência à Mudança:** A adoção por parte do dos utilizadores pode constituir um obstáculo, especialmente em organizações com processos enraizados.
- **Risco de Dependência:** Personalizações excessivas podem dificultar atualizações futuras e aumentar os custos de manutenção (Umble et al., 2002).

2.4 Evolução dos Sistemas ERP

A evolução dos ERPs resulta de um processo gradual de maturação tecnológica e de transformação das necessidades de gestão das organizações. A sua origem remonta às primeiras tentativas de informatizar processos industriais, evoluindo até aos atuais ecossistemas integrados e distribuídos.

Anos 1960: O surgimento do MRP

A primeira geração de sistemas de gestão integrada surgiu nos anos 1960 com o Material Requirements Planning (MRP), que se destinava a calcular necessidades de materiais para processos de produção (Jacobs et al., 2007).

Estes sistemas permitiam planear compras e controlar inventários, tornando-se num marco fundamental para a digitalização da produção. Apesar da sua utilidade, tinham limitações, nomeadamente a incapacidade de integrar outras áreas de gestão.

Anos 1970: MRP II e a expansão para além da produção

Na década de 1970, os sistemas evoluíram para MRP II – Manufacturing Resource Planning, incorporando funcionalidades adicionais relacionadas com capacidade produtiva e planeamento mais alargado dos recursos organizacionais (Jacobs et al., 2007).

O MRP II introduziu uma visão mais abrangente dos recursos da organização, constituindo um passo relevante em direção à integração empresarial.

Anos 1980: Informatização crescente e modularidade

Durante os anos 1980, assistiu-se a uma expansão significativa da informatização empresarial. Os sistemas tornaram-se progressivamente mais abrangentes, preparando o terreno para o conceito moderno de ERP (Jacobs et al., 2007).

Anos 1990: Consolidação do ERP moderno

A década de 1990 é amplamente reconhecida como o momento de consolidação do ERP tal como é entendido atualmente. O termo ERP foi popularizado no início da década de 1990 para descrever sistemas integrados que unificavam múltiplas funções organizacionais num único ambiente (Jacobs et al., 2007).

Os sistemas passaram a integrar funcionalidades que cobriam praticamente todos

os processos centrais da organização: finanças, recursos humanos, logística, vendas, produção e compras. Esta integração permitiu ganhos significativos de eficiência e alinhamento organizacional (Davenport, 1998).

Anos 2000: Globalização e integração alargada

Nos anos 2000, os ERPs evoluíram para suportar ambientes mais distribuídos e cadeias de valor alargadas, surgindo o conceito de ERP II ou *extended enterprise systems* (Møller, 2005).

Neste período intensificaram-se também as preocupações com governação, controlo interno e segregação de funções, sendo propostas abordagens de monitorização contínua de conformidade em sistemas ERP (Wolf et al., 2009).

Anos 2010: *Cloud Computing* e novos modelos de implementação

A década de 2010 marcou uma mudança estrutural com a adoção crescente de soluções ERP em *cloud*. Revisões sistemáticas identificam benefícios como escalabilidade, redução de custos de infraestrutura e maior flexibilidade, bem como desafios associados à segurança e dependência do fornecedor (Abd Elmonem et al., 2016).

Anos 2020 até ao presente: ERP inteligente e reforço da segurança

Os ERPs modernos caracterizam-se pela forte integração, elevada conectividade e crescente incorporação de mecanismos de controlo e monitorização contínua. A segurança e a conformidade regulamentar assumem um papel central, dada a criticidade dos processos e dados suportados (Wolf et al., 2009).

Atualmente, a segurança é um pilar central na adoção de ERP, dada a natureza sensível dos dados que processam e a criticidade dos processos que suportam. A evolução dos ERPs está intrinsecamente ligada às exigências de proteção de informação, continuidade de negócio e conformidade regulamentar.

2.5 Ciclo de Vida dos ERP

O ciclo de vida de um sistema ERP é descrito em seis fases principais, que acompanham todo o percurso do sistema, desde a sua adoção inicial até à substituição (Bjelland et al., 2018).

1. **Fase de Decisão de Adoção:** Nesta fase, as organizações começam a analisar as suas necessidades empresariais e técnicas, questionando a utilidade de um ERP para alcançar os seus objetivos estratégicos. É o momento em que se avalia a capacidade de um ERP para melhorar os processos de negócio, integrar fluxos de informação e gerar valor para a organização. Esta etapa exige uma análise cuidadosa do impacto que a adoção do ERP terá sobre a estrutura organizacional e os seus processos existentes.
2. **Fase de Aquisição:** A fase de aquisição centra-se na seleção do fornecedor e do

sistema ERP. Após identificar os requisitos do negócio, a organização avalia as opções disponíveis no mercado e escolhe o *software* que melhor se adapta às suas necessidades. Este processo inclui comparações entre diferentes fornecedores, análise de propostas e demonstrações práticas do *software*. É crucial envolver as equipas de negócio e TI para assegurar uma escolha informada.

3. **Fase de Implementação:** Esta é a etapa mais crítica e exigente do ciclo de vida. Envolve a instalação do sistema, a configuração para atender às especificidades da organização, a migração de dados a partir de sistemas anteriores e a formação de utilizadores. Adicionalmente, a implementação pode incluir a reengenharia de processos para alinhar os fluxos de trabalho às funcionalidades do ERP. A fase de implementação exige uma gestão de projetos rigorosa, dado que é a mais dispendiosa e demorada de todas as fases.
4. **Fase de Uso e Manutenção:** Uma vez implementado, o sistema começa a ser utilizado diariamente para suportar as operações da organização. Durante esta fase, os utilizadores finais interagem com o ERP para executar tarefas críticas de negócio. A manutenção inclui a correção de erros, a aplicação de atualizações e a introdução de melhorias que garantam a continuidade e eficiência do sistema. É também nesta fase que se monitoriza a aceitação dos utilizadores e o impacto do ERP nos processos organizacionais.
5. **Fase de Evolução:** Com o tempo, as organizações podem necessitar de funcionalidades adicionais ou de integração com outros sistemas, como soluções de Customer Relationship Management (CRM) ou Supply Chain Management (SCM). Esta fase foca-se na expansão e no aperfeiçoamento do ERP para acompanhar as mudanças nas necessidades do negócio e do mercado. A evolução exige um ERP maduro e estável, sendo um processo complexo que requer planeamento adequado e recursos especializados.
6. **Fase de Descontinuação (*Retirement*):** Quando um ERP deixa de responder às exigências organizacionais, surge a necessidade de o substituir. Nesta fase, o sistema pode ser abandonado e substituído por outro ERP ou por um sistema mais adequado. As razões para a descontinuação incluem a obsolescência tecnológica, alterações nos requisitos do negócio, ou uma escolha inicial inadequada. É importante planear cuidadosamente esta transição para minimizar os riscos e os custos associados.

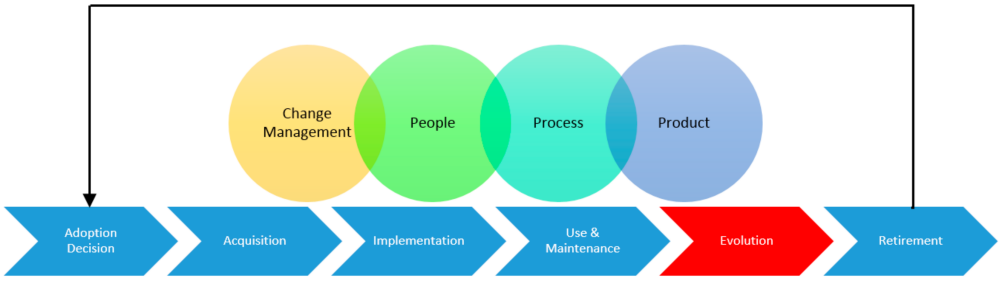

Figura 2.1: *Ciclo de Vida do ERP. Fonte: Adaptado de Bjelland e Haddara (2018).*

2.6 Principais Sistemas ERP no Mercado

O mercado global de sistemas ERP caracteriza-se por forte crescimento e competição entre um conjunto limitado de fornecedores multinacionais, que oferecem soluções completas de gestão empresarial com capacidades de integração, automação, análise em tempo real e suporte a vários processos (Gartner Inc., 2024).

Estes fornecedores disputam quotas de mercado significativas e evoluem as suas soluções para responder à crescente demanda por ERP baseado em *cloud*, inteligência artificial e análise de dados.

2.6.1 SAP

A SAP é uma das mais antigas e influentes empresas no espaço de ERP, tendo lançado o seu primeiro sistema em 1972 e evoluindo o portefólio para plataformas modernas como o SAP S/4HANA e soluções *cloud* integradas (SAP SE, 2024a).

O SAP ERP é utilizado em grande escala por organizações globais e integra módulos que cobrem finanças, logística, recursos humanos e cadeia de abastecimento, proporcionando visibilidade operacional em tempo real (SAP SE, 2024d).

De acordo com relatórios de mercado recentes, a SAP figura entre os maiores fornecedores de ERP por receita global, representando uma quota significativa do mercado total de aplicações ERP (Gartner Inc., 2024).

2.6.2 Oracle

A Oracle Corporation apresenta o seu produto principal, o Oracle *Cloud* ERP, uma suite *cloud* completa que engloba funções como gestão financeira, recursos humanos, compras e cadeia de abastecimento (Oracle Corporation, 2024).

Esta solução moderniza os processos empresariais com capacidades de automação, analítica integrada e suporte à conformidade. A Oracle é identificada por analistas como um dos líderes globais em aplicações ERP, frequentemente competindo com a SAP em termos de receita e quota de mercado global (Gartner Inc., 2024).

2.6.3 Microsoft Dynamics

A linha Microsoft Dynamics 365 representa a oferta ERP da Microsoft, fornecendo aplicações que combinam funções de planeamento de recursos empresariais com integração nativa com outros serviços Microsoft, como Office 365, Power BI e Azure (Microsoft Corporation, 2024).

Dynamics 365 inclui módulos para finanças, operações e gestão de projetos, com forte foco em capacidades *cloud* e inteligência artificial que melhoram a tomada de decisões e a automação de processos (Microsoft Corporation, 2024).

Mesmo não sendo o maior fornecedor em termos de receita global, a Microsoft Dynamics tem uma presença significativa no mercado ERP, especialmente em médias

empresas (Gartner Inc., 2024).

2.6.4 Sage

A Sage Group PLC é um fornecedor histórico de soluções de gestão empresarial para pequenas e médias empresas, oferecendo um portefólio ERP que abrange contabilidade, gestão comercial e operações financeiras (Sage Group plc, 2024).

Nos relatórios de mercado, a Sage aparece entre os principais fornecedores em termos de clientes e receita global ERP, com forte adoção especialmente no segmento PME em vários mercados regionais (Gartner Inc., 2024).

2.6.5 Sistemas ERP portugueses (Primavera BSS, PHC, Alidata)

Alguns dos fornecedores nacionais como Primavera BSS, PHC e Alidata desempenham um papel relevante em mercados locais, oferecendo soluções adaptadas às necessidades específicas de pequenas e médias empresas e às legislações fiscais e contabilísticas de países como Portugal (Primavera BSS, 2024; PHC Software, 2024; Alidata, 2024).

Estes fornecedores complementam o panorama global, especialmente em contextos onde requisitos legais e de integração local são críticos, ainda que não tenham a mesma escala de receita global que os líderes multinacionais.

2.7 Segurança nos sistemas ERP

Os sistemas ERP constituem hoje uma infraestrutura crítica para o funcionamento das organizações, assegurando a integração e automatização de áreas essenciais como finanças, recursos humanos, logística e produção (Aloini et al., 2007). Todavia, a centralização de informação sensível e a elevada interdependência entre módulos tornam estes sistemas particularmente atrativos para agentes maliciosos (Worrell et al., 2006). A proteção eficaz de um ERP é, por isso, indispensável para mitigar riscos associados a perdas financeiras, violações de dados, interrupções operacionais e danos reputacionais (National Institute of Standards and Technology, 2020).

2.7.1 Principais Riscos e Ameaças

Aumento da incidência de ataques cibernéticos

Com a crescente digitalização dos processos de negócio, os sistemas ERP tornaram-se alvos privilegiados de cibercriminosos. Configurações inadequadas, ausência de atualizações e gestão deficiente de permissões constituem vulnerabilidades que podem ser exploradas para a execução de ataques, incluindo *ransomware*, elevação de privilégios e roubo de credenciais (National Institute of Standards and Technology, 2020; European Union Agency for Cybersecurity (ENISA), 2023).

Integrações e interfaces vulneráveis

Os ERPs modernos interagem com um vasto ecossistema de plataformas externas, como serviços *cloud*, ferramentas de automação, sistemas CRM e aplicações de *Business Intelligence*. Integrações mal configuradas ou desprovidas de mecanismos de autenticação robusta ampliam a superfície de ataque e podem constituir pontos de entrada para intrusões (National Institute of Standards and Technology, 2020).

Acessos indevidos e má gestão de privilégios

A ausência de políticas rigorosas de gestão de acessos é uma das principais causas de incidentes de segurança em ERP. Utilizadores com permissões excessivas ou não alinhadas com as suas funções podem comprometer a integridade dos dados, provocando alterações não autorizadas ou falhas operacionais, quer de forma intencional, quer acidental (ISACA, 2012).

2.7.2 Estratégias para Reforçar a Segurança

Gestão de acessos e permissões

É fundamental garantir que cada utilizador dispõe apenas dos privilégios estritamente necessários ao desempenho das suas funções. A implementação de modelos de controlo de acesso baseados em funções contribui para reduzir significativamente o risco de acessos indevidos e limita o impacto potencial de credenciais comprometidas (National Institute of Standards and Technology, 2020).

Segregação de funções (Segregation of Duties (SoD))

Para minimizar riscos de fraude e assegurar a integridade dos processos, é essencial evitar que um único utilizador detenha controlo completo sobre atividades críticas. A literatura académica identifica a análise sistemática de conflitos de Segregação de Funções como mecanismo essencial de controlo interno em sistemas ERP (ISACA, 2012).

Atualizações, correções e gestão de vulnerabilidades

A manutenção contínua do ERP, incluindo a aplicação regular de *patches* de segurança, é crucial para impedir a exploração de falhas conhecidas (National Institute of Standards and Technology, 2020).

Monitorização contínua e auditorias regulares

A supervisão permanente das atividades do sistema, complementada por auditorias periódicas, facilita a deteção precoce de comportamentos anómalos, acessos suspeitos ou tentativas de intrusão. Estas práticas constituem um elemento essencial para a prevenção de incidentes e a resposta célere a potenciais ataques (Wolf et al., 2009).

3

Caracterização do SAP

A SAP é uma das maiores fornecedoras mundiais de *software* de gestão empresarial, desempenhando um papel central na digitalização e integração dos processos organizacionais. Fundada em 1972, em Walldorf, Alemanha, a empresa evoluiu de um pequeno grupo de engenheiros para uma multinacional com presença global, servindo organizações de diferentes sectores e dimensões (*SAP Company Information* 2023; Gartner Inc., 2024).

Desde o início, a SAP distinguiu-se por uma abordagem integrada à gestão da informação empresarial, introduzindo o conceito de processamento em tempo real aplicado a funções críticas de negócio. Esta filosofia materializou-se inicialmente nos sistemas SAP R/2 e SAP R/3, estes sistemas estabeleceram novos padrões para soluções (ERP), uma vez que consolidavam processos financeiros, logísticos e operacionais numa única plataforma (Monk et al., 2012).

Atualmente, o SAP S/4HANA representa a geração mais avançada da plataforma SAP, tirando partido da *in-memory computing* para permitir análises em tempo real em grandes volumes de dados transacionais. Esta evolução arquitetural suporta a integração de tecnologias emergentes, como a Inteligência Artificial (IA), *machine learning* e automação de processos o que reforça o papel dos sistemas SAP como núcleo digital das organizações modernas (Plattner, 2012).

A centralização da informação numa única fonte é uma das principais vantagens competitivas dos sistemas SAP, permitindo consistência dos dados, redução de redundâncias e suporte à tomada de decisão com base em informação atualizada. No entanto, esta mesma centralização transforma os ambientes SAP em alvos de elevado valor, tornando a segurança um requisito crítico para a sua operação contínua e fiável (Behl, 2020).

3.1 Áreas de Negócio SAP

O portefólio da SAP abrange um conjunto alargado de áreas funcionais que suportam transversalmente os processos de negócio das organizações. Entre estas destacam-se as soluções ERP no modelo *on-premise* e *cloud*, plataformas tecnológicas empresariais para integração e desenvolvimento, gestão financeira, cadeia logística, recursos humanos e gestão da experiência do cliente.

Nos últimos anos, a SAP tem reforçado a integração de capacidades analíticas avançadas e de Inteligência Artificial, permitindo otimizar processos, automatizar decisões e extrair valor estratégico dos dados empresariais. Adicionalmente, soluções como SAP Ariba, Concur e SuccessFactors expandiram o alcance da plataforma para áreas especializadas, promovendo uma abordagem integrada à gestão da despesa, capital humano e redes de negócio. Além destas plataformas a SAP disponibiliza a plataforma SAP RISE que permite ser gerida na totalidade pela cloud privada.(*SAP Product Portfolio* 2026).

3.2 Evolução dos Sistemas SAP

A evolução dos sistemas SAP acompanha a transformação tecnológica dos sistemas de informação empresariais ao longo das últimas cinco décadas. Desde as primeiras soluções de contabilidade executadas em ambientes centralizados até às atuais plataformas baseadas em *in-memory computing* e arquiteturas *cloud-native*, a trajetória da SAP reflete a progressiva complexificação das necessidades organizacionais e o avanço das infraestruturas tecnológicas.

A informação histórica que se segue, relativa às diferentes versões do sistema, incluindo SAP R/1, R/2, R/3, SAP ERP/ECC, SAP HANA e SAP S/4HANA, foi validada com base na documentação oficial disponibilizada pela SAP(SAP SE, 2024a).

3.2.1 SAP R/1: Primeiros Anos

Em 1973, a SAP lançou o primeiro produto comercial, um sistema de contabilidade financeira que serviu de base ao SAP R/1. Este sistema permitia processar dados em tempo real e integrar várias funções empresariais numa única plataforma o que marcou o início da visão da SAP.

3.2.2 SAP R/2

Lançado em 1979, o SAP R/2 operava em ambientes *mainframe* e consolidava todas as funções empresariais, incluindo gestão de materiais e planeamento da produção. A capacidade do processamento em tempo real contribuiu para que grandes empresas adotassem uma gestão centralizada dos seus processos.

3.2.3 SAP R/3: Arquitetura Cliente-Servidor

Em 1992, o SAP R/3 introduziu uma mudança paradigmática ao migrar de *mainframe* para uma arquitetura cliente-servidor de três camadas. Este modelo aumentou a flexibilidade, escalabilidade e acessibilidade dos sistemas SAP, tornando o R/3 um padrão global no mercado ERP e que é uma arquitetura ainda usada atualmente.

3.2.4 SAP ERP e SAP ECC

Em 2004 surgiu o SAP ERP Central Component (ECC) 5.0, baseado numa arquitetura orientada a serviços que facilitava a integração com aplicações externas. Em 2006 foi lançada a versão SAP ERP 6.0, amplamente utilizada ainda hoje, sendo mantida através de novos pacotes com constantes melhorias.

3.2.5 SAP HANA e SAP S/4HANA

Em 2011, a SAP revolucionou a sua arquitetura ao lançar o SAP HANA, uma plataforma de *in-memory computing* que é capaz de processar grandes volumes de dados em tempo real. Em 2015, a SAP introduziu o SAP S/4HANA, construído especificamente para base de dados HANA, apresentando:

- interface moderna com base em SAP Fiori;
- simplificação de modelos de dados;
- capacidades analíticas avançadas;
- integração com IA e IoT.

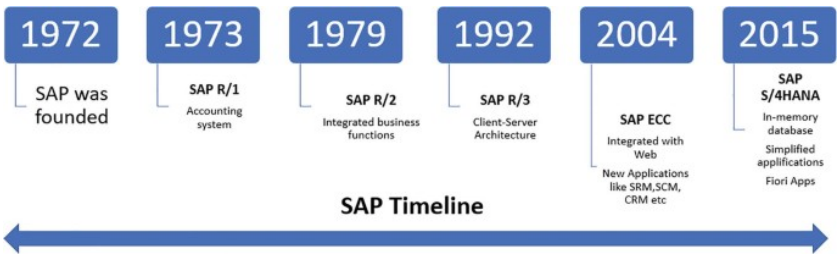

Figura 3.1: *Diagrama/Ilustração extraído de Goel (2022), introdução ao Handbook for SAP PP in S/4HANA.*

3.3 Arquitetura dos Sistemas SAP

A arquitetura clássica dos sistemas SAP baseia-se num modelo de três camadas (*three-tier architecture*), composto por uma camada de apresentação, uma camada de aplicação e uma camada de base de dados. Este modelo foi amplamente difundido com o SAP R/3 e permitiu separar responsabilidades funcionais, melhorar a escalabilidade e distribuir cargas de processamento entre diferentes servidores (Monk et al., 2012).

A separação entre camada de apresentação (interface com o utilizador), camada de aplicação (lógica de negócio) e camada de base de dados (armazenamento persistente)

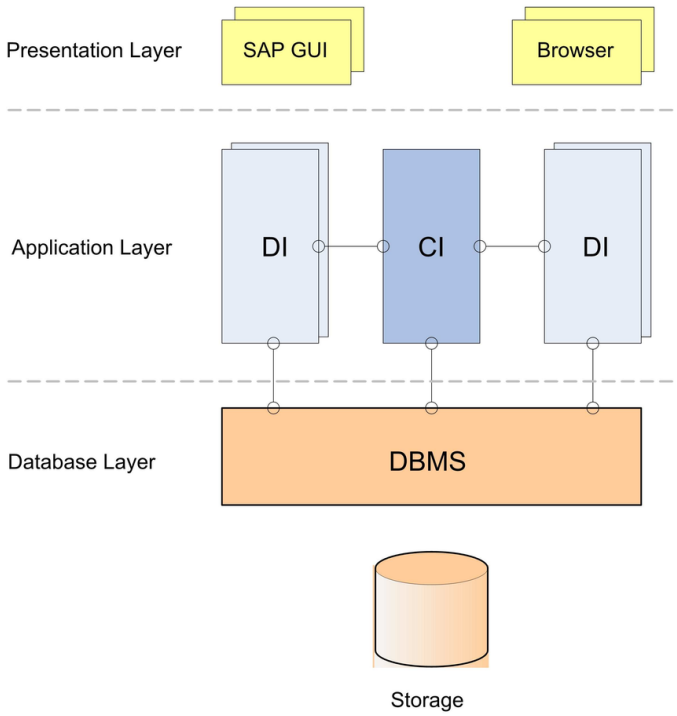

Figura 3.2: *Arquitetura clássica de três camadas em sistemas SAP, adaptada de* («*Running Business Applications in the Cloud – A Use Case Perspective*» *2010*)

constitui um princípio estruturante da arquitetura SAP tradicional. Este modelo pode ser analisado na Figura 3.2.

Como referido anteriormente, a introdução do SAP HANA em 2011 permitiu que a arquitetura evoluiu para um paradigma *in-memory computing*. O SAP HANA é descrito como um sistema de gestão de base de dados relacional, executado integralmente em memória principal, concebido para suportar simultaneamente cargas transacionais e analíticas de elevado desempenho e de grande volume(Färber et al., 2012; SAP SE, 2024d).

O SAP S/4HANA reforça este modelo, integrando aplicações empresariais e base de dados numa arquitetura otimizada para desempenho e simplificação estrutural. Entre as principais características deste sistema podem se destacara simplificação do modelo de dados e a incorporação de capacidades analíticas dos dados (SAP SE, 2024b).

Paralelamente, a SAP passou a suportar arquiteturas híbridas e *cloud-native*, o que ofereceu vários modelos de implementação: *on-premise*, *private cloud*, *public cloud* e cenários híbridos. O SAP S/4HANA é oficialmente suportado em infraestruturas de *hyperscalers* como Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (SAP SE, 2024c). Esta abordagem permite às organizações escolherem modelos de implementação alinhados com requisitos de segurança, conformidade e escalabilidade.

3.4 Benefícios e Desafios dos Sistemas SAP

3.4.1 Benefícios

Um dos principais benefícios dos sistemas SAP é a integração total dos processos empresariais numa única plataforma e com plataformas de outras áreas que necessitam de informação dos sistemas SAP e vice-versa, permitindo que diferentes áreas da organização partilhem informação de forma consistente e em tempo real. Esta integração é apontada na literatura como uma das características fundamentais dos sistemas ERP, contribuindo para a eliminação de redundâncias e para uma melhor coordenação organizacional (Davenport, 1998; Klaus et al., 2000).

Os sistemas SAP também apresentam flexibilidade para diferentes sectores e dimensões empresariais, uma vez que tem base em módulos configuráveis que podem ser adaptados às necessidades específicas de cada organização. Esta capacidade de adaptação tem sido identificada como um fator-chave para a adoção de ERP em contextos industriais distintos (Yusuf et al., 2004).

Outro benefício relevante é a elevada escalabilidade, permitindo que o sistema acompanhe o crescimento da organização, tanto em termos de volume de dados como de número de utilizadores e unidades organizacionais (Davenport, 1998).

Por fim, a evolução recente das soluções SAP, nomeadamente com a introdução do SAP HANA e do SAP S/4HANA, tem permitido uma inovação contínua, incorporando análises em tempo real e mecanismos avançados de apoio à decisão, suportados por processamento *in-memory* (Färber et al., 2012).

3.4.2 Desafios

Apesar dos altos benefícios, existem também vários desafios associados aos sistemas SAP. Um dos mais referidos é o custo elevado de implementação e manutenção, que inclui não apenas licenças de *software*, mas também custos de consultoria, formação e adaptação organizacional (Davenport, 1998).

Outro desafio significativo prende-se com a complexidade técnica dos sistemas, que exige competências especializadas para a sua implementação, configuração e operação. A falta de conhecimento interno é frequentemente apontada como um fator de risco em projetos ERP e neste caso em projetos SAP (Yusuf et al., 2004; Aloini et al., 2007).

Em suma, é comum existir uma dependência de empresas externas para personalização, integração e suporte, especialmente em ambientes SAP, o que pode aumentar os custos e reduzir a autonomia das organizações ao longo do ciclo de vida do sistema.

3.5 Segurança dos Sistemas SAP

A segurança dos sistemas SAP exige uma abordagem holística, de modo a que seja possível combinar o controlo de acessos, gestão de autorizações, segurança das comu-

nicações, proteção do código e monitorização contínua. Esta abordagem é necessária devido ao facto de os sistemas SAP suportarem processos empresariais críticos e armazenarem dados sensíveis, cujo o comprometimento pode ter impactos operacionais, financeiros e reputacionais significativos para as empresas(Behl, 2020; Pfleeger et al., 2015).

Em ambientes SAP e, de forma mais geral, em sistemas ERP, os mecanismos de segurança baseiam-se tipicamente em modelos de controlo de acessos suportados por utilizadores, *roles* e autorizações, seguindo princípios como o menor privilégio e a (SoD). Estes mecanismos são amplamente reconhecidos como essenciais para reduzir riscos de fraude, abuso de privilégios e acessos indevidos em sistemas integrados (Sadiq et al., 2007).

No entanto, a elevada complexidade funcional e configuracional destes sistemas pode levar à existência de permissões excessivas ou herdadas ao longo do tempo, especialmente em ambientes produtivos. Alguns estudos técnicos na área da segurança SAP destacam que configurações permissivas e a falta de revisão periódica de autorizações constituem vetores frequentes de risco (Onapsis, s.d.).

Neste contexto, a combinação de revisões periódicas de configurações críticas, testes manuais e automatizados e monitorização contínua é considerada uma boa prática essencial para a manutenção de um nível de segurança adequado em sistemas SAP e em outros sistemas ERP (Behl, 2020; Onapsis, s.d.).

4

Vulnerabilidades de Segurança em Sistemas SAP: Enquadramento e Análise

A segurança dos sistemas SAP constitui um dos pilares essenciais para a proteção da informação empresarial. Como referido no capítulo anterior, estes sistemas suportam processos de negócio críticos, incluindo contabilidade, finanças, logística, produção e recursos humanos, o que concentra grandes volumes de dados sensíveis numa única plataforma. Esta centralização, embora traga benefícios ao nível da eficiência e da consistência da informação, torna os ambientes SAP particularmente atrativos para ataques cibernéticos e para a exploração de configurações inseguras, conforme discutido na literatura sobre segurança em sistemas empresariais (Pfleeger et al., 2015; Behl, 2020).

Diversos estudos na área da cibersegurança têm salientado que a complexidade funcional e técnica dos sistemas ERP exige uma abordagem de segurança contínua e estruturada, com base na correta configuração de parâmetros, na gestão rigorosa de acessos e na monitorização permanente dos sistemas (Baskerville et al., 2014). Em ambientes reais, no entanto, é comum que os procedimentos de verificação de segurança sejam realizados de forma manual, pontual ou reativa, sobretudo em organizações onde a segurança compete com outras prioridades operacionais. Esta abordagem dificulta a deteção atempada de configurações inseguras e aumenta a probabilidade de exposição a riscos ao longo do tempo (Behl, 2020).

Neste contexto, a literatura técnica especializada sobre segurança em sistemas SAP tem identificado a automatização dos processos de análise e verificação de segurança como um fator crítico para a redução de riscos. Alguns estudos e relatórios técnicos apontam que muitas vulnerabilidades persistem não por ausência de mecanismos de segurança, mas devido à complexidade da configuração e à falta de validação regular em ambientes produtivos (Onapsis, s.d.).

Com isto, o presente projeto enquadra-se na necessidade de automatizar a análise

de segurança em sistemas SAP, procurando alinhar-se com as boas práticas. Este capítulo apresenta o enquadramento teórico das vulnerabilidades analisadas, discutindo as razões da sua persistência em ambientes empresariais reais, bem como uma revisão das principais abordagens, ferramentas e trabalhos académicos relacionados com a automatização da segurança em sistemas ERP e SAP.

A relevância da segurança em sistemas SAP é amplamente reconhecida tanto em literatura académica como por entidades independentes e importantes da área de cibersegurança. Trabalhos técnicos têm destacado utilizadores padrão, parâmetros de sistema e interfaces de comunicação como pontos particularmente sensíveis do ponto de vista da segurança, o que exige medidas específicas de endurecimento (*hardening*) para mitigar riscos associados a acessos indevidos e exposição de serviços (Onapsis, s.d.).

Adicionalmente, estudos independentes e relatórios de entidades de cibersegurança alertam que um número significativo de incidentes em ambientes SAP resultam de configurações inseguras, ausência de controlo adequado de acessos e utilização de credenciais insuficientemente protegidas, reforçando a necessidade de abordagens sistemáticas e automatizadas que permitam avaliar sistematicamente o nível de segurança dos sistemas (Baskerville et al., 2014; Behl, 2020).

4.1 Origem e Persistência das Vulnerabilidades Analisadas

As vulnerabilidades analisadas neste trabalho não decorrem, na sua maioria, de falhas no desenvolvimento do *software* SAP ou de código Advanced Business Application Programming (ABAP), mas estão, sobretudo, associadas a configurações inadequadas, opções operacionais e decisões tomadas ao longo do ciclo de vida dos sistemas. Em ambientes empresariais complexos, é comum que a necessidade de flexibilidade, compatibilidade e rapidez na implementação conduza à adoção de configurações permissivas, que nem sempre são posteriormente ajustadas de acordo com os requisitos de segurança (Aloini et al., 2007; Worrell et al., 2006).

Durante as fases iniciais de instalação e testes, os sistemas SAP disponibilizam contas padrão, parâmetros menos restritivos e serviços ativos, o que facilita a configuração inicial e o arranque do sistema. Embora estas opções sejam adequadas em contextos de teste ou desenvolvimento, tornam-se problemáticas e perigosas quando permanecem ativas em ambientes produtivos, especialmente na ausência de análises de segurança (Onapsis, s.d.).

A persistência deste tipo de vulnerabilidades é agravada pela complexidade do modelo de segurança SAP, que envolve múltiplos conceitos interdependentes, como mandantes, utilizadores, *roles*, perfis, objetos de autorização, ligações RFC, parâmetros e serviços *web*. Em cenários com vários sistemas interligados e integrações externas, a gestão consistente destes elementos torna-se particularmente exigente, aumentando a probabilidade de existirem execsso de permissões ou de configurações herdadas de

fases anteriores do sistema (Sadiq et al., 2007).

Para além disto, a administração segura requer competências técnicas especializadas e um conhecimento aprofundado da plataforma. Na prática, nem sempre existem processos formais ou mecanismos de validação contínua que assegurem a conformidade das configurações com as boas práticas de segurança, valida assim que os desvios se mantenham ativos durante longos períodos e evoluam para riscos estruturais consideravelmente graves (Behl, 2020; Baskerville et al., 2014).

Neste contexto, a automatização da análise de segurança assume um papel particularmente relevante, ao permitir a verificação sistemática e repetitiva de configurações críticas, reduzindo a dependência de processos manuais e reativos. Muitos dos problemas identificados nas auditorias de sistemas resultam precisamente da dificuldade em garantir que os mecanismos de segurança existentes são aplicados de forma consistente ao longo do tempo (Onapsis, s.d.).

Através deste enquadramento é possível ajudar a compreender o porquê de vulnerabilidades com base nas configurações continuarem a ser observadas em auditorias recentes, mesmo em sistemas tecnicamente atualizados, reforçando a importância de abordagens automatizadas e contínuas.

4.2 Principais Vulnerabilidades Analisadas

A fase de estudo e levantamento das vulnerabilidades teve como objetivo identificar configurações de segurança recorrentes e que são explicitamente referidas, na documentação oficial, como críticas ou fortemente recomendadas para revisão. As vulnerabilidades selecionadas refletem situações frequentemente observadas em auditorias SAP e cuja análise pode ser realizada de forma automatizada.

4.2.1 Contas Padrão com *passwords* por Omissão

A SAP disponibiliza, por defeito, um conjunto de contas padrão criadas durante o processo de instalação, muitas das quais possuem palavras-passe conhecidas e documentadas. É altamente recomendadado que estas contas sejam bloqueadas, removidas ou tenham as respetivas palavras-passe alteradas imediatamente após a instalação e configuração do sistema.

A manutenção destas contas em estado ativo representa um risco significativo, uma vez que permite o acesso direto ao sistema sem necessidade de exploração técnica adicional. Esta vulnerabilidade resulta, na maioria dos casos, de configurações iniciais que não foram revistas após a fase de implementação.

Além das contas existem também utilizadores padrão como elementos críticos de risco, é recomendado a alteração imediata das palavras-passe iniciais, a desativação de comportamentos automáticos com estes utilizadores e o bloqueio de contas não utilizadas em ambientes produtivos (*Protecting Standard Users* 2007).

4.2.2 Parâmetros de Segurança

Os parâmetros de sistema controlam aspetos críticos da segurança, uma vez que incluem políticas de autenticação, bloqueio de contas, registo de eventos e comunicação entre componentes. A documentação oficial define valores recomendados para diversos parâmetros de segurança, alertando para os riscos associados a configurações permissivas.

Configurações incorretas ou valores por omissão mantidos ao longo do tempo podem enfraquecer significativamente a postura de segurança do sistema. Estas situações são frequentemente consequência de alterações pontuais realizadas para resolver problemas operacionais, sem posterior revisão de segurança (*Profile Parameters for Logon and Password* 2010).

4.2.3 Mandantes Padrão Não Utilizados

Durante a instalação inicial, a SAP cria automaticamente vários mandantes padrão, como os identificados pelos números 000, 001 e 066. É recomendado que estes mandantes sejam protegidos, removidos ou restritos quando não estão a ser utilizados em ambientes produtivos.(SAP SE, 2012)

A permanência destes mandantes ativos resulta, em muitos casos como detalhado anteriormente no documento, de práticas históricas ou da ausência de políticas claras de limpeza pós-instalação, representando um vetor de acesso indevido ao sistema (Onapsis, 2016).

4.2.4 Ligações RFC com Privilégios Elevados

As ligações RFC permitem a comunicação entre sistemas SAP e aplicações externas, sendo um componente essencial para integração e troca de dados. A SAP fornece recomendações gerais sobre a segurança de chamadas RFC, incluindo a necessidade de configurar as conexões de forma segura, limitar as autorizações associadas ao utilizador RFC e proteger a própria configuração das comunicações (SAP SE, 2023). O objeto de autorização S_RFC é um exemplo de controlo que verifica se o utilizador possui autorização para a função remota solicitada (SAP SE, s.d.).

Em muitas configurações, por razões de simplicidade ou compatibilidade, são utilizadas contas com privilégios elevados em ligações RFC, ou as autorizações associadas aos utilizadores RFC não são suficientemente restritas. Esta prática pode permitir a execução remota de funções críticas com mais privilégios do que o necessário, o que cria uma superfície de ataque adicional. Alguns casos técnicos e manuais de segurança destacam que a utilização de ligações RFC com autorizações excessivas é um ponto de risco significativo que deve ser mitigado através de alteração de configurações e revisões de autorização adequadas (SAP SE, 2023; SAP RFC Security Resources, s.d.).

4.2.5 Utilização da Chave de Encriptação por Omissão

São utilizados mecanismos de armazenamento seguro para proteger dados sensíveis, como credenciais técnicas e informações da configuração. Nos sistemas SAP ABAP, este armazenamento é realizado através do *Secure Storage*, que recorre a uma chave de encriptação interna. Antes da configuração explícita da gestão de chaves, este mecanismo utiliza uma chave por omissão (*default*), cujo objetivo é apenas evitar guardar os dados em *clear text*.

Em ambientes produtivos, a utilização durante um longo período desta chave por omissão constitui uma vulnerabilidade conhecida, uma vez que não oferece um nível de proteção adequado para os dados sensíveis. A SAP disponibiliza a transação `SECSTORE` para a inicialização e gestão adequada da chave de encriptação do *Secure Storage*, permitindo substituir a chave por *default* por uma chave definida pela organização.

Na prática, esta situação ocorre frequentemente devido à falta de visibilidade sobre a configuração criptográfica do sistema ou à perceção incorreta de que os mecanismos padrão são suficientes para todos os contextos (*Secure Storage in the AS ABAP* s.d.).

4.2.6 Gestão Insegura de Palavras-Passe

A SAP disponibiliza um conjunto de parâmetros de sistema que permitem definir políticas de palavras-passe e de autenticação, incluindo requisitos de comprimento mínimo, validade temporal, histórico de palavras-passe e regras associadas ao processo de *login*. Estes parâmetros influenciam diretamente a robustez dos mecanismos de autenticação e devem ser configurados de forma adequada em ambientes produtivos (*Profile Parameters for Logon and Password* 2010).

Em clientes reais, a utilização de parâmetros inseguros ou a manutenção de configurações por omissão resulta, muitas vezes, de requisitos operacionais específicos ou de políticas internas divergentes. Este tipo de configuração pode comprometer a resistência do sistema a ataques de *brute-force* ou ao comprometimento das credenciais. Além disto, existem algumas organizações que têm as suas próprias políticas de *passwords*, nestes casos será necessário verificar o resultado da análise com a política da organização.

4.2.7 ACL Inseguro na RFC Gateway

A RFC Gateway no sistema SAP gere as ligações externas, em particular aquelas baseadas em RFCs, através de duas listas de controlo de acesso essenciais: os ficheiros *secinfo* e *reginfo*. O ficheiro *secinfo* controla quais os programas externos que podem ser executados e o ficheiro *reginfo* faz a gestão do registo de programas externos no gateway, definindo explicitamente quais as aplicações ou servidores que podem iniciar ligações através do mesmo (*SAP Gateway Security Files: secinfo and reginfo* 2015).

A configuração destes ficheiros e dos respetivos parâmetros associados (*gw/sec_info* e *gw/reg_info*) é bastante importante para garantir que apenas sistemas e programas au-

torizados conseguem estabelecer comunicações via RFC. Quando os ficheiros *secinfo* ou *reginfo* não existem ou estão sem dados, o *gateway* poderá não impor as restrições desejadas, o que coloca o sistema exposto a ligações não autorizadas ou a registos indevidos de servidores externos (*SAP Gateway Security Files: secinfo and reginfo* 2015).

A definição explícita e restritiva das Access Control Lists (ACLs) nestes ficheiros constitui uma medida básica de segurança para limitar ligações externas apenas a sistemas autorizados, através disto o risco de acessos indevidos ou a exploração de superfícies de ataque via RFC diminui.

4.2.8 *Web Services* Inseguros Ativos

Os sistemas SAP têm vários *web services* através do Internet Communication Framework (ICF), o que permite a integração com aplicações e plataformas externas. A ativação destes serviços é realizada de forma hierárquica, sendo necessário que todos os nós correspondentes de determinado caminho Uniform Resource Locator (URL) estejam ativos para que o serviço possa ser acedido (*Activating and Deactivating ICF Services* s.d.).

Em ambientes produtivos, é esperado que apenas os serviços estritamente necessários ao funcionamento das aplicações utilizadas permaneçam ativos e devidamente protegidos por mecanismos de autenticação e autorização. No entanto, a permanência de serviços web ativos sem necessidade operacional ocorre frequentemente devido a configurações herdadas, testes prévios ou desconhecimento da sua exposição, o que expõe os sistemas desnecessariamente (*Activating and Deactivating ICF Services* s.d.).

4.2.9 Utilizadores de Diálogo com Autorizações Críticas

Estes sistemas distinguem diferentes tipos de utilizadores, entre os quais incluem se utilizadores de diálogo (*Dialog*). Estes utilizadores são definidos como contas destinadas ao acesso interativo por utilizadores humanos, ao contrário de outros tipos como *System* ou *Communication*, que são usados para processos internos ou integrações entre sistemas (*User Types in the SAP System* s.d.).

Dado que os utilizadores de diálogo são utilizados para acesso interativo, a atribuição de autorizações especialmente sensíveis ou críticas deve ser feita com precaução e apenas quando estritamente necessária. A atribuição excessiva de autorizações críticas a contas de diálogo pode resultar de práticas acumuladas ao longo do tempo, da falta de SoD ou da ausência de revisões periódicas de autorizações, o que aumenta a probabilidade de uso indevido de privilégios elevados no sistema (*SAP Note 1529805: SU01 – Additional authorization check when setting password* 2011).

É, por isto, considerado uma boa prática limitar as autorizações administrativas atribuídas a utilizadores de diálogo, garantindo que estes apenas possuem as permissões necessárias às suas responsabilidades diárias e cumprindo os princípios de menor privilégio e segregação de funções.

A tabela 4.1 tem como objetivo evidenciar que cada análise implementada corresponde a mecanismos, configurações ou comportamentos explicitamente documentados ou reconhecidos como críticos, permitindo que a solução desenvolvida seja entendida como uma operacionalização sistemática de boas práticas de segurança aplicáveis a ambientes SAP reais.

Tabela 4.1: *Correspondência entre verificações automatizadas e documentação de referência*

Check Automatizado	**Justificação de Segurança**	**Fontes**
Contas default com passwords por omissão	Contas default com palavras-passe conhecidas permitem acesso direto ao sistema caso não sejam revistas após a instalação.	(*Protecting Standard Users* 2007)
Parâmetros de passwords	Configurações de autenticação inadequadas reduzem a resistência a ataques de força bruta e ao comprometimento de credenciais.	(*Profile Parameters for Logon and Password* 2010)
Parâmetros de segurança e login	Configurações de segurança inadequadas podem permitir acessos indevidos e comprometer a proteção do sistema.	(*Profile Parameters for Logon and Password* 2010)
Mandantes padrão ativos (`000`, `001`, `066`)	Mandantes técnicos criados durante a instalação podem conter configurações e utilizadores sensíveis se não forem devidamente protegidos.	(Onapsis, 2016)
Ligações RFC com utilizadores de privilégios elevados	Destinos RFC configurados com contas excessivamente privilegiadas permitem a execução remota de funções críticas.	(SAP SE, 2023; SAP SE, s.d.)
Utilização da chave de encriptação por omissão (`Secure Storage`)	A utilização da chave de encriptação por omissão não garante a proteção adequada de dados sensíveis.	(*Secure Storage in the AS ABAP* s.d.)
RFC Gateway com ACL (`secinfo/reginfo`)	Listas de controlo de acesso demasiado permissivas permitem o registo e a execução de programas externos não autorizados.	(*SAP Gateway Security Files: secinfo and reginfo* 2015)
Web Services / ICF ativos sem necessidade operacional	Serviços Web ativos sem utilização aumentam a superfície de ataque do sistema.	(*Activating and Deactivating ICF Services* s.d.; *Alert (AA19-122A): New Exploits for Unsecure SAP Systems* 2019; *10KBLAZE Threat Report* 2019)
Utilizadores de diálogo com autorizações críticas	A atribuição de privilégios administrativos excessivos a utilizadores de diálogo aumenta o risco de abuso interno e de comprometimento do sistema.	(*User Types in the SAP System* s.d.; *SAP Note 1529805: SU01 – Additional authorization check when setting password* 2011)

Foram selecionados estes nove checks por representarem verificações de segurança fundamentais e transversalmente aplicáveis aos diferentes ambientes SAP analisados, incluindo sistemas como SAP S/4HANA e SAP ERP. Desta forma, a utilização de um conjunto comum de análises permite garantir maior consistência, comparabilidade e uniformidade nos dados recolhidos entre os diferentes sistemas avaliados.

No entanto, a avaliação da conformidade deve de considerar as políticas internas de segurança definidas por cada organização. As políticas corporativas podem estabelecer requisitos mais restritivos do que os valores recomendados pela SAP, devendo estes prevalecer durante a análise. Por exemplo, caso a SAP recomende uma dimensão mínima de 10 caracteres para as palavras-passe, mas a política interna da organização exija um mínimo de 12 caracteres, o valor definido internamente deverá ser considerado como referência para a avaliação de conformidade. Assim, a análise dos sistemas deve assegurar não apenas o alinhamento com as recomendações da SAP, mas também o cumprimento dos requisitos de segurança específicos da organização.

4.3 Casos Reais e Incidentes Relacionados com Falhas de Segurança em SAP

A ocorrência de incidentes de segurança associados a estes sistemas tem sido documentada por entidades públicas e empresas especializadas em segurança. Em particular, a (Cybersecurity and Infrastructure Security Agency (CISA)) publicou alertas oficiais a advertir para a exploração ativa de sistemas SAP mal configurados, destacando o impacto potencial sobre infraestruturas críticas (*Alert (AA19-122A): New Exploits for Unsecure SAP Systems* 2019).

A relevância das vulnerabilidades analisadas é reforçada pela existência de múltiplos incidentes reais, relatados por entidades especializadas em segurança e pela própria comunidade SAP.

Importa salientar que, na maioria dos casos documentados, os incidentes não resultaram exclusivamente de vulnerabilidades de *software*, mas sim da combinação entre serviços expostos, configurações antigas, credenciais inadequadamente protegidas e ausência de mecanismos de verificação e análise contínua. Este padrão encontra-se alinhado com as advertências presentes na documentação oficial da SAP, que enfatiza a necessidade de proteger utilizadores padrão, restringir acessos remotos e rever periodicamente configurações críticas de segurança.

4.3.1 Exposição de Serviços e Falhas de Autenticação

Diversos incidentes públicos demonstraram que a exposição de serviços SAP sem mecanismos adequados de autenticação e controlo de acessos pode permitir o acesso não autorizado a funcionalidades críticas do sistema. Um dos casos mais relevantes foi o conjunto de vulnerabilidades conhecido como *RECON*, identificado pela Onapsis Research Labs, que afetou componentes do SAP NetWeaver Application Server (AS) Java

e permitiu, em determinados cenários, o acesso a funcionalidades administrativas sem autenticação adequada (Onapsis Research Labs, 2020).

Este incidente evidenciou os riscos associados à exposição de serviços *web* sem configuração segura, reforçando a necessidade de restringir serviços ativos apenas aos estritamente necessários e de garantir mecanismos robustos de autenticação e autorização nos componentes expostos.

4.3.2 Configurações Inseguras do RFC Gateway com ACL

De acordo com investigações publicadas pela Onapsis, o conjunto de vulnerabilidades conhecido como *10KBLAZE* demonstrou que sistemas SAP com configurações permissivas do Gateway, como no caso dos parâmetros *secinfo* e *reginfo* podiam ser comprometidos utilizando ferramentas publicamente disponíveis, sem necessidade de exploração complexa de vulnerabilidades de *software* não corrigidas (*10KBLAZE Threat Report* 2019).

Embora a SAP tenha disponibilizado correções e recomendações técnicas, a própria comunidade SAP reconheceu que muitas explorações só foram possíveis devido à inexistência ou à permissividade excessiva das regras de acesso do Gateway, reforçando assim a importância da sua configuração restritiva em ambientes produtivos (*10KBLAZE and SAP* (*From an administrative point*) 2019).

4.3.3 *Passwords* Fracas e Contas *Default*

A utilização de contas *default* e de *passwords* inadequadamente protegidas continua a ser identificada como um fator de risco relevante. Alguns relatórios de segurança e auditorias técnicas indicam que estas situações persistem em sistemas produtivos, frequentemente como resultado de configurações iniciais que não foram revistas após a fase de implementação.

Alguns casos reais documentados demonstram o impacto desta prática. Um exemplo é o utilizador padrão `TMSADM`, associado ao sistema de gestão de transportes, cuja a palavra-passe por omissão foi identificada em ambientes produtivos reais. A exploração desta configuração permitiu o acesso a funcionalidades críticas do sistema sem necessidade de técnicas avançadas, o que evidenciou a gravidade da utilização de *passwords default* em contas com privilégios elevados (Onapsis Research, 2019).

4.3.4 Incidentes Recentes com SAP *NetWeaver*

Mais recentemente, foram divulgados incidentes que confirmam a exploração de vulnerabilidades críticas em sistemas SAP em ambientes reais. Em 2025, foi reportada a exploração ativa da vulnerabilidade Common Vulnerabilities and Exposures (CVE)-2025-42957 em sistemas SAP S/4HANA, a qual permitia a injeção de código ABAP arbitrário a partir de uma conta autenticada com privilégios reduzidos. Apesar de exigir acesso inicial ao sistema, esta vulnerabilidade possibilitava o comprometimento

completo do ambiente SAP, incluindo a execução de código com impacto total sobre o sistema e processos de negócio da empresa em causa (SecurityBridge, 2025; Dutch National Cyber Security Centre, 2025).

No mesmo ano, foi também documentado um incidente em que uma campanha de *malware* direcionada a servidores Linux foi associada à exploração de uma vulnerabilidade no SAP NetWeaver Visual Composer (CVE-2025-31324). Neste caso, a exploração da falha permitiu a instalação de um *backdoor* persistente, demonstrando uma cadeia de ataque completa desde a exploração de uma vulnerabilidade SAP até à execução de código malicioso no *host* onde o sistema aplicacional operava. (Unit 42 (Palo Alto Networks), 2025; Darktrace Research, 2025).

4.3.5 Implicações para a Automatização da Análise de Segurança

Os casos apresentados demonstram que as vulnerabilidades analisadas neste trabalho não constituem apenas riscos teóricos, mas refletem problemas reais e recorrentes. A documentação oficial da SAP enfatiza a necessidade de revisão contínua de configurações críticas. No entanto, a dependência dos processos manuais dificulta a aplicação consistente dessas recomendações.

Neste contexto, a automatização da análise de segurança assume um papel fundamental, permitindo identificar de forma sistemática configurações inseguras antes que estas possam ser exploradas, reduzindo a superfície de ataque e alinhando a operação diária com as boas práticas definidas pelo fabricante.

4.4 Comparação com Ferramentas Comerciais de Segurança em sistemas SAP

Apesar da eficácia das ferramentas comerciais existentes, estas soluções apresentam características que podem dificultar a sua adoção e utilização em determinados contextos, nomeadamente custos elevados de licenciamento, complexidade de implementação e reduzida flexibilidade de adaptação a políticas internas específicas. A Tabela 4.2 apresenta uma comparação estruturada entre duas das principais ferramentas comerciais de segurança SAP e a solução proposta neste trabalho. Esta análise teve como base reuniões com as próprias empresas e informação retirada das páginas oficiais destas organizações.

Tabela 4.2: *Comparação entre ferramentas comerciais de segurança SAP e a solução proposta*

Característica	**Onapsis**	**SecurityBridge**	**Solução Proposta**
Modelo de licenciamento	Proprietário	Proprietário	Académico / *Open* (sem custos de licenciamento)
Foco principal	Vulnerabilidades e ameaças	Monitorização contínua	Automatização de auditorias de configuração
Complexidade de implementação	Elevada	Média	Baixa a média
Customização de *checks*	Limitada	Limitada	Elevada (orientada a políticas específicas)
Dependência de infraestrutura externa	Sim	Parcial	Não (execução local ou integrada)
Automatização de verificações recorrentes	Sim	Sim	Sim
Orientação académica / experimental	Não	Não	Sim
Transparência dos critérios de análise	Parcial	Parcial	Total (baseada em documentação SAP)
Integração direta com RFC	Sim	Sim	Sim

A comparação evidencia que a solução desenvolvida não pretende substituir plataformas comerciais existentes, mas sim complementar o ecossistema, através de uma abordagem leve, flexível, alinhada com objetivos académicos e experimentais, de modo a aumentar a rapidez de análise dos sistemas.

4.5 Síntese Crítica e Enquadramento da solução proposta

As vulnerabilidades analisadas refletem problemas recorrentes identificados pela própria SAP e documentados nas suas recomendações oficiais de segurança. A sua persistência em ambientes reais resulta da combinação entre complexidade técnica, decisões operacionais e ausência de mecanismos sistemáticos de verificação contínua.

Neste contexto, o projeto desenvolvido propõe uma abordagem automatizada que permite operacionalizar as recomendações de segurança da SAP, reduzindo a dependência de auditorias manuais e contribuindo para uma gestão de segurança mais proativa, consistente e alinhada com as boas práticas definidas pela SAP.

Página intencionalmente deixada em branco.

5

Análise e Especificação da Aplicação

A realização do sistema proposto neste projeto teve como principal objetivo o desenvolvimento de uma aplicação *web* para automatização da análise de segurança em sistemas SAP. A ferramenta foi idealizada para identificar, avaliar e apresentar vulnerabilidades consideradas críticas e fora das métricas ideais da SAP de forma estruturada, permitindo que os administradores de sistemas, equipas de segurança e até simples técnicos de TI atuem de forma mais eficiente, informada e rápida. As vulnerabilidades analisadas estão especificadas no capítulo anterior.

Este capítulo descreve a análise funcional que sustentou o desenvolvimento da aplicação, a definição dos requisitos e a arquitetura geral da solução.

5.1 Objetivo da Aplicação

O sistema proposto tem como objetivo automatizar o processo de verificação de configurações inseguras em sistemas SAP, com base nas vulnerabilidades mais recorrentes e com maior impacto operacional. Com isto, pretende-se reduzir a dependência de auditorias manuais, que são demoradas e sujeitas a erro humano, através de um processo automatizado capaz de detetar rapidamente configurações de risco e de apresentar recomendações para mitigação.

A aplicação foi concebida para oferecer:

- **Análise automática** de vulnerabilidades críticas;
- **Visualização de resultados** de forma clara e intuitiva;
- **Análise da configuração** por nível de *compliance* com a informação da SAP;
- **Geração de relatórios** de suporte à decisão e à auditoria.

5.2 Âmbito e Contexto da Análise

O desenvolvimento da aplicação baseou-se na análise de um conjunto de vulnerabilidades identificadas como mais relevantes em auditorias de segurança SAP. O sistema foi desenhado para verificar automaticamente os seguintes pontos:

1. Contas padrão com *passwords* por omissão;
2. Parâmetros de segurança SAP mal configurados;
3. Mandantes padrão não utilizados (000, 001 e 066);
4. Ligações RFC com utilizadores de privilégios elevados;
5. Utilização da chave de encriptação padrão;
6. Políticas inseguras de gestão de *passwords*;
7. ACL do RFC Gateway configurada de forma permissiva;
8. *Web services* inseguros ativos;
9. Utilizadores de diálogo com autorizações críticas.

Estes pontos representam áreas de risco elevadas que, se não forem devidamente controladas, podem comprometer a integridade, confidencialidade e disponibilidade do sistema.

5.3 Requisitos Funcionais

Com base no âmbito definido, foram estabelecidos os seguintes requisitos funcionais para a aplicação:

- **RF1 — Ligação ao SAP:** O sistema deve permitir a ligação segura ao ambiente SAP para recolha de informações relevantes à análise.
- **RF2 — Verificação Automática de Vulnerabilidades:** A aplicação deve executar, de forma automatizada, as verificações associadas às nove categorias de vulnerabilidade identificadas.
- **RF3 — Classificação de Resultados:** Cada vulnerabilidade detetada deve ser classificada com base no nível de risco (baixo, médio, alto).
- **RF4 — Visualização dos Resultados:** O utilizador deve poder visualizar os resultados em formato gráfico e tabular, o que irá facilitar a interpretação dos dados.
- **RF5 — Geração de Relatórios:** Deve ser possível exportar relatórios de análise com as vulnerabilidades encontradas e as respetivas recomendações.
- **RF6 — Histórico de Execuções:** O sistema deve manter um registo das análises anteriores para comparação de resultados ao longo do tempo.
- **RF7 — Autenticação e Gestão de Acesso:** O sistema deve garantir que apenas utilizadores autorizados possam executar análises e aceder aos resultados, respeitando os perfis definidos.

Os requisitos funcionais foram definidos tendo como base análises realizadas anteriormente de forma manual e outras que foram identificadas antes do projeto ser iniciado.

5.4 Requisitos Não Funcionais

Além das funcionalidades centrais, foram definidos requisitos que asseguram a qualidade e fiabilidade da aplicação:

- **RNF1 — Desempenho:** A análise deve ser executada de forma eficiente, reduzindo o tempo total comparativamente às auditorias manuais.
- **RNF2 — Segurança:** As credenciais de acesso ao SAP devem ser protegidas e cifradas, garantindo que a aplicação não introduz riscos adicionais.
- **RNF3 — Escalabilidade:** O sistema deve permitir integração com diferentes ambientes SAP sem necessidade de alterações estruturais.
- **RNF4 — Usabilidade:** A interface deve ser simples e intuitiva, permitindo utilização por técnicos e auditores com e sem formação avançada em SAP.
- **RNF5 — Portabilidade:** A aplicação deve poder ser executada em diferentes plataformas, através de um navegador *web*.

5.5 Princípios de *Design* Orientados à Segurança

A definição da arquitetura da aplicação foi orientada por princípios de *security-by-design*

5.5.1 Autenticação e Gestão dos Acessos

Foram implementados mecanismos de autenticação que garantem que apenas utilizadores devidamente autorizados possam aceder às funcionalidades da aplicação. O gestão dos acessos foi realizado de forma a limitar o acesso às diferentes operações com base no perfil do utilizador.

Esta abordagem permite reduzir o risco de acessos indevidos e assegurar que funcionalidades críticas, como a execução de análises ou a visualização de resultados sensíveis, estão protegidas contra utilização abusiva ou de outros utilizadores.

5.5.2 Proteção da Comunicação

Toda a comunicação entre os diferentes componentes da aplicação é realizada através de canais seguros, possibilitando a confidencialidade e integridade dos dados transmitidos. Esta medida é particularmente relevante no contexto da troca de informação sensível relacionada com configurações de segurança dos sistemas SAP.

5.5.3 Isolamento de Responsabilidades

A separação entre *frontend*, *backend* e sistemas SAP permite isolar falhas e limitar o impacto de eventuais compromissos de segurança. Mesmo em caso de exploração de vulnerabilidades numa das camadas, o impacto sobre os restantes componentes é mitigado.

5.5.4 Proteção de Dados e Criptografia

A proteção da informação armazenada pela aplicação constitui um aspeto crítico do desenvolvimento, uma vez que os resultados das análises e as credenciais dos utilizadores contêm dados sensíveis, com impacto direto na segurança dos sistemas SAP analisados.

Para garantir a confidencialidade e integridade da informação, foi adotado o algoritmo de encriptação simétrica *Advanced Encryption Standard* com chave de 256 bits, operando em modo *Galois/Counter Mode* (AES-256-GCM). Este mecanismo foi selecionado por oferecer, simultaneamente, mecanismos de encriptação e autenticação, reduzindo o risco de manipulação ou corrupção dos dados.

É utilizada uma única chave criptográfica para os processos de encriptação e desencriptação, devidamente protegida no contexto da aplicação. A utilização de criptografia simétrica permite assegurar um compromisso adequado entre desempenho e segurança, particularmente relevante em cenários de análise recorrente e geração de relatórios.

São cifrados os seguintes elementos:

- os *payloads* que contêm toda a informação associada aos relatórios de análise;
- as palavras-passe dos utilizadores, armazenadas de forma segura.

Esta abordagem garante que, mesmo em caso de acesso não autorizado à base de dados, a informação sensível permanece protegida contra leitura ou alteração indevida, uma vez que estes dados se encontram criptografados.

5.6 Funcionalidades Principais

A aplicação oferece um conjunto de funcionalidades destinadas a simplificar o processo de auditoria e análise de segurança SAP:

- **Análise automática:** execução completa da verificação de vulnerabilidades com apenas uma execução;
- **Classificação de riscos:** atribuição de níveis de criticidade de acordo com cada falta de *compliance* SAP;
- **Painel de gestão do(*dashboard*):** visualização consolidada do estado geral de segurança de cada sistema e *overview* geral de todos os sistemas analisados;

- **Detalhe dos resultados:** listagem das vulnerabilidades detetadas com descrição, impacto e recomendação;
- **Exportação de relatórios:** criação automática de ficheiros Portable Document Format (PDF) com os resultados da análise para fins de auditoria ou documentação.

5.7 Desafios de Implementação

Durante o desenvolvimento da aplicação foram identificados vários desafios técnicos e operacionais:

- **Heterogeneidade das configurações SAP:** cada sistema pode possuir versões e estruturas diferentes, exigindo flexibilidade nos mecanismos de análise;
- **Gestão segura das credenciais de acesso:** foi necessário implementar métodos de cifragem e de acesso controlado para garantir a proteção de todas as contas e acessos;
- **Equilíbrio entre automatização e precisão:** a automatização total pode gerar falsos positivos. Por isso, a aplicação foi desenhada para apresentar resultados claros, mas com espaço para validação e análise humana. Neste contexto, a questão de falsos negativos não existe. Os resultados foram validados através de um auditoria manual aos mesmos sistemas;
- **Apresentação de informação técnica de forma acessível:** o desafio de traduzir resultados complexos de análise SAP para visualizações simples e compreensíveis foi um ponto central no *design* do *frontend*.

Apesar destes desafios, o desenvolvimento permitiu alcançar uma solução equilibrada, capaz de reduzir significativamente o tempo e o esforço necessários para a análise de segurança SAP, mantendo elevados níveis de precisão e fiabilidade. No entanto, esta análise será fundamentada nos próximos capítulos do presente documento.

Página intencionalmente deixada em branco.

6

Desenvolvimento da Aplicação

O presente capítulo descreve o processo de desenvolvimento da aplicação proposta para a automatização da análise de segurança em sistemas SAP, constituindo um dos pilares centrais deste trabalho. Após a definição do projeto, é necessário apresentar de forma estruturada a solução desenvolvida, evidenciando as decisões técnicas adotadas e a relação direta com os objetivos de segurança estabelecidos.

Ao longo deste capítulo é apresentada a arquitetura geral da aplicação, os principais componentes do sistema e os mecanismos implementados para garantir a confidencialidade, integridade e disponibilidade da informação analisada. Para além da descrição funcional, são descritas as decisões de *design* orientadas à segurança, bem como as limitações identificadas durante todo o desenvolvimento.

6.1 Visão Geral da Arquitetura da Aplicação

A arquitetura do projeto segue um modelo cliente–servidor e encontra-se organizada em duas camadas principais da aplicação: a camada de apresentação e a camada lógica. Para permitir o funcionamento do projeto, existe ainda uma componente de persistência dos dados e um conjunto de sistemas externos com os quais a aplicação comunica de forma controlada e estruturada.

A **camada de apresentação** corresponde ao *frontend*, responsável pela interação com o utilizador. A **camada aplicacional** corresponde ao *backend*, onde se encontram implementadas a lógica dos processos, a execução das análises e os mecanismos de segurança. A estas camadas junta-se a **componente de persistência**, materializada na base de dados, e os **sistemas externos com os quais a aplicação comunica**, que constituem os alvos de análise da aplicação.

Esta separação permite isolar responsabilidades, reduzir a superfície de ataque e impedir ligações diretas entre o utilizador final e os sistemas SAP, reforçando assim o modelo de segurança adotado.

Camadas e Componentes Principais

A **camada de apresentação**, implementada através do *frontend*, foi desenvolvida com recurso ao *Next.js*, uma *framework* de *React.js*. Esta camada disponibiliza a interface gráfica da aplicação, permitindo ao utilizador configurar análises, consultar resultados, ordenar análises e exportar relatórios. Não possui acesso direto aos sistemas SAP, nem à base de dados, comunicando exclusivamente com o *backend*.

A **camada aplicacional**, implementada no *backend* e desenvolvida em *Java*, constitui o núcleo lógico da solução. É nesta camada que se encontram implementados os mecanismos de autenticação, controlo de acessos, gestão das análises e consolidação dos resultados obtidos. A separação entre *frontend* e *backend* reforça o isolamento de responsabilidades e facilita a evolução futura da aplicação.

No *backend* encontra-se igualmente o motor de análise, responsável pela execução dos diferentes *checks* de segurança sobre os sistemas SAP. Estas verificações incidem sobre configurações e parâmetros considerados críticos, incluindo contas padrão com palavras-passe por omissão, parâmetros de segurança sensíveis, clientes padrão ativos, ligações RFC com utilizadores privilegiados, utilização de chaves de encriptação por omissão, políticas de palavras-passe inseguras, configurações permissivas do *RFC Gateway* com ACL, *web services* inseguros ativos e utilizadores de diálogo com autorizações críticas.

A **componente de persistência** é suportada por uma base de dados *MySQL*, utilizada para armazenar informação relativa aos utilizadores, análises realizadas, irregularidades identificadas, classificações de *compliance* SAP e recomendações associadas. O acesso a esta componente é restrito ao *backend*, contribuindo para a proteção da informação sensível armazenada.

Por fim, os **sistemas SAP alvo de análise** constituem sistemas externos à aplicação, com os quais o *backend* comunica de forma controlada e restrita. Estes sistemas não integram a arquitetura interna da aplicação, mas fazem parte do ecossistema operacional da solução, na medida em que fornecem os dados e configurações sobre os quais incidem as análises de segurança.

Comunicação com os Sistemas SAP

A comunicação entre a aplicação e o sistema SAP é efetuada exclusivamente via RFC, através do SAP Java Connector (JCo). Este canal constitui o único ponto de interação com os sistemas SAP, respeitando as credenciais técnicas e os perfis de autorização configurados para cada ligação no início de cada análise.

Embora existam outras formas de integração com os sistemas SAP, como serviços OData via SAP Gateway, *web services* Simple Object Access Protocol (SOAP) ou através do acesso direto à base de dados, optou-se pela utilização exclusiva de RFC através do JCo. Esta escolha justifica-se pelo facto de o RFC respeitar integralmente o modelo de autorização nativo do SAP, garantindo que todas as operações são executadas sob

as permissões do utilizador técnico configurado no início da análise. Com isto, não é possível contornar os mecanismos de controlo de acesso do sistema.

A utilização de apenas um canal permite aplicar o princípio do privilégio mínimo, garantindo que as análises são realizadas, por omissão, em modo *read-only*. Operações corretivas ou ações com impacto no sistema SAP, apenas são permitidas quando explicitamente configuradas e autorizadas, reduzindo o risco de alterações não intencionais.

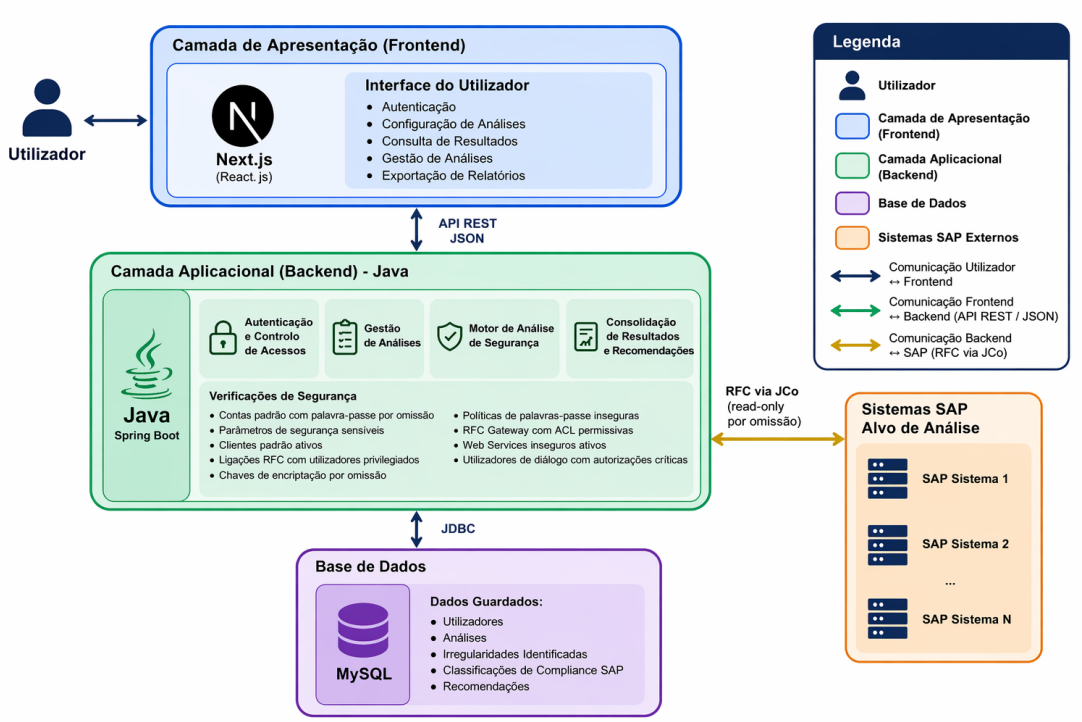

Figura 6.1: *Arquitetura da Aplicação*

6.1.1 Fluxos Principais de Funcionamento

Os fluxos principais da aplicação seguem uma sequência bem definida. O utilizador interage inicialmente com o *frontend*, a partir do qual são enviados pedidos de configuração ou execução de análises para o *backend*. O *backend*, por sua vez, estabelece comunicação com os sistemas SAP, através de RFC, para obter a informação necessária à execução dos *checks*. Os resultados obtidos são processados, classificados e armazenados na base de dados, sendo posteriormente disponibilizados no *frontend* sob a forma de *dashboards*, tabelas ordenáveis e relatórios exportáveis.

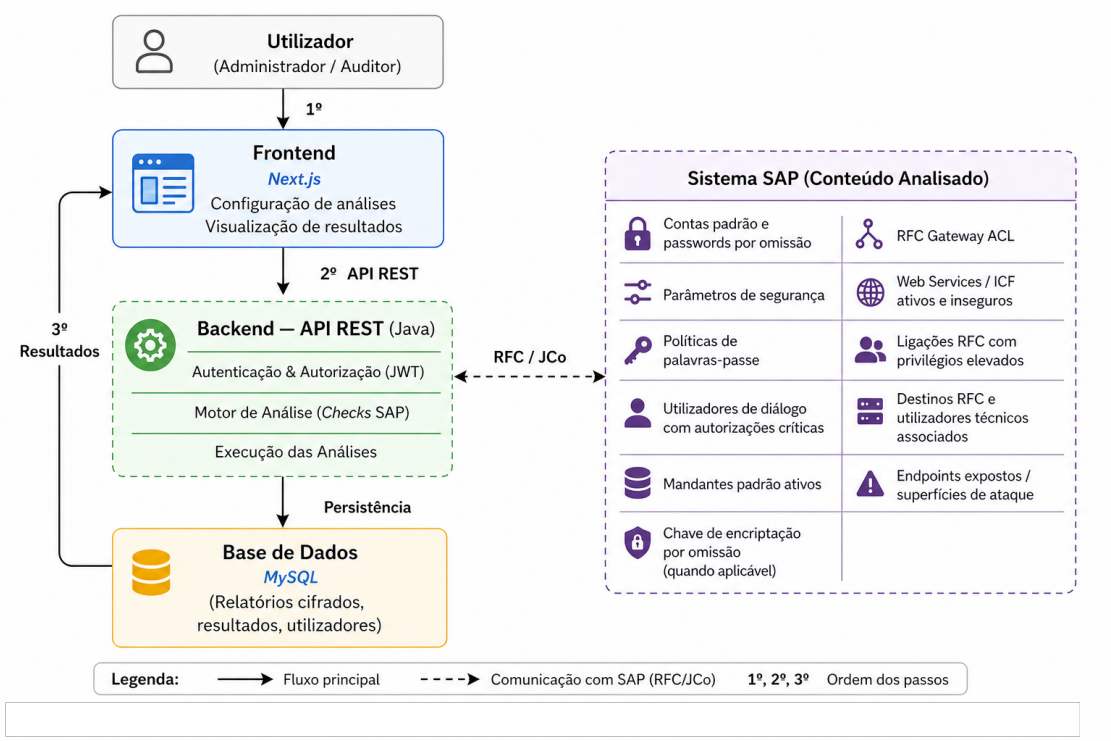

Figura 6.2: *Arquitetura lógica da aplicação e fluxo da aplicação com interação dos sistemas SAP.*

A comunicação entre o *frontend* e o *backend* é realizada através de uma Application Programming Interface (API) Representational State Transfer (REST), o que permite a separação entre as diferentes camadas e a expansão futura da aplicação. Esta arquitetura modular contribui para a escalabilidade da solução e facilita a integração com ferramentas externas de monitorização, auditoria ou gestão de segurança.

6.2 Metodologia

O desenvolvimento da aplicação seguiu uma abordagem incremental e iterativa, permitindo a validação progressiva das funcionalidades implementadas e a adaptação contínua às necessidades identificadas ao longo do projeto. Esta metodologia revelou-se particularmente adequada num contexto de integração com sistemas complexos como o SAP, onde alterações de configuração, permissões e dependências técnicas podem influenciar diretamente o comportamento da aplicação.

A abordagem adotada permitiu identificar limitações técnicas numa fase inicial, reduzir o risco de erros estruturais e garantir que os requisitos de segurança fossem considerados desde as fases iniciais do desenvolvimento.

O processo metodológico foi estruturado em várias etapas principais:

1. Recolha e análise de informação sobre segurança SAP e normas aplicáveis;
2. Análise e definição dos requisitos funcionais, não funcionais e de segurança da solução;
3. Definição e desenho da arquitetura da aplicação;

4. Desenvolvimento do *backend* e do *frontend*, incluindo a ligação à base de dados;
5. Integração progressiva com os sistemas SAP através de RFC, permitindo a execução das várias análises de segurança;
6. Realização de testes funcionais e de segurança, incluindo análise e validação dos resultados obtidos;
7. Documentação do sistema e validação final da solução desenvolvida.

6.3 Testes Realizados

Após a implementação das principais funcionalidades da aplicação, foram realizados testes com o objetivo de validar o correto funcionamento do sistema e avaliar a eficácia dos mecanismos de segurança implementados. Estes testes incidiram em vários pontos, tanto na fiabilidade funcional da aplicação, como em tentativas de acesso indevido e exploração de vulnerabilidades.

Numa primeira fase, foram efetuados **testes funcionais**, com o propósito de confirmar que os resultados apresentados pela aplicação correspondiam efetivamente ao comportamento esperado. Em particular, procedeu-se à validação dos dados devolvidos em cada análise, verificando se os resultados obtidos refletiam corretamente a informação exata dos sistemas SAP e se não existiam falhas ao nível doo processamento, inconsistências ou omissões na apresentação dos mesmos. Esta verificação permitiu confirmar a fiabilidade da aplicação ao nível da execução das análises e da visualização dos resultados.

Posteriormente, foram realizados **testes de segurança ao mecanismo de autenticação e controlo de acessos**. Entre estes testes, procurou-se avaliar a resistência do processo de *login* a tentativas de Structured Query Language (SQL) *injection*, através do teste de introdução de entradas maliciosas nos campos de autenticação. O objetivo consistiu em verificar se a aplicação verificava e agia corretamente os dados recebidos e se a interação com a base de dados era efetuada de forma segura, sem permitir manipulação indevida/forçada das pesquisas.

Foram igualmente realizados testes de **autorizações**, tentando aceder a relatórios que não se encontravam associados ao utilizador autenticado. Esta validação teve como finalidade confirmar que os mecanismos de controlo de acessos impediam a visualização de informação pertencente a outros utilizadores, o que permitiu assegurar o isolamento dos dados e a confidencialidade dos relatórios armazenados.

Adicionalmente, foram efetuadas tentativas de **acesso direto à base de dados**, com o intuito de verificar se a arquitetura implementada impedia o contacto direto entre o utilizador e a componente de armazenamento dos dados. Estes testes permitiram confirmar que a base de dados apenas se encontra acessível através do *backend*, não estando exposta diretamente ao *frontend* nem ao utilizador final.

Por fim, todos os testes que foram realizados permitiram validar a robustez da aplicação desenvolvida, demonstrou assim que a aplicação apresenta um comportamento

funcional consistente e de acordo com o esperado.

6.4 Tecnologias Utilizadas

A implementação da aplicação recorreu a um conjunto de tecnologias amplamente utilizadas em contextos empresariais e académicos, selecionadas com base em critérios de robustez, segurança e facilidade de integração com os sistemas SAP.

O **backend** da aplicação foi desenvolvido em *Java*, onde se encontra com base numa arquitetura orientada a serviços, sendo responsável pela execução das análises de segurança, pela gestão de utilizadores, pelo controlo de acessos e pela comunicação com os sistemas SAP e a base de dados. Esta camada realiza a gestão de toda a lógica de negócio da aplicação, o que permite que as operações críticas sejam executadas de forma controlada e segura.

O **frontend** foi implementado recorrendo a uma tecnologia *web* moderna, concretamente o *Next.js*, que disponibiliza uma interface gráfica intuitiva, responsiva e com *templates* originais da SAP. Através desta interface, o utilizador pode configurar as análises a executar, consultar os resultados obtidos, visualizar gráficos de apoio à interpretação dos dados e gerar relatórios.

A persistência da informação é assegurada por uma **base de dados relacional**, neste caso *MySQL*, utilizada para o armazenamento de dados de configuração, resultados das análises efetuadas e informação associada à autenticação dos utilizadores. Conforme descrito no capítulo anterior, estes dados são armazenados de forma encriptada. O acesso à base de dados é exclusivo do *backend* da aplicação, reforçando o modelo de segurança adotado e prevenindo acessos diretos não autorizados.

6.5 Implementação da Automatização da Análise de Segurança

Como detalhado anteriormente, a funcionalidade central da aplicação reside na automatização da análise das configurações de segurança em sistemas SAP, permitindo substituir procedimentos tradicionalmente manuais por um processo sistemático, repetível e menos dependente de intervenção humana. Esta abordagem, visa não só aumentar a eficiência das análises, mas também assegurar maior consistência, fiabilidade e rastreabilidade nos resultados obtidos.

O processo de análise foi concebido de forma estruturada, iniciando-se com o estabelecimento de uma ligação segura ao sistema SAP alvo de análise. Esta ligação é efetuada através de um utilizador técnico previamente configurado, cujas autorizações são definidas de acordo com o princípio do privilégio mínimo, garantindo que apenas os acessos estritamente necessários à recolha de informação são permitidos.

Após a autenticação, são recolhidos os parâmetros, perfis e configurações relevantes para a análise, o que inclui definições de sistema, políticas de autenticação, configurações de acesso remoto e informação associada a utilizadores e integrações. Por omissão,

todas as operações de recolha são realizadas em modo *read-only*, permite garantir que a execução das análises não provoca qualquer alteração ao estado do sistema, nem interfere com o seu funcionamento normal.

A informação recolhida é, posteriormente, avaliada de forma automática, com base em critérios previamente definidos e alinhados com as recomendações oficiais da SAP e com boas práticas reconhecidas no domínio da segurança, como descrito no Capítulo 4.

Com base nesta avaliação, os resultados são classificados de acordo com diferentes níveis de risco e conformidade, facilitando a priorização de ações corretivas.

A adoção do modelo utilizado contribui para a redução da dependência da interpretação individual do auditor, minimizando o risco de omissões e garantindo maior uniformidade nas análises realizadas, mesmo quando aplicadas de forma recorrente a diferentes sistemas ou ambientes SAP.

6.6 Desenvolvimento do *Backend*

O **backend** constitui o componente central da solução desenvolvida, assumindo o papel de camada de gestão entre o *frontend* e os sistemas SAP alvo de análise. É nesta camada que se concentra a lógica do funcionamento da aplicação, sendo responsável pela disponibilização de uma API REST para autenticação dos utilizadores e para a execução das auditorias de segurança. Para além disto, o *backend* executa os diferentes *checks* aos sistemas, estabelece a comunicação controlada com os sistemas SAP através de RFCs, utilizando o JCo, e envia todos os dados para a base de dados de modo a manter a persistência segura dos relatórios e dos resultados obtidos.

Tal como dito anteriormente, a implementação do *backend* foi desenvolvida em *Java*, recorrendo ao *Spring Boot* como *framework* principal. Através desta escolha foi possível estruturar a aplicação seguindo um modelo modular, que promove uma separação clara de responsabilidades entre os diferentes componentes funcionais. Esta abordagem facilita a manutenção do código e permite uma extensão futura, nomeadamente através da introdução de novos *checks* de segurança ou da integração com outros sistemas e/ou ferramentas externas.

6.6.1 Estrutura do Projeto e Separação de Responsabilidades

O *backend* encontra-se estruturado por camadas de modo a refletir as diferentes áreas e ações da aplicação. Esta abordagem permite isolar componentes com funções distintas, reduzir o acoplamento entre os módulos e facilitar a manutenção e escalabilidade do sistema.

A organização do projeto tem como base as seguintes camadas principais[1]:

[1] Os nomes técnicos apresentados no formato `typewriter`, como `AuthController`, `CryptoService` ou `Report`, correspondem a elementos concretos do desenvolvimento da aplicação, nomeadamente pacotes, classes ou métodos do código.

- `auth`: responsável pelos mecanismos de autenticação com base no *JSON Web Token* (JWT), que inclui o controlador de autenticação (`AuthController`) e o componente que permite gerir e validar os *tokens* (`JwtUtil`). Após validação das credenciais, é emitido um *token* assinado digitalmente, que segue todos os pedidos seguintes e permite ao *backend* validar a identidade do utilizador, assegurando assim um modelo de autenticação *stateless*. O token fica válido durante 1 hora, após essa hora é necessário realizar o *login* novamente.;
- `controller`: camada exposta da API REST, nomeadamente o que permite gerir toda a análise SAP (`SapJcoController`) e os respetivos *endpoints* associados às operações de análises e *checks*;
- `configuration`: camada responsável pelas configurações globais da aplicação, incluindo a definição de políticas Cross-Origin Resource Sharing (CORS), parâmetros de segurança Hypertext Transfer Protocol (HTTP) e outras definições estruturais;
- `crypto`: parte dedicada à cifragem[2] dos dados armazenados, onde integra a configuração criptográfica (`CryptoConfig`), o serviço responsável pelas operações de cifragem e decifragem (`CryptoService`) e o conversor Java Persistence API (JPA) para atributos encriptados (`EncryptedStringAttributeConverter`). O JPA é utilizado para o mapeamento objeto-relacional no *backend* da aplicação. Foi utilizado através do *framework Hibernate*; com isto é possível manter a persistência das entidades do sistema de forma abstrata, sem dependência direta do SQL específico da base de dados;
- `service`: camada lógica da aplicação, onde está implementado o motor de análise. Inclui os diferentes serviços responsáveis pela execução dos *checks* de segurança, tais como `PasswordManagement`, `SecurityParameters`, `StandardAccounts` e todos os outros;
- `provider`: camada de ligação com o sistema SAP através do JCo, permite assim o registo dinâmico dos destinos RFC, através da classe `MyDestinationDataProvider`;
- `model` / `repo` / `dto`: definição das entidades persistentes (como `User` e `Report`), dos repositórios JPA responsáveis pelo acesso à base de dados e dos objetos de transferência de dados (Data Transfer Object (DTO)) utilizados na comunicação entre todas as camadas.

Como a estrutura do projeto é uma estrutura modular possibilita introduzir novos *checks* de segurança sob a forma de serviços independentes, sem a necessidade de alterações na estrutura da aplicação ou nos restantes componentes do sistema. Como consequência, a solução apresenta elevada extensibilidade, mantendo simultaneamente uma organização clara e coerente do código.

[2] Entende-se por cifragem o processo criptográfico de conversão de dados em formato ilegível, utilizando algoritmos e chaves, com o objetivo de garantir a confidencialidade da informação.

6.6.2 API REST e *Endpoints* Principais

A API do *backend* encontra-se exposta com o prefixo `/api`. Do ponto de vista funcional, os *endpoints* dividem-se em dois grupos:

- **Autenticação e gestão da sessão** (`/api/auth`): inclui operações de *login* e *registo*, devolvendo um *token* JWT para autenticação subsequente, o que permite saber se existe alguém com *login* efetuado e, se existir, é possível identificar o utilizador;
- **Execução e consulta das auditorias** (`/api`): inclui *endpoints* para executar os *checks* e consultar o histórico das análises.

Em termos operacionais, os *endpoints* são **protegidos por *token* JWT** enviado no cabeçalho `Authorization: Bearer <token>`. O *backend* valida o *token*, obtém o utilizador autenticado e associa os relatórios ao respetivo utilizador.

6.6.3 Fluxo de Execução de uma Auditoria

As execuções das auditorias seguem um padrão uniforme e contínuo, implementado no *controller* (`SapJcoController`) através de um padrão comum de execução e persistência. Este fluxo pode ser descrito em quatro etapas:

1. **Autenticação**: validação do *token* JWT e identificação do utilizador.
2. **Configuração do destino SAP**: receção dos parâmetros de ligação SAP (por exemplo, `ashost`, `sysnr`, `client`, `user`, `passwd`, `lang`) e registo dinâmico do destino RFC.
3. **Execução do *check***: invocação do serviço de auditoria correspondente (por exemplo, `PasswordManagement.runAudit()`).
4. **Persistência e resposta**: serialização do *payload* em JavaScript Object Notation (JSON). Após isto, é armazenado num relatório associado ao utilizador e devolve o resultado ao *frontend*.

Para suportar a rastreabilidade e o agrupamento dos resultados, cada execução utiliza um identificador (`groupId`). Este identificador permite associar vários relatórios (por exemplo, múltiplos *checks*) à mesma sessão de auditoria e facilita a organização dos relatórios na página principal da aplicação. Este fluxo pode ser analisado na Figura 6.3

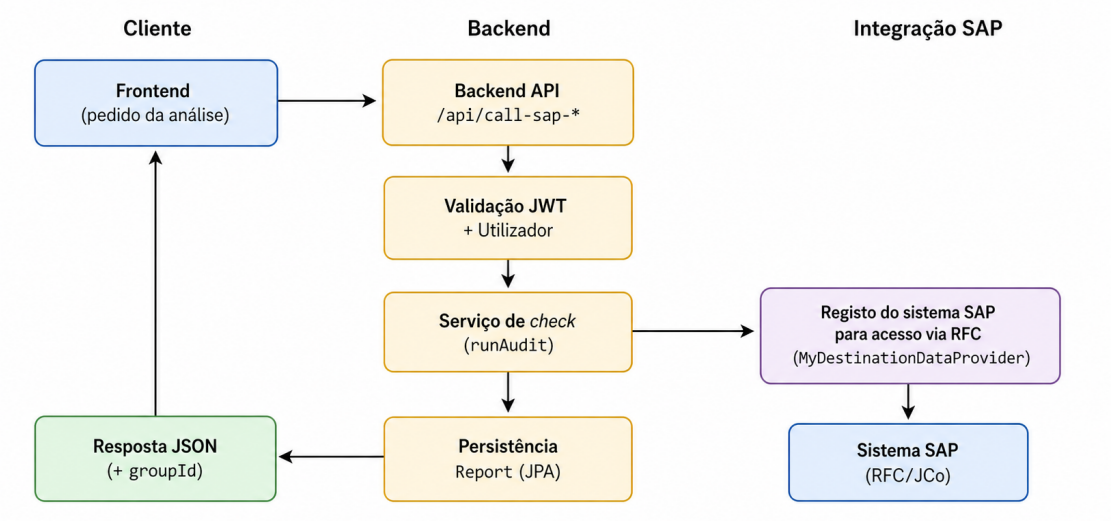

Figura 6.3: *Fluxo de execução de um check no backend: autenticação, configuração do destino RFC, execução do serviço, persistência e devolução do resultado*

6.6.4 Integração com o SAP via RFC (SAP JCo)

Como dito anteriormente, a comunicação com os sistemas SAP é efetuada através do JCo, utilizando o RFC como o mecanismo de acesso. A configuração do destino é realizada dinamicamente através de um *DestinationDataProvider* (`MyDestinationDataProvider`), que permite criar/atualizar destinos em tempo de execução com base nos parâmetros previamente fornecidos pelo utilizador no *frontend*.

Foi escolhida esta abordagem de modo a reduzir o acoplamento a configurações estáticas e, deste modo, permite auditar diferentes sistemas SAP com a mesma instância da aplicação. Contudo, o controlo de acessos permanece centralizado no *backend*.

6.6.5 Motor de Análise: Serviços de *Checks* e Cálculo de Risco

O motor que realiza a análise é composto por um conjunto de serviços em `service/`. Cada serviço é responsável por uma diferente análise e todos os serviços seguem um padrão semelhante: recolhem dados do SAP por RFC, comparam com um critério esperado e devolvem um resultado estruturado.

O formato de retorno tende a incluir, de forma consistente:

- `riskLevel`: classificação qualitativa do nível de risco associado à verificação. Assume o valor *HIGH* quando é identificada uma configuração ou parâmetro que não cumpre os requisitos de *compliance* definidos pela SAP. Caso não sejam detetadas não conformidades, o nível de risco é classificado como *LOW*.
- `outOfSpec`: lista de elementos fora dos valores esperados;
- `details`: evidência detalhada por cada parâmetro/dado analisado.

Alguns destes *checks* utilizam valores armazenados na base de dados (por exemplo, parâmetros recomendados), o que permite ajustar o critério de conformidade sem alterar o código-fonte.

6.6.6 Armazenamento dos Relatórios

Os resultados das auditorias são armazenados através do JPA, por meio da entidade `Report`. Cada relatório contém o tipo de auditoria (`reportType`), o *payload* em JSON, a data em que foi executado o relatório (`createdAt`) e o sistema que foi analisado (`system_host`).

Para suportar o histórico e a visualização no *frontend*, existem *endpoints* para:

- enumerar os relatórios do utilizador (`/api/reports`);
- enumerar os relatórios agrupados por execução (`/api/reportsByGroup?groupId=...`).

6.6.7 Mecanismos de Segurança Implementados no *Backend*

A aplicação desenvolvida incorpora um conjunto de mecanismos de segurança destinados a proteger, tanto o processo de autenticação dos utilizadores, como a confidencialidade dos dados armazenados. Tendo em consideração que os relatórios produzidos pela ferramenta contêm informação sensível sobre a configuração de segurança de sistemas SAP, foi adotada uma abordagem com base em princípios de *security-by-design*, o que garantiu que os requisitos de segurança foram considerados desde as fases iniciais do desenvolvimento.

Os principais mecanismos implementados no *backend* incluem autenticação baseada em *JSON Web Tokens* (JWT), proteção das palavras-passe dos utilizadores através de *hashing* com BCrypt e cifragem de dados sensíveis armazenados na base de dados utilizando o modelo AES-256-GCM.

Autenticação baseada em JSON Web Tokens

O mecanismo de autenticação da aplicação foi implementado recorrendo a *JSON Web Tokens* (JWT). Após a validação das credenciais de um utilizador, o sistema gera um *token* assinado digitalmente que é devolvido ao cliente e utilizado para autenticar pedidos subsequentes. O desenvolvimento do *token* está presente na Figura 6.4

Este *token* é enviado pelo cliente através do cabeçalho HTTP `Authorization`, utilizando o formato:

```
Authorization: Bearer <token>
```

```
String token = Jwts.builder()
        .setSubject(username)
        .setIssuedAt(new Date())
        .setExpiration(new Date(System.currentTimeMillis() + jwtExpiryMs))
        .signWith(SignatureAlgorithm.HS256, jwtSecret)
        .compact();
```

Figura 6.4: *Criar um token JWT após autenticação bem sucedida do utilizador*

O *backend* valida a assinatura do *token* e extrai a identidade do utilizador presente no mesmo. Cada pedido contém toda a informação necessária para validar a autenticidade do utilizador, o que simplifica a arquitetura da aplicação e melhora a sua escalabilidade.

Os *tokens* são assinados digitalmente, o que garante a integridade da informação contida no *token* e impede a alteração do mesmo sem conhecimento da chave criptográfica utilizada para a assinatura. Estes *tokens* têm validade de uma hora, ou seja, após uma hora é necessário realizar o *login* na aplicação novamente.

De modo a evitar a exposição da chave criptográfica no código-fonte, a chave utilizada na assinatura dos *tokens* não é armazenada diretamente na aplicação. Em vez disso, este valor é obtido através de variáveis de ambiente do sistema operativo, o que permite separar a informação sensível do código e facilita a gestão segura de credenciais em diferentes ambientes de execução.

Proteção das palavras-passe dos utilizadores

As *passwords* dos utilizadores não são armazenadas em *clear-text* na base de dados. Como mostra a Figura 6.5 é utilizado o algoritmo BCrypt para criar um *hash* criptográfico das credenciais, antes de serem armazenadas na base de dados.

```
// Hash the password with a salt
String salt = BCrypt.gensalt();
String hashed = BCrypt.hashpw(password, salt);


User user = new User();
user.setUsername(username);
user.setPasswordHash(hashed);
userRepo.save(user);
```

Figura 6.5: *Desenvolvimento do hash da password através do algoritmo BCrypt*

BCrypt é um algoritmo de *hashing* realizado especificamente para o armazenamento seguro de *passwords*. Ao contrário de funções criptográficas tradicionais como Secure Hash Algorithm (SHA)-256 ou SHA-512, que são extremamente rápidas, BCrypt introduz um custo computacional configurável que aumenta o tempo necessário para calcular o *hash*. Esta característica dificulta significativamente ataques de *brute-force*.

Adicionalmente, o algoritmo incorpora automaticamente um *salt* criptográfico único para cada palavra-passe. Esta propriedade impede ataques com base em *rainbow tables*, o que garante que duas *passwords* idênticas produzem *hashes* diferentes.

Durante o processo de autenticação, a *password* fornecida pelo utilizador é comparada com o *hash*, armazenado utilizando a função de verificação do BCrypt. Assim, as credenciais nunca são manipuladas ou armazenadas em formato legível.

Cifragem de dados sensíveis na base de dados

Os relatórios criados pela aplicação contêm informação sensível sobre o estado de segurança dos sistemas SAP analisados, incluindo parâmetros de configuração, utilizadores com privilégios elevados e potenciais vulnerabilidades identificadas. Para proteger esta informação, em caso de acesso indevido à base de dados, os dados são cifrados antes de serem armazenados.

A cifragem é realizada utilizando o algoritmo *Advanced Encryption Standard* com chave de 256 bits em modo *Galois/Counter Mode* (AES-256-GCM). Este modo de operação disponibiliza, simultaneamente, confidencialidade e autenticação dos dados, permitindo detetar qualquer tentativa de modificação dos dados cifrados durante o processo de decifragem.

A implementação da cifragem é realizada de forma transparente através de um *AttributeConverter* do JPA, que interceta automaticamente as operações de leitura e escrita da entidade responsável pelo armazenamento dos relatórios. Sempre que um relatório é armazenado, o respetivo *payload* é cifrado antes de ser armazenado na base de dados, sendo apenas decifrado no momento da sua leitura pela aplicação. O processo pode ser analisado na Figura 6.6.

```
SecretKey key = keys.get(activeKeyId);
Cipher cipher = Cipher.getInstance(CIPHER);
cipher.init(Cipher.ENCRYPT_MODE, key, new GCMParameterSpec(TAG_BITS, iv));

byte[] ct = cipher.doFinal(plain.getBytes(java.nio.charset.StandardCharsets.UTF_8));
byte[] ivct = new byte[iv.length + ct.length];
System.arraycopy(iv, 0, ivct, 0, iv.length);
System.arraycopy(ct, 0, ivct, iv.length, ct.length);
return activeKeyId + ":" + Base64.getEncoder().encodeToString(ivct);
```

Figura 6.6: *Processo de cifragem do payload através de AES-256-GCM.*

6.7 Desenvolvimento do *Frontend*

O *frontend* foi desenvolvido com recurso ao *Next.js*, seguindo uma abordagem assente em *components*, adequada ao desenvolvimento de aplicações *web* atuais. O principal objetivo desta camada é disponibilizar uma interface responsiva, simples e ajustada ao contexto empresarial em que a solução se insere.

Do ponto de vista arquitetural, o *frontend* assume um papel exclusivamente relacionado com a apresentação e interação com o utilizador. Não existe qualquer ligação direta entre esta camada, os sistemas SAP analisados e a base de dados.

6.7.1 Estrutura das Páginas e Navegação

A aplicação encontra-se estruturada em páginas funcionais que acompanham as diferentes fases do ciclo de vida de uma auditoria, garantindo uma navegação simples e intuitiva.

- **Autenticação**: permite o acesso à aplicação, se a validação das credenciais do utilizador for aceite, e permite criar novos utilizadores;
- **Painel do utilizador**: apresenta uma visão global de todas as auditorias realizadas pelo utilizador, incluindo indicadores de cada sistema e da qualidade dos sistemas analisados;
- **Configuração da auditoria**: possibilita a definição dos parâmetros de ligação ao sistema SAP e a seleção dos *checks* a executar;
- **Execução e visualização**: corresponde à fase em que as análises são executadas e os respetivos resultados são apresentados;
- **Consulta das auditorias**: permite aceder ao histórico das auditorias, onde é possível verificar novamente cada análise pormenorizada.

Deste modo, a compreensão do estado do processo em cada momento, desde a configuração inicial até, à análise dos resultados, fica mais simples e sustenta o histórico das auditorias efetuadas..

6.7.2 Validação da Sessão e Controlo dos Acessos

Como descrito no subcapítulo **Desenvolvimento do Backend**, esta camada implementa a autenticação com base em JWT. Após o *login*, o *token* é armazenado para permitir a autenticação dos pedidos subsequentes ao *backend*.

Para reforçar o controlo dos acessos, são aplicados mecanismos de controlo de acessos. Estes mecanismos impedem o acesso a páginas internas sem uma sessão válida. Esta abordagem reduz o risco de acessos não autorizados através da navegação direta por URL.

6.7.3 Integração com o Backend e Gestão do Processo de Auditoria

A comunicação com o *backend* é realizada por meio de uma API REST, com uma ligação configurada por uma variável de ambiente (por exemplo `NEXT_PUBLIC_API_BASE`).

Quando o utilizador inicia uma auditoria, o *frontend*:

1. recolhe e valida os parâmetros de ligação ao SAP;
2. inicia, via *backend*, a execução dos *checks*;
3. recebe os resultados e apresenta-os na página destinada ao efeito;
4. permite a persistência e consulta posterior de cada análise.

O processo é realizado de forma a maximizar a experiência do utilizador, uma vez que o utilizador acompanha o progresso da análise e obtém os resultados à medida que são produzidos pelo *backend*, com indicadores de risco e indicação do que é recomendado pela SAP, quando existe.

6.7.4 Fluxo Principal do Frontend

A Figura 6.7 apresenta o fluxo principal da camada do *frontend*, desde a autenticação do utilizador até, à execução e à consulta das auditorias. O diagrama evidencia a separação entre a navegação (*frontend*) e a execução técnica (*backend*), bem como o papel da sessão JWT na validação da sessão e no controlo dos acessos.

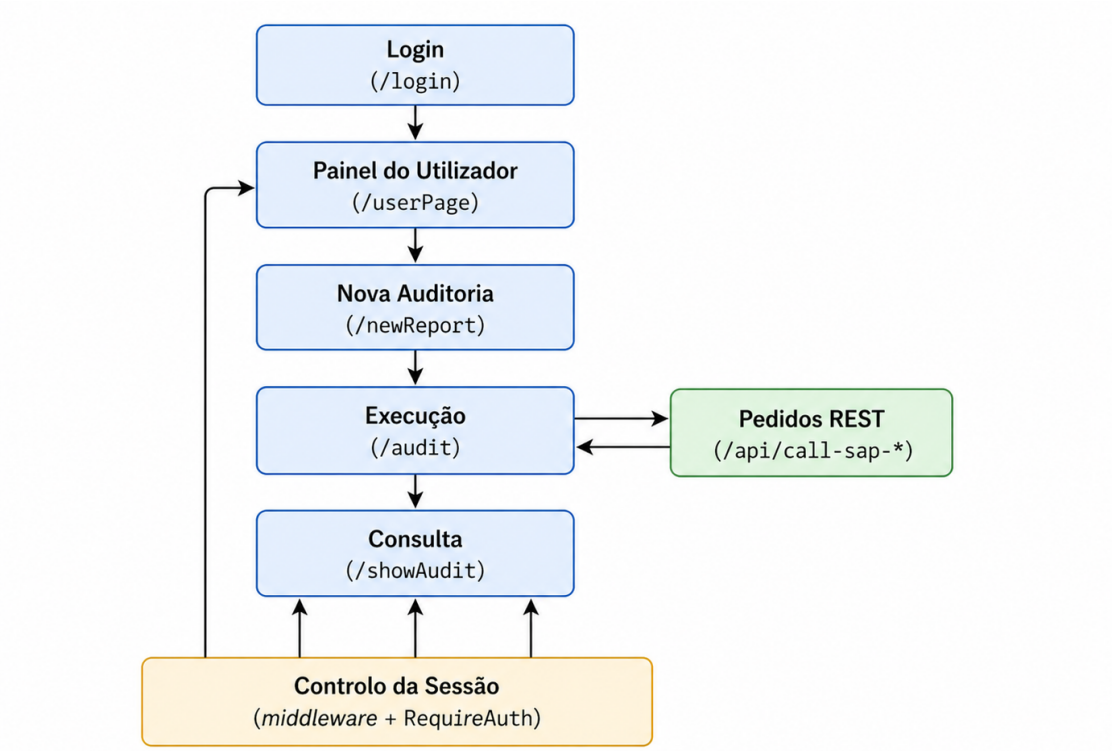

Figura 6.7: *Fluxo de navegação do frontend e interação com o backend. O acesso às páginas internas é condicionado pelo controlo de sessão.*

6.7.5 Apresentação de Resultados e Exportação

Os resultados obtidos através do *backend* são apresentados em listas de modo que o utilizador consiga interpretar e visualizar sem dificuldades, incluindo listas que é possível ordenar, indicadores de *compliance* com a SAP e, quando possível, componentes gráficos para suporte à interpretação dos dados. Através disto, o utilizador consegue identificar rapidamente problemas com um nível de severidade elevado e consegue aceder à evidência correspondente. Além disto, são disponibilizados mecanismos de exportação para formato PDF.

6.8 Configuração da Base de Dados

A persistência dos dados foi realizada com recurso a uma base de dados *MySQL*, onde foram suportados os requisitos fundamentais para o sistema: autenticação de utilizadores, histórico de auditorias, consulta dos resultados e armazenamento de dados relativos a parâmetros *default* e recomendados pela SAP. A opção por uma base de dados com modelo relacional deve-se à necessidade da integridade, suporte a consultas consistentes e facilidade de manutenção em contexto empresarial. Esta camada é exclusivamente acedida pelo *backend*, através de *Spring Data* JPA e *Hibernate*.

6.8.1 Modelo de Dados e Entidades Principais

O modelo de dados assenta em duas entidades centrais:

- **`User`** (tabela `users`): representa os utilizadores com acesso à aplicação;
- **`Report`** (tabela `reports`): representa os relatórios gerados pelos *checks* da auditoria, que ficam associados ao utilizador que os executou.

A relação entre estas entidades é do tipo **1:N**, onde um utilizador pode possuir vários relatórios e cada relatório fica apenas associado a um utilizador.

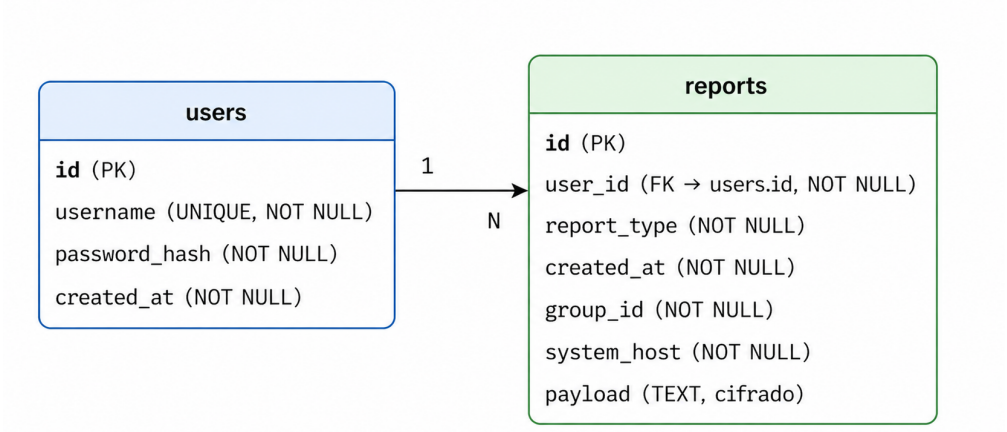

Figura 6.8: *Modelo relacional simplificado da base de dados, evidenciando a relação entre utilizadores e relatórios.*

6.8.2 Persistência dos Relatórios e Identificação pelo `groupId`

Cada auditoria é representada por um relatório que contém diferentes *checks*. Para permitir a rastreabilidade e agregação entre os vários *checks*, a tabela `Report` inclui o campo `group_id`, que identifica todos os *checks* realizados na mesma auditoria. Com isto, é possível agregar todos os *checks* realizados ao mesmo sistema e que foram executados na mesma auditoria. Esta abordagem suporta:

- consulta do histórico por utilizador, com uma lista ordenada cronologicamente;
- consulta por uma execução específica, através do identificador `groupId`;
- síntese do nível de risco por execução, com agregação dos resultados dos vários *checks*.

Além do `group_id`, é guardado `system_host` para identificar o sistema SAP auditado, sendo útil para realizar auditorias a múltiplos ambientes do mesmo cliente (desenvolvimento, qualidade, produção).

6.8.3 Considerações do Desempenho

Apesar do modelo ser simples, a natureza do sistema (execuções recorrentes e histórico crescente) pode justificar otimizações ao nível de índices e de filtragem. Em ambiente produtivo, recomenda-se para um futuro a criação de índices sobre:

- `reports(user_id, created_at)` para melhorar o histórico por utilizador;
- `reports(user_id, group_id)` para consulta por execução;
- `reports(system_host)` para filtragem por sistema auditado.

Estas otimizações mostram-se relevantes em cenários com múltiplos utilizadores e com um elevado número de execuções.

6.8.4 Configuração dos Valores de Referência da SAP

Para suportar a validação dos *checks* de auditoria, os valores recomendados pela SAP não são definidos diretamente na lógica da aplicação. Em vez disso, são armazenados em tabelas dedicadas na base de dados.

Estas tabelas contêm os parâmetros e os respetivos valores de referência utilizados na avaliação dos sistemas analisados. Cada registo corresponde a um critério de validação, podendo incluir o identificador do parâmetro, o valor recomendado e, opcionalmente, informação adicional (por exemplo, descrição ou nível de severidade).

Esta abordagem apresenta várias vantagens:

- **Facilidade de manutenção**: os valores podem ser atualizados diretamente na base de dados, sem necessidade de alterar o código;
- **Flexibilidade**: permite adicionar, remover ou ajustar os campos a validar de forma dinâmica, acompanhando alterações nas recomendações da SAP;

- **Evolução do sistema**: novos *checks* podem ser introduzidos com base na configuração, reduzindo a ligação entre a lógica de negócio e os critérios de validação;
- **Consistência**: centraliza os valores de referência, garantindo que todos os *checks* utilizam a mesma base de comparação.

Desta forma, o sistema torna-se mais adaptável a alterações nas boas práticas de segurança e configuração da SAP, sem comprometer a estabilidade da aplicação.

Com isto, estas melhorias reforçam a robustez operacional e a escalabilidade, mantendo o princípio de minimizar o risco associado à persistência de informação sensível.

6.9 Justificação da Arquitetura Cliente–Servidor

A opção pela arquitetura cliente–servidor com uma separação clara entre *frontend*, *backend* e sistemas SAP foi escolhida com base nos critérios de segurança, escalabilidade e manutenção, uma vez que esta abordagem permite isolar responsabilidades e reduzir o impacto de eventuais vulnerabilidades ou falhas numa das camadas da aplicação.

Ou seja, a camada do *frontend* é responsável exclusivamente pela interação com o utilizador e não possui qualquer acesso direto aos sistemas SAP, nem à base de dados. Todo o processamento sensível, incluindo autenticação, gestão dos acessos e execução das análises de segurança é realizado pelo *backend*.

Ainda assim, esta arquitetura facilita a evolução futura da aplicação, permitindo a substituição ou atualização de componentes individuais, sem gerar um impacto significativo nas restantes camadas.

6.10 Decisão Tecnológica: API REST

A comunicação entre o *frontend* e o *backend* foi implementada através de uma API REST, utilizando o protocolo HTTP e mensagens no formato JSON. Esta escolha foi motivada pela simplicidade, compatibilidade e pelo conhecimento das ferramentas adquiridas ao longo do caminho profissional e académico, o que tornou a execução mais rápida e simples.

Foram consideradas alternativas como SOAP ou a comunicação direta à base de dados. No entanto, estas abordagens apresentam maior complexidade, menor flexibilidade e dificuldades acrescidas na integração com interfaces *web* modernas.

A utilização da API REST permite:

- criar uma separação clara entre a camada do *frontend* e a lógica no *backend*;
- possibilitar uma integração simples com ferramentas ou outros serviços externos;
- definir rigorosamente as permissões de acesso ao nível de cada *endpoint*;
- utilizar mecanismos de autenticação como o JWT.

Esta opção revelou-se a mais adequada tendo em conta o objetivo e enquadramento da aplicação.

6.11 *Security-by-design* no Desenvolvimento

O desenvolvimento da aplicação foi realizado segundo os princípios de *security-by-design*, permitindo que os requisitos de segurança fossem considerados desde as fases iniciais do projeto e não apenas como um complemento posterior.

Entre os métodos utilizados destacam-se:

- princípio do menor privilégio;
- articulação das responsabilidades entre os componentes;
- validação de todos os utilizadores e permissões;
- proteção da comunicação entre todas as camadas;
- minimização da exposição de dados sensíveis.

A aplicação destes princípios traduziu-se em decisões concretas, como a utilização de utilizadores técnicos SAP, a execução das análises em modo *read-only* por omissão e a implementação de mecanismos de autenticação e autorização.

6.12 Criptografia Simétrica

A proteção dos dados foi implementada através de criptografia simétrica, utilizando o algoritmo AES-256, em modo GCM. Esta escolha resultou da necessidade de garantir a confidencialidade e a integridade dos dados, mantendo, simultaneamente, um impacto mínimo no desempenho da aplicação.

A criptografia simétrica apresenta várias vantagens em cenários onde grandes volumes de dados precisam de ser cifrados e decifrados de forma frequente e rápida, como é o caso dos relatórios de auditoria criados pela aplicação. O modo GCM foi selecionado devido ao facto de fornecer mecanismos de autenticação integrados, reduzindo o risco de manipulação ou corrupção dos dados.

6.13 Visualização dos Resultados

Os resultados das análises são apresentados de forma estruturada, permitindo ao utilizador identificar rapidamente as configurações inseguras, fora da ***compliance*** da SAP ou suscetíveis de melhorias.

Para além da visualização imediata, a aplicação permite a criação de relatórios PDF que consolidam os resultados obtidos, dando a possibilidade de serem utilizados em contextos de auditoria, conformidade e acompanhamento da evolução do nível de segurança ao longo do tempo nos sistemas.

6.13.1 Visão Geral das Funcionalidades

A aplicação integra um conjunto de funcionalidades organizadas de forma modular, permitindo uma utilização estruturada e intuitiva. De forma geral, estas funcionalida-

des abrangem:

- configuração e gestão de ligações aos sistemas SAP;
- execução automatizada de análises de segurança;
- visualização e interpretação dos resultados obtidos;
- criação de relatórios que suportam a auditoria;
- gestão de utilizadores e controlo dos acessos.

Esta organização funcional contribui para a separação de responsabilidades e facilita a evolução da aplicação.

6.13.2 Configuração e Ligação aos Sistemas SAP

A funcionalidade de configuração permite definir os parâmetros necessários para estabelecer a ligação aos sistemas SAP alvo de análise. O utilizador é obrigado a especificar o sistema a analisar e os dados técnicos associados, garantindo que a comunicação é realizada de forma controlada e segura.

6.13.3 Execução de Análises de Segurança

Após a configuração do sistema SAP, a aplicação inicia a execução das várias análises de segurança de forma automatizada. Estas análises incidem sobre um conjunto de configurações e parâmetros reconhecidos como críticos no contexto da segurança SAP.

O processo de execução é desencadeado pelo utilizador e decorre integralmente no *backend* da aplicação, garantindo que a recolha e avaliação da informação não interferem com o funcionamento normal do sistema SAP analisado e que o utilizador não consegue alterar ou interagir diretamente com a análise.

6.13.4 Visualização dos Resultados

Os resultados das análises são apresentados através de interfaces gráficas (tabelas, gráficos circulares e de barras) que permitem ao utilizador identificar rapidamente as configurações inseguras ou suscetíveis de melhoria. Cada resultado é acompanhado por uma classificação de *compliance* SAP.

6.13.5 Gestão dos Utilizadores e Controlo dos Acessos

A aplicação integra funcionalidades que permitem realizar a gestão de utilizadores, onde é possível realizar a criação e modificação. O controlo dos acessos é aplicado de forma a restringir o uso das funcionalidades com base no perfil do utilizador.

Esta abordagem garante que todas as operações sensíveis, como a execução de análises ou a consulta de resultados detalhados, estão protegidas contra acessos não autorizados e que cada utilizador apenas consegue ter acesso às suas próprias análises.

6.14 Limitações da Aplicação Desenvolvida

Apesar de os resultados alcançados serem bastante positivos, a aplicação apresenta algumas limitações que importa reconhecer e analisar. A eficácia das análises depende, em grande parte, das permissões atribuídas aos utilizadores técnicos utilizados durante a ligação aos sistemas SAP. Algumas das configurações restritivas podem limitar o acesso a determinados parâmetros/configurações, o que condiciona a qualidade da análise.

Adicionalmente, a aplicação centra-se em vulnerabilidades recorrentes e configurações amplamente reconhecidas como críticas. Com isto, as auditorias mais detalhadas ou análises especializadas a código não *standard* SAP não podem ser ignoradas. Estas limitações refletem opções conscientes do *design*, orientadas para a automatização e escalabilidade, em detrimento de análises exaustivas de todos os componentes do sistema SAP.

6.15 Síntese do Capítulo

No presente capítulo foi apresentado o desenvolvimento da aplicação proposta, destacando a arquitetura, os principais mecanismos de segurança implementados e o processo de automatização da análise. A solução desenvolvida permite reduzir significativamente o esforço manual associado a auditorias de segurança, promovendo uma abordagem sistemática e repetível.

As decisões de *design* adotadas durante todo o projeto refletem o compromisso entre a segurança, usabilidade e escalabilidade, reconhecendo simultaneamente as limitações inerentes à automatização. O capítulo seguinte incide sobre a visualização e interação com a aplicação do lado do utilizador.

Página intencionalmente deixada em branco.

7

Visualização e Interação com a Aplicação

Após a descrição detalhada da arquitetura, das decisões de *design* e da implementação técnica da solução, torna-se relevante apresentar o aspeto visual da aplicação desenvolvida e a forma como o utilizador interage com a aplicação. Este capítulo tem como objetivo ilustrar a interface gráfica da aplicação, evidenciando a organização funcional e a forma como funciona o processo da auditoria de segurança nos sistemas SAP.

A apresentação visual da aplicação não tem apenas um propósito estético, mas desempenha um papel fundamental na usabilidade, na clareza da informação apresentada e no apoio à tomada de decisão por parte do utilizador. As interfaces foram projetadas de forma a permitir uma navegação intuitiva, garantindo simultaneamente que a informação sensível é apresentada de forma controlada e contextualizada.

7.1 Ecrã de Autenticação

O primeiro ponto de contacto do utilizador com a aplicação é o ecrã de autenticação, responsável por garantir que apenas utilizadores devidamente registados e autorizados conseguem aceder às funcionalidades internas do sistema. Este ecrã solicita as credenciais de acesso (nome de utilizador e palavra-passe) e estabelece a sessão autenticada através dos mecanismos descritos no capítulo anterior. Caso o utilizador não possua uma conta, pode registar-se e criar uma nova conta.

A simplicidade do ecrã de autenticação contribui para reduzir erros durante a utilização e reforça a separação clara entre utilizadores autenticados e não autenticados.

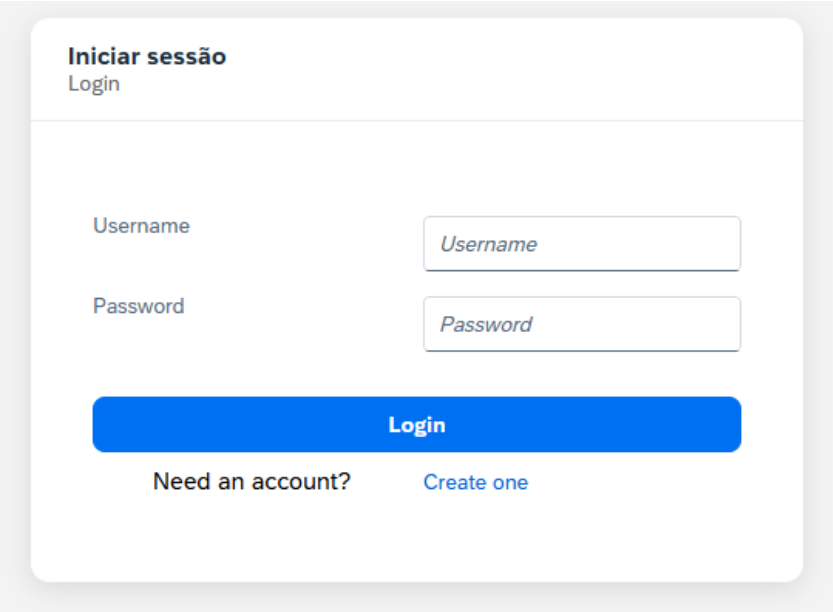

Figura 7.1: *Ecrã de autenticação da aplicação.*

7.2 Painel Principal

Após a autenticação, o utilizador é redirecionado para o painel principal da aplicação. Este painel disponibiliza uma visão global do estado das auditorias realizadas, incluindo informação agregada sobre o nível de conformidade, número de auditorias executadas e distribuição dos resultados por sistema SAP.

A apresentação dos gráficos e indicadores visuais permite que o utilizador identifique, rapidamente, situações de maior risco, facilitando a priorização de ações corretivas e a visualização de todo o histórico de análises.

Caso não exista nenhuma auditoria executada o utilizador apenas tem acesso a um botão onde é permitido realizar uma nova auditoria.

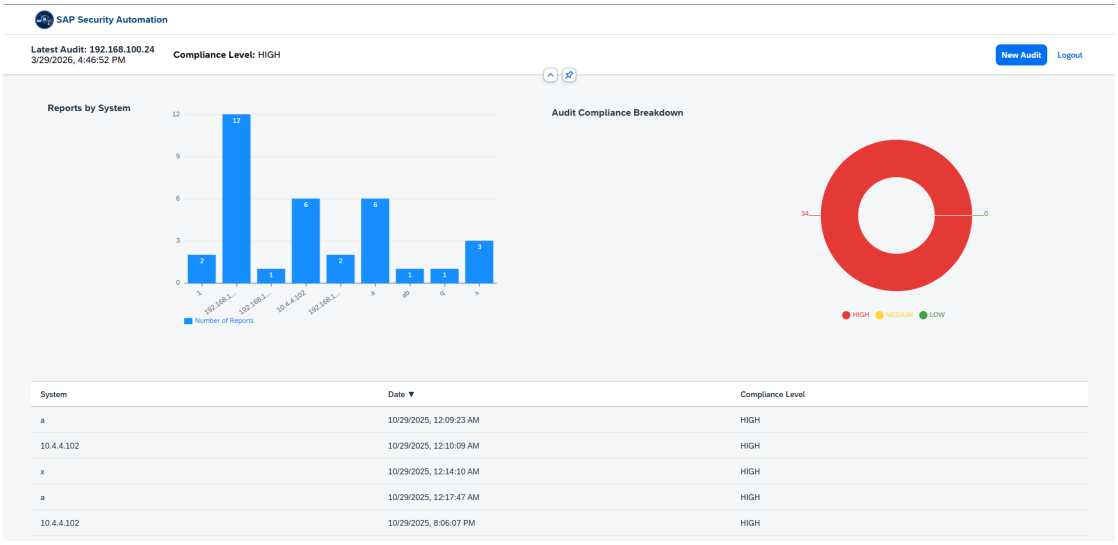

Figura 7.2: *Painel principal da aplicação.*

7.3 Configuração da Auditoria

A aplicação disponibiliza um ecrã dedicado à configuração de novas auditorias de segurança. Neste ecrã, o utilizador introduz os parâmetros necessários para estabelecer a ligação ao sistema SAP alvo de análise, tais como o IP do sistema, o número da instância, mandante, utilizador técnico, palavra-passe do utilizador e o idioma do *login*.

Todos estes primeiros dados e configuração é realizada de forma explícita e controlada, com isto permite o utilizador definir o contexto da auditoria antes da sua execução. A separação deste passo contribui para reduzir erros de configuração e reforça a rastreabilidade das auditorias efetuadas.

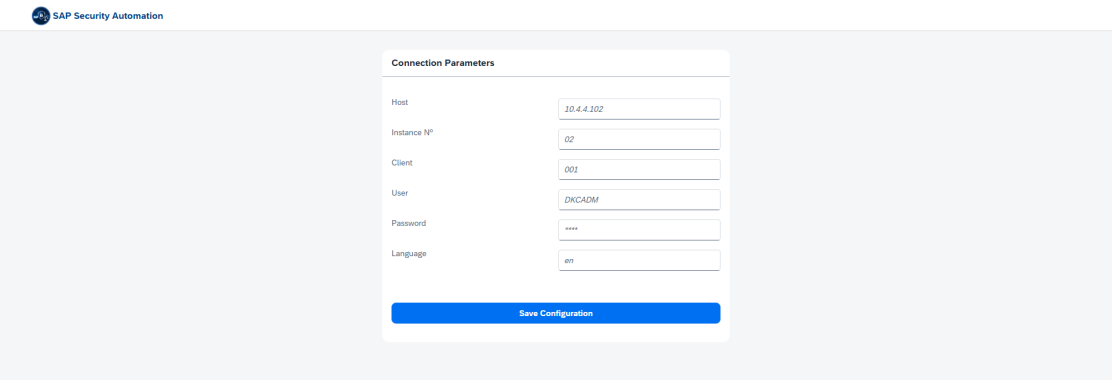

Figura 7.3: *Ecrã de configuração de uma nova auditoria de segurança.*

7.4 Execução e Consulta Detalhada de Auditorias

Após a execução da auditoria, os resultados podem ser consultados de forma detalhada. A aplicação apresenta os resultados organizados por cada tipo de verificação (*check*), incluindo o nível global de conformidade, a data de execução e as evidências recolhida.

Os resultados são apresentados de forma estruturada e em formato de tabelas, através disto é possível identificar rapidamente as configurações incorretas. A utilização de cores e indicadores visuais facilita a distinção entre os diferentes níveis de risco.

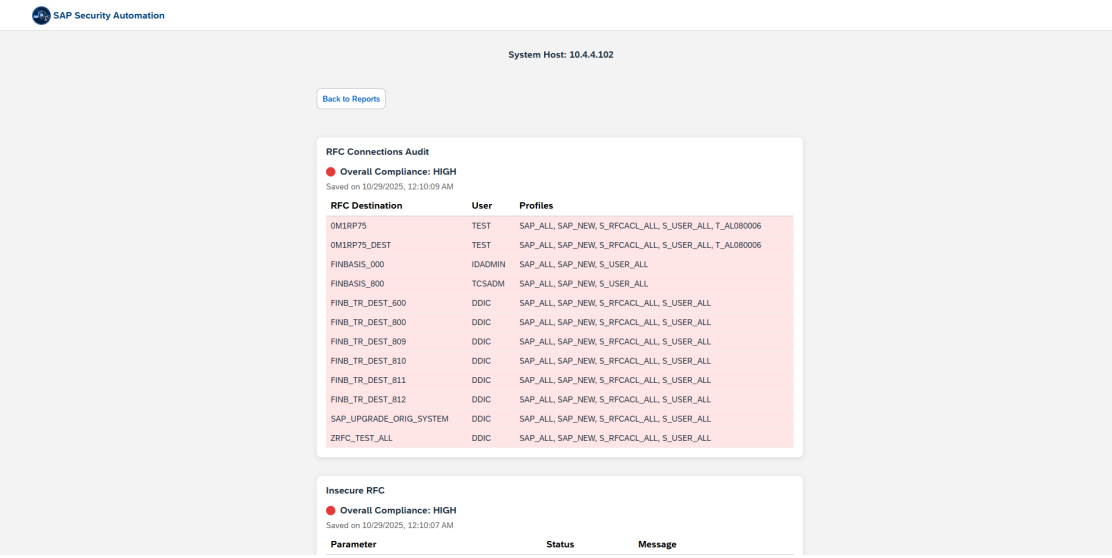

Figura 7.4: *Consulta detalhada de uma auditoria de segurança, evidenciando as verificações e os resultados.*

7.5 Histórico de Auditorias

Para além da consulta imediata, a aplicação mantém um histórico das auditorias realizadas. Este histórico permite acompanhar a evolução do sistema ao longo do tempo, consultar as auditorias anteriores e comparar resultados entre diferentes execuções e sistemas SAP.

Esta funcionalidade é particularmente relevante em contextos de auditoria contínua e conformidade, pois permite demonstrar as melhorias progressivas ou identificar a recorrência das configurações.

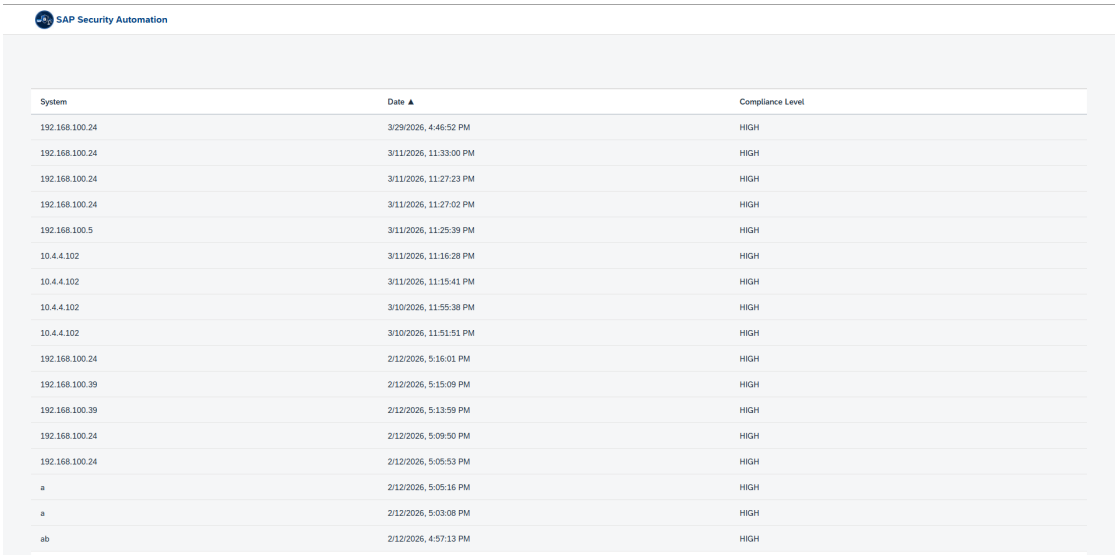

Figura 7.5: *Histórico de auditorias realizadas, organizado por data.*

7.6 Síntese do Capítulo

Neste capítulo foi apresentada a interface gráfica da aplicação desenvolvida, ilustrando os principais ecrãs e modos de interação disponíveis ao utilizador a prática. A componente visual complementa a implementação técnica descrita nos capítulos anteriores, pois demonstra a forma concreta como a solução suporta o processo de auditoria de segurança em sistemas SAP de forma intuitiva, estruturada e segura.

No capítulo seguinte será realizada a análise de resultados e a avaliação dos sistemas, o que permitirá visualizar as reais vantagens da aplicação.

Página intencionalmente deixada em branco.

8

Resultados e Avaliação

Este capítulo apresenta os resultados obtidos com a aplicação desenvolvida para automatização da análise de segurança em sistemas SAP. Os testes foram realizados em diferentes ambientes, com particular incidência num sistema SAP IDES, que contém uma configuração completa de módulos e dados representativos de um cenário empresarial real.

Este tipo de sistema inclui uma elevada diversidade de configurações, utilizadores e parâmetros, o que o torna particularmente adequado para avaliar a capacidade de ferramentas de auditoria em identificar vulnerabilidades e configurações inseguras. Em vários casos, estes ambientes mantêm configurações menos restritivas ou componentes ativos para efeitos de demonstração e aprendizagem, o que permite observar diferentes tipos de problemas de segurança. O relatório deste sistema analisado pode ser consultado no documento "*System Audit Report*"na secção de Anexos.

O objetivo principal desta fase consistiu em avaliar a capacidade da aplicação para identificar vulnerabilidades e parâmetros de segurança inadequados, bem como validar o correto funcionamento dos mecanismos de análise, armazenamento e apresentação dos resultados.

8.1 Objetivos da Avaliação Experimental

A fase dos resultados e avaliação teve como principal objetivo validar a eficácia, eficiência e fiabilidade da aplicação desenvolvida para automatização da análise de segurança nos sistemas SAP. Esta validação não se limitou à verificação funcional da aplicação, procurou também avaliar o seu impacto prático quando comparada com as abordagens tradicionais de auditoria manual.

De forma mais específica, a avaliação experimental procurou responder às seguintes questões:

- A aplicação é capaz de identificar vulnerabilidades reais em ambientes SAP?
- Os resultados obtidos são consistentes e reprodutíveis?

- Qual é a vantagem em termos de eficiência face às auditorias manuais tradicionais?
- O armazenamento e a apresentação dos resultados preservam os princípios de segurança definidos?

Estas questões orientaram a definição das métricas utilizadas, a seleção dos ambientes de teste e a interpretação crítica dos resultados obtidos.

8.2 Ambientes de Teste

Os testes foram realizados em três contextos distintos:

- **Ambiente de Desenvolvimento (Development System (DES)):**
  Este ambiente foi utilizado principalmente para testes iniciais de integração entre a aplicação desenvolvida e os sistemas SAP. Nesta fase foram validadas as chamadas RFC, o tratamento de exceções e a execução dos diferentes *checks* de segurança implementados.
- **Ambiente de Testes / Qualidade (Quality Assurance System (QAS)):**
  Este ambiente corresponde a um cenário intermédio entre desenvolvimento e produção. Normalmente trata-se de uma cópia do sistema produtivo com dados anonimizados, sendo utilizado para validar alterações e novos desenvolvimentos antes da sua introdução em produção.
  Este sistema permitiu avaliar o comportamento da aplicação em condições mais próximas de um ambiente real de operação.
- **Ambiente do tipo IDES:**
  Este sistema inclui múltiplos módulos SAP, como Financial Accounting (FI), Controlling Obejcts (CO), Materials Management (MM), Sales and Distribution (SD) e Human Resources (HR), bem como uma base de dados extensa e diversas configurações de segurança. Devido à sua complexidade e diversidade de dados, revelou-se particularmente adequado para identificar vulnerabilidades típicas em sistemas que não seguem rigorosamente as melhores práticas de segurança.

A maioria das análises foram realizada neste último ambiente, uma vez que permite observar um conjunto mais diversificado de vulnerabilidades e configurações inseguras.

8.3 Avaliação da Eficiência Temporal

Um dos principais benefícios da automatização da análise de segurança consiste na redução significativa do tempo necessário para a realização de auditorias. Para avaliar este aspeto, foi analisado o tempo necessário para executar uma auditoria completa através da aplicação desenvolvida.

O processo de auditoria automatizada inclui as seguintes etapas:

- estabelecimento da ligação ao sistema SAP através de RFCs;
- execução sequencial das verificações de segurança implementadas;
- processamento e classificação dos resultados obtidos;
- armazenamento seguro do relatório gerado;
- disponibilização imediata dos resultados no *frontend*.

Durante os testes realizados, o tempo total necessário para executar uma auditoria completa situou-se entre, aproximadamente **30 e 90 segundos**. Esta variação depende essencialmente de fatores como:

- latência da ligação RFC;
- número de verificações ativas;
- volume de dados existente no sistema analisado.

Mesmo em ambientes com maior quantidade de dados, o tempo de execução manteve-se consistentemente inferior a dois minutos, demonstrando a eficiência da abordagem automatizada.

8.4 Reprodutibilidade e Consistência dos Resultados

Para além da eficiência operacional, a consistência dos resultados constitui um aspeto fundamental na avaliação de ferramentas de auditoria de segurança.

Durante os testes realizados, a aplicação foi executada repetidamente sobre os mesmos sistemas SAP, mantendo-se inalteradas as configurações e parâmetros do sistema. Em todas as execuções realizadas, os resultados obtidos permaneceram consistentes, tendo sido identificadas as mesmas vulnerabilidades sempre que o estado do sistema se manteve inalterado.

Esta estabilidade decorre do caráter determinístico da solução, baseada em regras de verificação explícitas e critérios objetivos de análise. Ao contrário das auditorias manuais, nas quais a interpretação humana pode introduzir variações, a automatização garante uniformidade na execução das verificações e na geração dos resultados.

8.5 Resultados Obtidos

Durante os testes realizados, a aplicação identificou diversas vulnerabilidades e configurações inseguras nos sistemas analisados. Entre os principais resultados obtidos destacam-se os seguintes:

Tabela 8.1: *Algumas das vulnerabilidades identificadas nos sistemas SAP analisados*

Verificação	Exemplo de vulnerabilidade identificada	Incidência
Contas padrão com *passwords* por omissão	Utilizadores como `SAP*` ou `DDIC` com *passwords* conhecidas	1 sistema
Parâmetros de segurança inadequados	Parâmetros de segurança configurados não compatíveis com os valores recomendados pela SAP	3 sistemas
Gestão insegura de *passwords*	Parâmetros de *passwords* configurados não compatíveis com os valores recomendados pela SAP	3 sistemas
Clientes padrão ativos	Clientes `000`, `001` ou `066` acessíveis	3 sistemas
RFCs inseguras	Ligações RFC com utilizadores com privilégios elevados	1 sistema
Default Encryption Key	Utilização da chave de cifragem por omissão do sistema	3 sistemas
RFC Gateway ACL inseguro	Configurações de *gateway* com permissões insuficientemente restritivas	3 sistemas
Web Services inseguros	Serviços SOAP ou HTTP ativos sem autenticação adequada	3 sistemas
Utilizadores de diálogo com autorizações críticas	Perfis com acesso a funcionalidades administrativas	3 sistemas

Estes resultados demonstram que a aplicação foi capaz de identificar automaticamente diferentes categorias de vulnerabilidades presentes nos sistemas analisados.

8.6 Avaliação de Desempenho e Comparação com Auditoria Manual

Para além da identificação de vulnerabilidades, um dos objetivos centrais da solução desenvolvida consiste na redução significativa do tempo necessário para a realização de auditorias de segurança em sistemas SAP. Nesta secção é apresentada uma comparação entre o tempo médio associado às auditorias manuais tradicionais e o tempo observado durante a execução da aplicação desenvolvida.

A automatização das verificações de segurança permite reduzir substancialmente o esforço manual necessário para analisar configurações, parâmetros e autorizações em sistemas SAP. Desta forma, torna-se possível executar auditorias com maior frequência e com menor dependência de intervenção humana.

8.6.1 Auditoria Manual em Sistemas SAP

A realização de auditorias de segurança em sistemas SAP de forma manual exige conhecimento especializado da plataforma e envolve a execução de múltiplas transações administrativas. Entre as transações mais utilizadas neste tipo de análise encontram-se, por exemplo, `SU01`, `RZ10`, `RZ11`, `SM59`, `SCC4` e `SMGW`.

Cada uma destas transações permite analisar diferentes aspetos da configuração de segurança do sistema, incluindo utilizadores, parâmetros de autenticação, ligações remotas, clientes ativos e permissões atribuídas. O processo manual implica não só a consulta destas configurações, mas também a interpretação dos resultados obtidos, a comparação com valores considerados seguros e recomendados e ainda a realização da documentação relativa a cada análise.

Mesmo quando executada por profissionais da área de SAP Basis, este processo pode exigir várias horas de trabalho, uma vez que envolve a recolha e análise manual de informação dispersa por diferentes componentes do sistema.

Com base em práticas comuns de auditoria e na experiência profissional em ambientes SAP, é possível estimar o tempo médio necessário para avaliar manualmente cada categoria de vulnerabilidade analisada.

8.6.2 Execução Automatizada com a Aplicação Desenvolvida

A aplicação desenvolvida automatiza o processo de auditoria através da execução sistemática de verificações de segurança implementadas em módulos específicos. Estas verificações são realizadas através de chamadas RFC, permitindo aceder diretamente às configurações e parâmetros do sistema.

Durante a execução de uma auditoria automatizada são realizadas as seguintes etapas:

- estabelecimento da ligação ao sistema SAP;
- execução sequencial dos *checks* de segurança definidos;
- recolha e processamento dos dados obtidos;
- classificação das vulnerabilidades identificadas;
- armazenamento seguro do relatório gerado;
- disponibilização dos resultados na interface de utilizador.

Nos testes realizados, o tempo total necessário para executar uma auditoria completa situou-se entre aproximadamente **30 e 90 segundos**.

Mesmo em ambientes com maior quantidade de dados e configurações, o tempo de execução manteve-se consistentemente inferior a dois minutos, evidenciando a eficiência da aplicação desenvolvida.

8.6.3 Comparação de Tempos

A Tabela 8.2 apresenta uma comparação entre o tempo necessário para executar manualmente cada verificação de segurança e o tempo observado durante a execução da aplicação desenvolvida. As métricas do tempo manual foram obtidas através da experiência do autor na execução das análises.

Tabela 8.2: *Comparação entre auditoria manual e automatizada*

Verificação	Atividades	Tempo Manual	Tempo Auto.
Contas padrão	Análise de utilizadores e testes de autenticação	20–30 min	<5 s
Parâmetros de segurança	Consulta e validação nas transações `RZ10` e `RZ11`	30–45 min	<10 s
Clientes padrão	Verificação de mandantes ativos na transação `SCC4`	10–15 min	<5 s
Ligações RFC	Análise de utilizadores e permissões associadas	30–60 min	10–15 s
RFC Gateway	Verificação de configurações de segurança e *ACLs*	20–30 min	<10 s
Web Services	Identificação de serviços ativos e análise de autenticação	20–30 min	<10 s
Autorizações críticas	Análise de perfis, *roles* e privilégios administrativos	60–90 min	10–20 s
Chaves de encriptação	Análise da *Secure Storage*	5–10 min	5–10 s
Auditoria completa	—	**3–5 horas**	**30–90 s**

Os resultados demonstram que a abordagem automatizada permite reduzir drasticamente o tempo necessário para realizar auditorias de segurança em sistemas SAP. Enquanto uma auditoria manual completa pode exigir várias horas de trabalho especializado, a solução desenvolvida permite executar o mesmo conjunto de verificações em menos de dois minutos.

8.6.4 Impacto Operacional

A redução significativa do tempo necessário para executar auditorias tem impacto direto na forma como a segurança pode ser gerida nos ambientes SAP.

A automatização das verificações permite aumentar a frequência das auditorias, possibilitando a deteção mais precoce de configurações inseguras ou alterações potencialmente perigosas no sistema. Além disto, reduz a dependência de tarefas manuais repetitivas, permitindo que os profissionais responsáveis pela segurança concentrem a análise dos resultados obtidos e na implementação de medidas corretivas.

É importante salientar que a automatização não substitui auditorias de segurança mais aprofundadas ou análises específicas que exigem conhecimento especializado. No

entanto, constitui um mecanismo eficaz de verificação inicial, capaz de identificar rapidamente riscos críticos e apoiar a monitorização contínua da segurança dos sistemas.

8.7 Limitações da Avaliação Experimental

Apesar dos resultados positivos obtidos, é importante reconhecer algumas limitações inerentes ao presente projeto.

Os testes foram realizados num conjunto limitado de sistemas, o que impede generalizações absolutas para todos os ambientes SAP. Além disso, a aplicação centra-se principalmente na identificação de vulnerabilidades relacionadas com configurações de segurança e parâmetros do sistema, não incluindo uma análise aprofundada a código ABAP personalizado.

Estas limitações não invalidam os resultados obtidos, mas ajudam a delimitar o âmbito da solução desenvolvida.

8.8 Considerações Finais

A avaliação realizada demonstrou que a aplicação desenvolvida é capaz de identificar automaticamente diversas vulnerabilidades e configurações inseguras nos sistemas SAP.

Os resultados obtidos evidenciam também que a automatização da auditoria permite reduzir significativamente o tempo necessário para realizar análises de segurança, mantendo simultaneamente consistência e fiabilidade nos resultados produzidos.

Deste modo, a solução proposta constitui um contributo relevante para a melhoria dos processos de auditoria de segurança em ambientes SAP, permitindo apoiar equipas técnicas na identificação precoce de riscos e na melhoria contínua das configurações de segurança dos sistemas.

Página intencionalmente deixada em branco.

9
Conclusões e Trabalho Futuro

O presente capítulo sintetiza os principais resultados obtidos ao longo do desenvolvimento do projeto, assim como as conclusões que retiradas da análise do trabalho realizado. Procura-se, assim, refletir sobre o grau de concretização dos objetivos inicialmente definidos, avaliando o contributo da solução proposta no contexto da segurança dos sistemas SAP.

Para além da análise conclusiva, são apresentadas e analisadas possíveis melhorias futuras, tendo em consideração as limitações identificadas e as oportunidades de melhoria detetadas. Estas perspetivas permitem enquadrar o trabalho desenvolvido como um ponto de partida para investigações e desenvolvimentos subsequentes, reforçando o seu potencial de adaptação a novos requisitos e contextos tecnológicos.

9.1 Conclusões

O presente trabalho teve como objetivo o desenvolvimento de uma solução para a automatização da análise de segurança em sistemas SAP, respondendo a uma necessidade concreta das organizações que dependem destes sistemas para suportar processos de negócio críticos. Ao longo do projeto demonstrou-se que a automatização de verificações de segurança recorrentes permite reduzir significativamente o esforço manual associado às auditorias, aumentar a consistência das análises e acelerar a deteção precoce de configurações inseguras.

A aplicação desenvolvida possibilitou a identificação sistemática de um conjunto alargado de vulnerabilidades amplamente documentadas pela SAP, incluindo contas padrão com palavras-passe por omissão, parâmetros de segurança inadequados, clientes padrão ativos, ligações RFC inseguras, configurações permissivas do RFC Gateway, *web services* expostos e utilizadores com autorizações críticas excessivas. Todos estes resultados validam a relevância prática da solução apresentada no domínio das ferramentas de auditoria preventiva.

Do ponto de vista técnico, a arquitetura adotada, assente numa separação clara en-

tre *frontend*, *backend* e sistemas SAP, revelou-se adequada para garantir modularidade, segurança e escalabilidade. A utilização exclusiva da comunicação via RFC entre o *backend* e os sistemas SAP, de forma controlada, permitiu realizar análises sem impacto operacional nos sistemas analisados, assegurando por defeito um modo de execução *read-only*.

A implementação dos mecanismos de proteção de dados, nomeadamente o armazenamento cifrado dos relatórios, garantiu a confidencialidade e integridade da informação sensível produzida pela aplicação, evitando que o próprio sistema se tornasse um novo vetor de risco. Os testes efetuados demonstraram que o impacto da cifragem no desempenho é residual, o que validou a escolha tecnológica adotada.

A comparação entre auditorias manuais e auditorias automatizadas evidenciou um ganho substancial de eficiência, reduzindo o tempo de análise, que antes variava entre 3 a 5 horas, para apenas de 30 a 90 segundos. Este aspeto assume particular relevância em contextos organizacionais onde a realização de auditorias frequentes é limitada por restrições de tempo e pela disponibilidade de recursos especializados e financeiros.

Para além destes resultados, o trabalho desenvolvido apresenta contributos relevantes no domínio da segurança de sistemas SAP. Destaca-se a criação de uma solução automatizada que promove a execução contínua de análises, reduz a dependência da intervenção manual (o que limita erros humanos) e permite uma identificação mais rápida de riscos críticos. A arquitetura modular adotada facilita a extensão da aplicação com novos *checks*, garantindo flexibilidade e capacidade de evolução. Adicionalmente, a integração de mecanismos de segurança desde a fase de desenvolvimento, nomeadamente autenticação, controlo de acessos e a cifragem de dados, evidencia a aplicação prática dos princípios de *security-by-design*.

Apesar dos resultados positivos obtidos, o trabalho apresenta algumas limitações que importa considerar. A abordagem adotada centra-se principalmente na análise de configurações e vulnerabilidades conhecidas, não abrangendo auditorias mais aprofundadas, como a análise de código ABAP ou validações altamente específicas de determinados módulos SAP. Para além disto, a eficácia das análises depende das permissões associadas ao utilizador técnico utilizado na ligação ao sistema, o que pode demonstrar em limitações no acesso a determinados dados em ambientes mais restritos.

Do ponto de vista da persistência, a opção de armazenar os resultados cifrados garante a proteção da informação sensível, o que limita a capacidade de realizar consultas diretas ao conteúdo dos relatórios ao nível da base de dados. Por fim, a aplicação ainda não integra mecanismos de monitorização contínua ou a integração com plataformas externas de gestão de eventos de segurança.

Em suma, os resultados obtidos demonstram que o projeto desenvolvido cumpre os objetivos definidos, constituindo uma abordagem eficaz, segura e escalável para a automatização da análise de segurança em sistemas SAP. Embora o projeto não substitua na totalidade auditorias mais completas ou análises especializadas a determinados tópicos, a aplicação posiciona-se como uma ferramenta de primeira linha, capaz de

apoiar equipas de segurança e auditoria na identificação célere de riscos críticos.

9.2 Trabalho Futuro

Apesar dos resultados alcançados, o projeto apresenta diversos pontos passíveis de evolução, tanto ao nível técnico, como funcional. O trabalho futuro poderá desenvolver-se em vários tópicos.

9.2.1 Análise Seletiva e Modular dos Componentes SAP

Uma evolução relevante consiste na possibilidade de realizar análises direcionadas apenas a determinadas categorias, permitindo uma maior flexibilidade operacional. Em vez de executar todos os *checks* de forma agregada e sequencial, poderá ser disponibilizada a opção de auditoria segmentada, por exemplo:

- análise exclusiva a ligações e configurações RFC;
- auditoria específica de utilizadores e autorizações;
- verificação isolada de parâmetros de segurança;
- avaliação dedicada a *web services* expostos.

Esta abordagem permitiria adaptar a ferramenta a necessidades concretas, como revisões técnicas pontuais ou validação após alterações específicas no sistema. A modularização dos *checks* reforçaria a eficiência e reduziria o tempo de execução quando apenas determinadas áreas necessitam de validação.

9.2.2 Adaptação a Ambientes SAP na *Cloud*

Uma evolução natural do projeto consiste na adaptação a cenários de migração para ambientes *cloud*, incluindo SAP S/4HANA *Cloud*, SAP RISE e infraestruturas híbridas. Nestes contextos emergem novos desafios relacionados com modelos de responsabilidade partilhada, exposição de APIs externas e gestão de identidades distribuídas.

O trabalho futuro poderá incluir a adaptação dos mecanismos de análise para suportar interfaces específicas de ambientes *cloud*, bem como a integração com ferramentas de monitorização e segurança disponibilizadas pelo ecossistema SAP *Cloud* e por outras ferramentas específicas da SAP.

9.2.3 Expansão dos Tipos de Verificações

Outro ponto de evolução passa pela expansão do tipo de verificações realizadas. Poderão ser incorporados novos *checks* relacionados com:

- segregação de funções (SoD);
- análise aprofundada de autorizações ao nível de objetos e campos;
- deteção de código ABAP inseguro ou desatualizado;

- validação de configurações específicas de outros módulos.

Esta expansão permitirá aumentar o alcance da auditoria e reduzir ainda mais a dependência de processos manuais.

9.2.4 Integração de Técnicas de *Machine Learning*

Esta seria uma evolução com maior nível de complexidade, uma vez que exigiria a integração de técnicas de *machine learning* no processo de análise. Em vez de depender exclusivamente de regras estáticas, a solução poderá evoluir para um modelo adaptativo capaz de:

- identificar padrões históricos de configuração e risco;
- sugerir parâmetros de segurança ajustados ao contexto específico de cada versão do sistema;
- priorizar vulnerabilidades com base em padrões de exposição e criticidade.

Esta abordagem permitiria contextualizar a análise, aproximando-a de um modelo inteligente de apoio à decisão, específico e adequado a cada tipo e versão de sistema SAP.

9.2.5 Evolução para Auditoria Contínua

Por fim, a consolidação do projeto enquanto plataforma de auditoria contínua constitui uma linha de desenvolvimento estratégica. A execução periódica automática das análises, associada a mecanismos de alerta e a indicadores históricos de risco, permitiria acompanhar a evolução do nível de segurança ao longo do tempo.

A integração com *dashboards* analíticos e sistemas de notificações reforçaria o posicionamento da aplicação como instrumento de gestão contínua do risco em ambientes SAP.

Em conjunto, estas linhas de evolução demonstram que o projeto constitui uma base sólida para investigação e desenvolvimento futuros, com potencial para acompanhar a evolução tecnológica dos sistemas SAP e os desafios emergentes no domínio da cibersegurança.

Página intencionalmente deixada em branco.

Bibliography

10KBLAZE and SAP (From an administrative point) (2019). SAP Community (SAP-authored blog). Orientação prática de mitigação e *hardening* em resposta ao 10KBLAZE. URL: https://community.sap.com/t5/technology-blog-posts-by-sap/10kblaze-and-sap-from-an-administrative-point/ba-p/13416227.

10KBLAZE Threat Report (2019). Onapsis Research. Relatório técnico sobre exploração e mitigação de riscos associados ao SAP Gateway (10KBLAZE). URL: https://onapsis.com/resources/reports/10kblaze/.

Abd Elmonem, Mohamed A., Eman S. Nasr e Mohamed H. Geith (2016). «Benefits and challenges of cloud ERP systems – A systematic literature review». Em: *Future Computing and Informatics Journal* 1.1-2, pp. 1–9. DOI: 10.1016/j.fcij.2017.03.003.

Activating and Deactivating ICF Services (s.d.). SAP Help Portal / SAP Library. Descreve o funcionamento do Internet Communication Framework (ICF), a activação hierárquica de serviços web e a gestão de serviços activos através da transacção SICF. URL: https://help.sap.com/doc/saphelp_nw74/7.4.16/en-us/46/d28dfa34bb12bee10000000a1553f7/content.htm.

Alert (AA19-122A): New Exploits for Unsecure SAP Systems (2019). Cybersecurity and Infrastructure Security Agency (CISA). Alerta público sobre exploração de sistemas SAP mal configurados (10KBLAZE). URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-122a.

Alidata (2024). *Alidata ERP*. Acedido em 2026. URL: https://www.alidata.pt.

Aloini, Davide, Riccardo Dulmin e Valeria Mininno (2007). «Risk management in ERP project introduction: Review of the literature». Em: *Information & Management* 44.6, pp. 547–567. DOI: 10.1016/j.im.2007.05.004.

Baskerville, Richard, Paolo Spagnoletti e Jong Seok Kim (2014). «Incident-centered information security: Managing a strategic balance between prevention and response». Em: *Information & Management*.

Behl, Abhishek (2020). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Bjelland, Eirik e Moutaz Haddara (2018). «Evolution of ERP Systems in the Cloud: A Study on System Updates». Em: *Systems* 6.2. O modelo de ciclo de vida de ERP inclui seis fases: adoption decision, acquisition, implementation, use and maintenance, evolution and retirement, p. 22. DOI: 10.3390/systems6020022.

Chang, Yu-Wei (2025). «Analyzing the Impact of ERP and BI Integration on Business Performance: The Technology-Organization-Environment Framework and Balanced Scorecard Perspective». Em: *Journal of Global Information Management* 33.1, pp. 1–19.

Darktrace Research (2025). *Investigation of SAP NetWeaver Exploitation Leading to Malware Infection*. Darktrace Threat Intelligence.

Davenport, Thomas H. (jul. de 1998). «Putting the Enterprise into the Enterprise System». Em: *Harvard Business Review* 76.4, pp. 121–131.

Dutch National Cyber Security Centre (2025). *Advisory on Active Exploitation of SAP S/4HANA Vulnerability CVE-2025-42957*. National Cyber Security Advisory.

European Union Agency for Cybersecurity (ENISA) (2023). *ENISA Threat Landscape 2023*. Rel. téc. ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Färber, Franz et al. (2012). «SAP HANA Database: Data Management for Modern Business Applications». Em: *Proceedings of the VLDB Endowment* 5.12, pp. 1800–1811. DOI: 10.14778/2367502.2367511.

Gartner Inc. (2024). *Market Share Analysis: Enterprise Application Software, Worldwide, 2024*. Gartner Research.

ISACA (2012). *Segregation of Duties Controls: Best Practices*. Rel. téc. ISACA.

Jacobs, F. Robert e F. C. Ted Jr. Weston (2007). «Enterprise resource planning (ERP)—A brief history». Em: *Journal of Operations Management* 25.2, pp. 357–363. DOI: 10.1016/j.jom.2006.11.005.

Klaus, Helmut, Michael Rosemann e Guy G. Gable (2000). «What is ERP?» Em: *Information Systems Frontiers* 2.2, pp. 141–162.

Kumar, K. e J. Van Hillegersberg (2000). «ERP Experiences and Evolution». Em: *Communications of the AIS* 4, pp. 39–61.

Microsoft Corporation (2024). *Microsoft Dynamics 365 ERP Solutions*. Acedido em 2026. URL: https://www.microsoft.com/dynamics-365.

Møller, Charles (2005). «ERP II: a conceptual framework for next-generation enterprise systems?» Em: *Journal of Enterprise Information Management* 18.4, pp. 483–497. DOI: 10.1108/17410390510609626.

Monk, Ellen e Bret Wagner (2012). *Concepts in Enterprise Resource Planning*. Cengage Learning.

National Institute of Standards and Technology (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. Rel. téc. NIST. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

O'Leary, D. E. (2000). «Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk». Em: *Cambridge University Press*.

Onapsis (2016). *Securing Clients in SAP S/4HANA and NetWeaver ABAP*. Discusses default clients (001, 066) and recommends removal if unused to reduce attack surface. URL: https://onapsis.com/blog/securing-clients-sap-s4hana-and-netweaver-abap/.

Onapsis (s.d.). *SAP Cybersecurity 101: Understanding the Basics*. Acedido em 2026-02-17. URL: https://onapsis.com/blog/sap-cybersecurity-101-understanding-the-basics.

Onapsis Research (2019). *TMSADM User Default Password: Another Risk for Your SAP System*. Onapsis Blog. Caso real de utilizador padrão SAP com palavra-passe por omissão identificado em ambientes produtivos. URL: https://onapsis.com/blog/tmsadm-user-default-password-another-risk-your-sap-system/.

Onapsis Research Labs (2020). *RECON: Critical Vulnerabilities in SAP NetWeaver AS Java*. Onapsis Threat Research. Acedido em 19 fevereiro 2026. URL: https://onapsis.com/threat-research/recon/.

Oracle Corporation (2024). *Oracle Cloud ERP Overview*. Acedido em 2026. URL: https://www.oracle.com/erp/.

Pfleeger, Charles P. e Shari Lawrence Pfleeger (2015). *Security in Computing*. 5th. Prentice Hall.

PHC Software (2024). *Sobre a PHC*. Acedido em 2026. URL: https://www.phcsoftware.com/pt/.

Plattner, Hasso (2012). *SAP HANA: An In-Memory Database and Computing Platform*. Springer.

Primavera BSS (2024). *Sobre a Primavera BSS*. Acedido em 2026. URL: https://www.primaverabss.com/pt/.

Profile Parameters for Logon and Password (2010). SAP Help Portal. Documenta os parâmetros de sistema relacionados com autenticação e políticas de palavras-passe, incluindo comprimento mínimo, validade, histórico e controlo de tentativas de login. URL: https://help.sap.com/saphelp_em700_ehp01/helpdata/en/4a/c3f18f8c352470e10000000a42189c/content.htm.

Protecting Standard Users (2007). SAP Help Portal. Recomenda a alteração de passwords e proteção de utilizadores standard (SAP*, DDIC, EARLYWATCH). URL: https://help.sap.com/docs/SAP_NETWEAVER_701/6f3c4a7b6c4b1014a618b83e6fade755/3ecdaccbedc411d3a6510000e835363f.html.

«Running Business Applications in the Cloud – A Use Case Perspective» (2010). Em: *Running Business Applications in the Cloud: A Use Case Perspective*. DOI: 10.1007/978-3-642-21878-1_73.

Sadiq, Shazia, Guido Governatori e Kioumars Namiri (2007). «Modeling Control Objectives for Business Process Compliance». Em: *Business Process Management Journal* 13.5.

Sage Group plc (2024). *Sage Business Solutions*. Acedido em 2026. URL: https://www.sage.com.

SAP Company Information (2023). SAP Official Website. URL: https://www.sap.com/about/company.html.

SAP Gateway Security Files: secinfo and reginfo (2015). SAP Help Portal / SAP Library. Documenta os ficheiros de controlo de acesso do RFC Gateway (secinfo e reginfo), os parâmetros de perfil associados e o papel destes ficheiros na segurança de ligações externas via RFC. URL: https://help.sap.com/docs/ABAP_PLATFORM_NEW/621bb4e3951b4a8ca633ca7ed1c0aba2/e216d0427a2440fc8bfc25e786b8e11c.html.

SAP Note 1529805: SU01 – Additional authorization check when setting password (2011). SAP Support Portal. Introduz verificações adicionais de autorização para operações sensíveis relacionadas com manutenção de utilizadores. URL: https://me.sap.com/notes/1529805.

SAP Product Portfolio (2026). SAP Official Website. URL: https://www.sap.com/products.html.

SAP RFC Security Resources (s.d.). *Technical Considerations for Securing RFC Connections*. Discusses risks e boas práticas de segurança para conexões RFC em SAP, incluindo autorizações e medidas de mitigação. URL: https://onapsis.com/blog/securing-sap-remote-function-calls-the-crucial-role-of-s-icf-authorization/.

SAP SE (2012). *SAP Note 1749142*. SAP Support Portal. Acesso sujeito a autenticação no SAP Support Portal. URL: http://service.sap.com/sap/support/notes/1749142.

SAP SE (2023). *SAP Security Recommendations: Securing Remote Function Calls (RFC)*. Security Whitepapers (SAP Support Portal). SAP recomenda configurações seguras para chamadas RFC, limitação de autorizações e proteção de comunicações. URL: https://support.sap.com/en/security-whitepapers.html.

SAP SE (2024a). *SAP History*. Acedido em 2026. URL: https://www.sap.com/about/company/history.html.

SAP SE (2024b). *SAP S/4HANA Architecture Overview*. URL: https://help.sap.com/docs/SAP_S4HANA.

SAP SE (2024c). *SAP S/4HANA Deployment Options and Cloud Strategy*. URL: https://www.sap.com/products/s4hana/deployment.html.

SAP SE (2024d). *SAP S/4HANA Overview*. Acedido em 2026. URL: https://www.sap.com/products/s4hana-erp.html.

SAP SE (s.d.). *RFC Authorizations and the S_RFC Authorization Object*. SAP Help Portal. Descrição do objeto de autorização S_RFC que controla acesso a funções RFC. URL: https://help.sap.com/doc/saphelp_nw75/7.5.5/en-US/48/95128d94cc73eae10000000a42189b/content.htm.

Secure Storage in the AS ABAP (s.d.). SAP Help Portal / SAP Library. Descreve o funcionamento do Secure Storage em sistemas SAP ABAP, incluindo a utilização de uma chave por omissão antes da inicialização da gestão de chaves através da transacção SECSTORE. URL: https://help.sap.com/doc/saphelp_nw74/7.4.16/en-US/4e/eb2dce10f2398de10000000a42189b/content.htm.

SecurityBridge (2025). *CVE-2025-42957: Critical SAP S/4HANA Vulnerability Exploited in the Wild*. SecurityBridge Research. Relato de exploração real de vulnerabilidade crítica com impacto total no sistema SAP.

Umble, Elisabeth J., Ronald R. Haft e Michael M. Umble (2002). «Enterprise Resource Planning: Implementation Procedures and Critical Success Factors». Em: *European Journal of Operational Research* 146.2, pp. 241–257.

Unit 42 (Palo Alto Networks) (2025). *Malware Deployment via Exploitation of SAP NetWeaver Visual Composer*. Unit 42 Threat Research. Análise de campanha de malware associada à exploração de vulnerabilidade SAP.

User Types in the SAP System (s.d.). SAP Help Portal / SAP Library. Define os diferentes tipos de utilizador no SAP, incluindo Dialog, System e Communication, com as suas respetivas finalidades e características. URL: https://help.sap.com/docs/SAP_NETWEAVER_700/129affcf6c531014b28cae6d2a9cf86f/7aad9040bca2ef4ae10000000a1550b0.html.

Wolf, Patrick e Nick Gehrke (2009). «Continuous Compliance Monitoring in ERP Systems – A Method for Identifying Segregation of Duties Conflicts». Em: *Wirtschaftsinformatik Proceedings 2009*.

Worrell, John L., O. William Gilley e Larry Wallace (2006). «A Risk and Security Analysis Framework for Enterprise Resource Planning Systems». Em: *Information Systems Security* 15.3, pp. 25–34. DOI: 10.1201/1086.1065898X/4628.15.3.20060501/93370.4.

Yusuf, Yahaya, Angappa Gunasekaran e Mike Abthorpe (2004). «Enterprise information systems project implementation: A case study of ERP in Rolls-Royce». Em: *International Journal of Production Economics* 87.

Página intencionalmente deixada em branco.

Anexos

Página intencionalmente deixada em branco.

POLITÉCNICO DE LEIRIA

DECLARAÇÃO DE AUTORIZAÇÃO PARA REALIZAÇÃO DE TESTES DE SEGURANÇA NOS SISTEMAS SAP

1. Identificação das Partes

Entidade Recetora:
Grupo Rolear, empresa com sede em Parque Rolear - Sitio Do, 8001-906 Faro, doravante designada por Entidade Recetora.

Autor do Projeto:
Rúben Mendes, estudante do Mestrado em Cibersegurança e Informática Forense do Instituto Politécnico de Leiria, doravante designado por Autor do Projeto.

2. Enquadramento do Projeto

No âmbito do desenvolvimento do projeto académico integrado no Mestrado em Cibersegurança e Informática Forense do Instituto Politécnico de Leiria, o Autor do Projeto desenvolveu uma aplicação destinada à automatização da análise de segurança em sistemas SAP.

O objetivo desta aplicação consiste em identificar configurações potencialmente inseguras, vulnerabilidades conhecidas e problemas relativamente às boas práticas de segurança recomendadas pela documentação oficial da SAP.

Para validação técnica e experimental da solução desenvolvida, torna-se necessário realizar testes em ambientes SAP disponibilizados pela Entidade Recetora.

3. Objeto da Autorização

A Entidade Recetora autoriza o Autor do Projeto a executar a aplicação desenvolvida nos seguintes sistemas SAP pertencentes à infraestrutura da empresa:

- Sistema SAP de **Formação** (IDES)
- Sistema SAP de **Desenvolvimento** (DEV)
- Sistema SAP de **Qualidade/Testes** (QAS)

Os testes têm como finalidade avaliar a eficácia da aplicação na identificação de configurações de segurança inadequadas, sendo realizados exclusivamente no âmbito académico do projeto.

POLITÉCNICO DE LEIRIA

4. Âmbito das Atividades de Teste

A aplicação realizará verificações automáticas relacionadas com a segurança dos sistemas SAP, incluindo, entre outras:

- análise de contas padrão e verificação de palavras-passe por omissão;
- avaliação de parâmetros de segurança do sistema;
- verificação de clientes padrão ativos;
- análise de ligações RFC (Remote Function Call) e respetivas autorizações;
- verificação das configurações de segurança do RFC Gateway;
- identificação de serviços web potencialmente expostos;
- análise de utilizadores com autorizações administrativas ou críticas.

As verificações realizadas terão caráter exclusivamente de leitura (*read-only*), não sendo efetuadas alterações diretas às configurações ou aos dados dos sistemas SAP sem autorização expressa da Entidade Recetora.

5. Período de Validade

A presente autorização é válida até ao dia **30 de junho de 2026**, período durante o qual poderão ser realizados testes controlados nos ambientes referidos.

Após esta data, qualquer atividade adicional deverá ser objeto de nova autorização formal por parte da Entidade Recetora.

6. Confidencialidade e Proteção de Informação

O Autor do Projeto compromete-se a:

- manter confidencial toda a informação técnica ou organizacional obtida durante a execução dos testes;
- não divulgar dados internos, configurações de sistema, credenciais, arquitetura tecnológica ou qualquer informação considerada sensível pela Entidade Recetora;
- utilizar os resultados obtidos exclusivamente para fins académicos relacionados com o projeto;
- garantir que qualquer informação apresentada no projeto ou em publicações académicas será anonimizada, não permitindo identificar sistemas, utilizadores ou infraestruturas da empresa.

7. Utilização dos Resultados

Os resultados obtidos poderão ser utilizados no relatório final do projeto em eventuais apresentações académicas, desde que:

- não revelem informação sensível da Entidade Recetora;
- não exponham vulnerabilidades específicas de sistemas identificáveis;
- respeitem os princípios de confidencialidade estabelecidos neste documento.

8. Aceitação

Ambas as partes declaram ter tomado conhecimento do conteúdo do presente documento e concordam com os termos e condições nele estabelecidos.

Entidade Recetora (Grupo Rolear)

Nome: António Carrasqueiro

Assinatura: _____

Autor do Projeto

Nome: Rúben Mendes

Assinatura: _____

System Audit Report

System Host:	1(
Client:	0(
Environment:	er
Generated By:	dc
Generated At:	4/
Prepared By:	dc

System Audit Report

Password Management — Overall: HIGH

Parameter	Actual Value	Recommended	Status
login/min_password_lng	6	8	OUT_OF_SPEC
login/min_password_digits	0	1	OUT_OF_SPEC
login/min_password_letters	0	3	OUT_OF_SPEC
login/min_password_lowercase	0	1	OUT_OF_SPEC
login/min_password_uppercase	0	1	OUT_OF_SPEC
login/min_password_specials	0	1	OUT_OF_SPEC
login/password_expiration_time	0	90	OUT_OF_SPEC
login/password_max_idle_produc	<not set>	90	OUT_OF_SPEC
login/password_max_idle_initia	<not set>	14	OUT_OF_SPEC
login/password_history_size	5	5	OK
login/password_change_waittime	1	1	OK
login/min_password_diff	1	1	OK
login/password_charset	1	1	OK
login/password_compliance_to_c	<not set>	1	OUT_OF_SPEC
login/password_change_for_SSO	1	1	OK
login/password_downwards_compa	<not set>	1	OUT_OF_SPEC
login/password_max_new_valid	<not set>	7	OUT_OF_SPEC
login/password_max_reset_valid	<not set>	7	OUT_OF_SPEC

Security Parameters — Overall: HIGH

Parameter	Actual Value	Recommended	Status
login/fails_to_session_end	3	3	OK
login/fails_to_user_lock	5	5	OK
login/failed_user_auto_unlock	0	0	OK
login/disable_multi_gui_login	0	1	OUT_OF_SPEC
login/multi_login_users	<not set>		OK
login/disable_password_logon	0	0	OK
login/password_logon_usergroup	<not set>		OK
login/system_client	001	As	OUT_OF_SPEC
login/no_automatic_user_sap*	0	1	OUT_OF_SPEC
rdisp/max_alt_modes	6	3	OUT_OF_SPEC

System Audit Report

Parameter	Actual Value	Recommended	Status
rdisp/gui_auto_logout	0	18	OUT_OF_SPEC
rdisp/plugin_auto_logout	1800	30	OUT_OF_SPEC
rdisp/tm_max_no	1000	20	OUT_OF_SPEC
auth/no_check_in_some_cases	Y	Y	OK
auth/tcodes_not_checked	<not set>	N	OUT_OF_SPEC
auth/authorization_trace	<not set>	N	OUT_OF_SPEC
auth/object_disabling_active	Y	N	OUT_OF_SPEC
auth/rfc_authority_check	1	1	OK
auth/system_access_check_off	<not set>	0	OUT_OF_SPEC
rsau/enable	0	1	OUT_OF_SPEC
rsau/max_diskspace/local	1000000000	20	OUT_OF_SPEC
rsau/selection_slots	2	2	OK
rsau/local/file	<not set>	1	OUT_OF_SPEC
rsau/user_selection	0	1	OUT_OF_SPEC
snc/enable	0	0	OK
snc/data_protection/use	3	3	OK
snc/data_protection/min	3	2	OUT_OF_SPEC
snc/data_protection/max	3	3	OK
snc/permit_insecure_start	0	0	OK
icm/HTTPS/verify_client	1	1	OK
icm/HTTP/logging	<not set>	1	OUT_OF_SPEC

Standard Accounts (Unlocked Problems) — Overall: HIGH

Client	User	Password Status
000	TMSADM	Password $1Pawd2& is well known
001	TMSADM	Password $1Pawd2& is well known
066	EARLYWATCH	Does not exist.
066	SAPCPIC	Does not exist.
066	TMSADM	Does not exist.
800	DDIC	Password 19920706 well known.
800	SAP*	Does not exist.Logon possible with p/w PASS. See Note 2383

Client	User	Password Status
800	SAPCPIC	Does not exist.
800	TMSADM	Does not exist.
809	DDIC	Password 19920706 well known.
809	SAP*	Password 06071992 well known.
809	SAPCPIC	Does not exist.
809	TMSADM	Does not exist.
810	DDIC	Password 19920706 well known.
810	SAP*	Password 06071992 well known.
810	SAPCPIC	Does not exist.
810	TMSADM	Does not exist.
811	DDIC	Password 19920706 well known.
811	SAP*	Does not exist.Logon possible with p/w PASS. See Note 2383
811	SAPCPIC	Does not exist.
811	TMSADM	Does not exist.
812	DDIC	Password 19920706 well known.
812	SAP*	Password 06071992 well known.
812	SAPCPIC	Does not exist.
812	TMSADM	Does not exist.

Unused Clients — Overall: HIGH

Client	Note
000	(standard SAP client) – consider disabling or removing after review.
001	(standard SAP client) – consider disabling or removing after review.
066	(standard SAP client) – consider disabling or removing after review.

System Audit Report

RFC Connections Audit — Overall: HIGH

RFC Destination	User	Profiles
0M1RP75	TEST	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL, T_AL080006
0M1RP75_DEST	TEST	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL, T_AL080006
FINBASIS_000	IDADMIN	SAP_ALL, SAP_NEW, S_USER_ALL
FINBASIS_800	TCSADM	SAP_ALL, SAP_NEW, S_USER_ALL
FINB_TR_DEST_600	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
FINB_TR_DEST_800	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
FINB_TR_DEST_809	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
FINB_TR_DEST_810	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
FINB_TR_DEST_811	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
FINB_TR_DEST_812	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
SAP_UPGRADE_ORIG_SYSTEM	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL
ZRFC_TEST_ALL	DDIC	SAP_ALL, SAP_NEW, S_RFCACL_ALL, S_USER_ALL

Insecure Web Services — Overall: HIGH

Found & Active
/sap/bc/IDoc_XML
/sap/bc/gui/sap/its/certmap
/sap/bc/srt/IDoc
/sap/bc/bsp/sap/certmap
/sap/bc/gui/sap/its/certreq
/sap/bc/soap
/sap/bc/bsp/sap/certreq
/sap/bc/echo
/sap/bc/webrfc
/sap/bc/xrfc_test
/sap/bc/error
/sap/bc/FormToRfc

Missing or Inactive
None

System Audit Report

Encryption Keys Audit — Overall: HIGH

STILL using Kernel Default (no original entry found)
Active value: F:\usr\sap\DRI\SYS\global\security\data\SecStoreDBKey.pse

System Audit Report

Insecure RFC — Overall: HIGH

Parameter	Status	Message
gw/logging	BAD	ACTION=Ss LOGFILE=gw_log-%y-%m-%d SWITCHTF=day MAXSIZEKB=100 (wanted=1)
gw/reg_info	OK	F:\usr\sap\DRI\D02\data\reginfo.DAT
gw/acl_mode	OK	1
gw/reg_no_conn_info	OK	1
gw/sec_info	OK	F:\usr\sap\DRI\SYS\global\secinfo.DAT
gw/monitor	OK	1

Critical Dialog Users — Overall: HIGH

Text of Criterion	User
Administration: All Rights for Background Jobs	ARCHIVE
Administration: All Rights for Background Jobs	BASIS
Administration: All Rights for Background Jobs	BATIPPS
Administration: All Rights for Background Jobs	BCDEPLOY
Administration: All Rights for Background Jobs	BEZRUKOV
Administration: All Rights for Background Jobs	BLOCHING
Administration: All Rights for Background Jobs	BLUMOEHR
Administration: All Rights for Background Jobs	BOEHMA
Administration: All Rights for Background Jobs	BOLLINGER
Administration: All Rights for Background Jobs	BREINING
Administration: All Rights for Background Jobs	BRENNER
Administration: All Rights for Background Jobs	BRUNSG
Administration: All Rights for Background Jobs	BUCHERT
Administration: All Rights for Background Jobs	BUCHWALD
Administration: All Rights for Background Jobs	CCMS
Administration: All Rights for Background Jobs	CURA
Administration: All Rights for Background Jobs	DAVISCH
Administration: All Rights for Background Jobs	DDIC
Administration: All Rights for Background Jobs	DDICSUPPORT
Administration: All Rights for Background Jobs	DIEHL
Administration: All Rights for Background Jobs	DISANTO
Administration: All Rights for Background Jobs	DKCADM

System Audit Report

Text of Criterion	User
Administration: All Rights for Background Jobs	DROESCHER
Administration: All Rights for Background Jobs	ECC_UPGR
Administration: All Rights for Background Jobs	ENTERPRISE
Administration: All Rights for Background Jobs	EX_DEMO_SUP
Administration: All Rights for Background Jobs	FISCHER
Administration: All Rights for Background Jobs	FISCHERB
Administration: All Rights for Background Jobs	FISCHERK
Administration: All Rights for Background Jobs	FORTMANN
Administration: All Rights for Background Jobs	FRICKE
Administration: All Rights for Background Jobs	GARBRISCH
Administration: All Rights for Background Jobs	GAUTHIER
Administration: All Rights for Background Jobs	GENTNERB
Administration: All Rights for Background Jobs	GIRI
Administration: All Rights for Background Jobs	GODZIEBA
Administration: All Rights for Background Jobs	GONSIOR
Administration: All Rights for Background Jobs	GRAUENHORST
Administration: All Rights for Background Jobs	HABERSACK
Administration: All Rights for Background Jobs	HAMID
Administration: All Rights for Background Jobs	HOCHADEL
Administration: All Rights for Background Jobs	HOEVERMANN
Administration: All Rights for Background Jobs	HORSTA
Administration: All Rights for Background Jobs	HUETT
Administration: All Rights for Background Jobs	ID3TEST
Administration: All Rights for Background Jobs	IDADMIN
Administration: All Rights for Background Jobs	ISM
Administration: All Rights for Background Jobs	KARASU
Administration: All Rights for Background Jobs	KATZSCHNER
Administration: All Rights for Background Jobs	KILIAN
Administration: All Rights for Background Jobs	KIRST
Administration: All Rights for Background Jobs	KOCHS
Administration: All Rights for Background Jobs	KOCHUL
Administration: All Rights for Background Jobs	KRELLJ
Administration: All Rights for Background Jobs	KUEHN
Administration: All Rights for Background Jobs	LANGSTON

System Audit Report

Text of Criterion	User
Administration: All Rights for Background Jobs	LCHAMDONDOG
Administration: All Rights for Background Jobs	LEITSCH
Administration: All Rights for Background Jobs	LEUPOLD
Administration: All Rights for Background Jobs	LORENZ
Administration: All Rights for Background Jobs	LORENZC
Administration: All Rights for Background Jobs	LOTUS
Administration: All Rights for Background Jobs	LUETKEHOFF
Administration: All Rights for Background Jobs	MAASSBERG
Administration: All Rights for Background Jobs	MEERWARTH
Administration: All Rights for Background Jobs	MICHALSKY
Administration: All Rights for Background Jobs	MIZUNO
Administration: All Rights for Background Jobs	MONSNG
Administration: All Rights for Background Jobs	MONUSA
Administration: All Rights for Background Jobs	MUELLERUW
Administration: All Rights for Background Jobs	NATZMER
Administration: All Rights for Background Jobs	NGDCREF3C
Administration: All Rights for Background Jobs	NGDCREF4
Administration: All Rights for Background Jobs	NIEDEROEST
Administration: All Rights for Background Jobs	OBERBOERSCHG
Administration: All Rights for Background Jobs	OERDING
Administration: All Rights for Background Jobs	OLZOG
Administration: All Rights for Background Jobs	PALADM
Administration: All Rights for Background Jobs	PCSETUP
Administration: All Rights for Background Jobs	PEISL
Administration: All Rights for Background Jobs	PETER
Administration: All Rights for Background Jobs	PSS
Administration: All Rights for Background Jobs	RAMOS
Administration: All Rights for Background Jobs	RBAEIM3C
Administration: All Rights for Background Jobs	RBAEIM4
Administration: All Rights for Background Jobs	RBANK3C
Administration: All Rights for Background Jobs	RBANK4
Administration: All Rights for Background Jobs	RBIHANA3C
Administration: All Rights for Background Jobs	RBIHANA4
Administration: All Rights for Background Jobs	RCIO3C

Text of Criterion	User
Administration: All Rights for Background Jobs	RCIO4
Administration: All Rights for Background Jobs	RCLA4
Administration: All Rights for Background Jobs	RCRM3C
Administration: All Rights for Background Jobs	RCRM4
Administration: All Rights for Background Jobs	RCSA3C
Administration: All Rights for Background Jobs	RCSA4
Administration: All Rights for Background Jobs	REINELTD
Administration: All Rights for Background Jobs	RENSEL
Administration: All Rights for Background Jobs	REPM3C
Administration: All Rights for Background Jobs	REPM4
Administration: All Rights for Background Jobs	RFC_CONV
Administration: All Rights for Background Jobs	RFIGRC3C
Administration: All Rights for Background Jobs	RFIGRC4
Administration: All Rights for Background Jobs	RFIORI3C
Administration: All Rights for Background Jobs	RFIORI4
Administration: All Rights for Background Jobs	RHANA3C
Administration: All Rights for Background Jobs	RHANA4
Administration: All Rights for Background Jobs	RHCM3C
Administration: All Rights for Background Jobs	RHCM4
Administration: All Rights for Background Jobs	RINSHC3C
Administration: All Rights for Background Jobs	RINSHC4
Administration: All Rights for Background Jobs	RLOB3C
Administration: All Rights for Background Jobs	RLOB4
Administration: All Rights for Background Jobs	RMANU3C
Administration: All Rights for Background Jobs	RMANU4
Administration: All Rights for Background Jobs	RMOBIL3C
Administration: All Rights for Background Jobs	RMOBIL4
Administration: All Rights for Background Jobs	RPLM3C
Administration: All Rights for Background Jobs	RPLM4
Administration: All Rights for Background Jobs	RPS3C
Administration: All Rights for Background Jobs	RPS4
Administration: All Rights for Background Jobs	RRDS3C
Administration: All Rights for Background Jobs	RRDS4
Administration: All Rights for Background Jobs	RRETAIL3C

System Audit Report

Text of Criterion	User
Administration: All Rights for Background Jobs	RRETAIL4
Administration: All Rights for Background Jobs	RSCM3C
Administration: All Rights for Background Jobs	RSCM4
Administration: All Rights for Background Jobs	RSRM3C
Administration: All Rights for Background Jobs	RSRM4
Administration: All Rights for Background Jobs	RSUSTAIN3C
Administration: All Rights for Background Jobs	RSUSTAIN4
Administration: All Rights for Background Jobs	RUBENADM
Administration: All Rights for Background Jobs	RUTTELC3C
Administration: All Rights for Background Jobs	RUTTELC4
Administration: All Rights for Background Jobs	SAP*
Administration: All Rights for Background Jobs	SAPCPIC
Administration: All Rights for Background Jobs	SAWKENG
Administration: All Rights for Background Jobs	SCHULZET
Administration: All Rights for Background Jobs	SDCAUTO
Administration: All Rights for Background Jobs	SDCMONI
Administration: All Rights for Background Jobs	SELVARAJ
Administration: All Rights for Background Jobs	SE_DEMO_SUP
Administration: All Rights for Background Jobs	SE_MON
Administration: All Rights for Background Jobs	SE_SAPADMIN
Administration: All Rights for Background Jobs	SIMONSON
Administration: All Rights for Background Jobs	SMTMSMD
Administration: All Rights for Background Jobs	SM_ADMIN_SMC
Administration: All Rights for Background Jobs	SM_SMD
Administration: All Rights for Background Jobs	SOLMANM58001
Administration: All Rights for Background Jobs	SOLMANSAM000
Administration: All Rights for Background Jobs	STADEL
Administration: All Rights for Background Jobs	STSADMIN
Administration: All Rights for Background Jobs	SUPPORT
Administration: All Rights for Background Jobs	TCSADM
Administration: All Rights for Background Jobs	TCS_DEMO_2ND
Administration: All Rights for Background Jobs	TCS_DEMO_SUP
Administration: All Rights for Background Jobs	TDC
Administration: All Rights for Background Jobs	TDC_CATT

Text of Criterion	User
Administration: All Rights for Background Jobs	TDC_SAPADMIN
Administration: All Rights for Background Jobs	TEST
Administration: All Rights for Background Jobs	TOEWEU
Administration: All Rights for Background Jobs	TRANS
Administration: All Rights for Background Jobs	U4UMGMTPSS
Administration: All Rights for Background Jobs	UPGRADE
Administration: All Rights for Background Jobs	VEITSHANSC
Administration: All Rights for Background Jobs	VERNAQ
Administration: All Rights for Background Jobs	VERNITSKAJAK
Administration: All Rights for Background Jobs	VP_SAPADMIN
Administration: All Rights for Background Jobs	WATKINSG
Administration: All Rights for Background Jobs	WEISSAN
Administration: All Rights for Background Jobs	WF-BATCH
Administration: All Rights for Background Jobs	WORSCH
Administration: Release Background Jobs	BASIS
Administration: Release Background Jobs	BATIPPS
Administration: Release Background Jobs	BCDEPLOY
Administration: Release Background Jobs	BEZRUKOV
Administration: Release Background Jobs	BLOCHING
Administration: Release Background Jobs	BLUMOEHR
Administration: Release Background Jobs	BOEHMA
Administration: Release Background Jobs	BOLLINGER
Administration: Release Background Jobs	BREINING
Administration: Release Background Jobs	BRENNER
Administration: Release Background Jobs	BRUNSG
Administration: Release Background Jobs	BUCHERT
Administration: Release Background Jobs	BUCHWALD
Administration: Release Background Jobs	CCMS
Administration: Release Background Jobs	COMPARE
Administration: Release Background Jobs	CURA
Administration: Release Background Jobs	DAVISCH
Administration: Release Background Jobs	DDIC
Administration: Release Background Jobs	DDICSUPPORT
Administration: Release Background Jobs	DIEHL

System Audit Report

Text of Criterion	User
Administration: Release Background Jobs	DISANTO
Administration: Release Background Jobs	DKCADM
Administration: Release Background Jobs	DROESCHER
Administration: Release Background Jobs	ECC_UPGR
Administration: Release Background Jobs	ENTERPRISE
Administration: Release Background Jobs	EX_DEMO_SUP
Administration: Release Background Jobs	FISCHER
Administration: Release Background Jobs	FISCHERB
Administration: Release Background Jobs	FISCHERK
Administration: Release Background Jobs	FORTMANN
Administration: Release Background Jobs	FRICKE
Administration: Release Background Jobs	GARBRISCH
Administration: Release Background Jobs	GAUTHIER
Administration: Release Background Jobs	GENTNERB
Administration: Release Background Jobs	GIRI
Administration: Release Background Jobs	GODZIEBA
Administration: Release Background Jobs	GONSIOR
Administration: Release Background Jobs	GRAUENHORST
Administration: Release Background Jobs	HABERSACK
Administration: Release Background Jobs	HAMID
Administration: Release Background Jobs	HOCHADEL
Administration: Release Background Jobs	HOEVERMANN
Administration: Release Background Jobs	HORSTA
Administration: Release Background Jobs	HUETT
Administration: Release Background Jobs	ID3TEST
Administration: Release Background Jobs	IDADMIN
Administration: Release Background Jobs	ISM
Administration: Release Background Jobs	KARASU
Administration: Release Background Jobs	KATZSCHNER
Administration: Release Background Jobs	KILIAN
Administration: Release Background Jobs	KIRST
Administration: Release Background Jobs	KOCHS
Administration: Release Background Jobs	KOCHUL
Administration: Release Background Jobs	KRELLJ

System Audit Report

Text of Criterion	User
Administration: Release Background Jobs	KUEHN
Administration: Release Background Jobs	LANGSTON
Administration: Release Background Jobs	LCHAMDONDOG
Administration: Release Background Jobs	LEITSCH
Administration: Release Background Jobs	LEUPOLD
Administration: Release Background Jobs	LORENZ
Administration: Release Background Jobs	LORENZC
Administration: Release Background Jobs	LOTUS
Administration: Release Background Jobs	LUETKEHOFF
Administration: Release Background Jobs	MAASSBERG
Administration: Release Background Jobs	MEERWARTH
Administration: Release Background Jobs	MICHALSKY
Administration: Release Background Jobs	MIZUNO
Administration: Release Background Jobs	MONSNG
Administration: Release Background Jobs	MONUSA
Administration: Release Background Jobs	MUELLERUW
Administration: Release Background Jobs	NATZMER
Administration: Release Background Jobs	NGDCREF3C
Administration: Release Background Jobs	NGDCREF4
Administration: Release Background Jobs	NIEDEROEST
Administration: Release Background Jobs	OBERBOERSCHG
Administration: Release Background Jobs	OERDING
Administration: Release Background Jobs	OLZOG
Administration: Release Background Jobs	PALADM
Administration: Release Background Jobs	PCSETUP
Administration: Release Background Jobs	PEISL
Administration: Release Background Jobs	PETER
Administration: Release Background Jobs	PSS
Administration: Release Background Jobs	RAMOS
Administration: Release Background Jobs	RBAEIM3C
Administration: Release Background Jobs	RBAEIM4
Administration: Release Background Jobs	RBANK3C
Administration: Release Background Jobs	RBANK4
Administration: Release Background Jobs	RBIHANA3C

Text of Criterion	User
Administration: Release Background Jobs	RBIHANA4
Administration: Release Background Jobs	RCIO3C
Administration: Release Background Jobs	RCIO4
Administration: Release Background Jobs	RCLA4
Administration: Release Background Jobs	RCRM3C
Administration: Release Background Jobs	RCRM4
Administration: Release Background Jobs	RCSA3C
Administration: Release Background Jobs	RCSA4
Administration: Release Background Jobs	REINELTD
Administration: Release Background Jobs	RENSEL
Administration: Release Background Jobs	REPM3C
Administration: Release Background Jobs	REPM4
Administration: Release Background Jobs	RFC_CONV
Administration: Release Background Jobs	RFIGRC3C
Administration: Release Background Jobs	RFIGRC4
Administration: Release Background Jobs	RFIORI3C
Administration: Release Background Jobs	RFIORI4
Administration: Release Background Jobs	RHANA3C
Administration: Release Background Jobs	RHANA4
Administration: Release Background Jobs	RHCM3C
Administration: Release Background Jobs	RHCM4
Administration: Release Background Jobs	RINSHC3C
Administration: Release Background Jobs	RINSHC4
Administration: Release Background Jobs	RLOB3C
Administration: Release Background Jobs	RLOB4
Administration: Release Background Jobs	RMANU3C
Administration: Release Background Jobs	RMANU4
Administration: Release Background Jobs	RMOBIL3C
Administration: Release Background Jobs	RMOBIL4
Administration: Release Background Jobs	RPLM3C
Administration: Release Background Jobs	RPLM4
Administration: Release Background Jobs	RPS3C
Administration: Release Background Jobs	RPS4
Administration: Release Background Jobs	RRDS3C

Text of Criterion	User
Administration: Release Background Jobs	RRDS4
Administration: Release Background Jobs	RRETAIL3C
Administration: Release Background Jobs	RRETAIL4
Administration: Release Background Jobs	RSCM3C
Administration: Release Background Jobs	RSCM4
Administration: Release Background Jobs	RSRM3C
Administration: Release Background Jobs	RSRM4
Administration: Release Background Jobs	RSUSTAIN3C
Administration: Release Background Jobs	RSUSTAIN4
Administration: Release Background Jobs	RUBENADM
Administration: Release Background Jobs	RUTTELC3C
Administration: Release Background Jobs	RUTTELC4
Administration: Release Background Jobs	SAP*
Administration: Release Background Jobs	SAPCPIC
Administration: Release Background Jobs	SAP_WSRT
Administration: Release Background Jobs	SAWKENG
Administration: Release Background Jobs	SCHULZET
Administration: Release Background Jobs	SDCAUTO
Administration: Release Background Jobs	SDCMONI
Administration: Release Background Jobs	SELVARAJ
Administration: Release Background Jobs	SE_DEMO_SUP
Administration: Release Background Jobs	SE_MON
Administration: Release Background Jobs	SE_SAPADMIN
Administration: Release Background Jobs	SIMONSON
Administration: Release Background Jobs	SMTMSMD
Administration: Release Background Jobs	SM_ADMIN_SMC
Administration: Release Background Jobs	SM_SMD
Administration: Release Background Jobs	SOLMANM58001
Administration: Release Background Jobs	SOLMANSAM000
Administration: Release Background Jobs	STADEL
Administration: Release Background Jobs	STSADMIN
Administration: Release Background Jobs	SUPPORT
Administration: Release Background Jobs	TCSADM
Administration: Release Background Jobs	TCS_DEMO_2ND

Text of Criterion	User
Administration: Release Background Jobs	TCS_DEMO_SUP
Administration: Release Background Jobs	TDC
Administration: Release Background Jobs	TDC_CATT
Administration: Release Background Jobs	TDC_SAPADMIN
Administration: Release Background Jobs	TEST
Administration: Release Background Jobs	TOEWEU
Administration: Release Background Jobs	TRANS
Administration: Release Background Jobs	U4UMGMTPSS
Administration: Release Background Jobs	UPGRADE
Administration: Release Background Jobs	VEITSHANSC
Administration: Release Background Jobs	VERNAQ
Administration: Release Background Jobs	VERNITSKAJAK
Administration: Release Background Jobs	VP_SAPADMIN
Administration: Release Background Jobs	WATKINSG
Administration: Release Background Jobs	WEISSAN
Administration: Release Background Jobs	WF-BATCH
Administration: Release Background Jobs	WORSCH
Administration: Start Background Jobs with Any User	BASIS
Administration: Start Background Jobs with Any User	BATIPPS
Administration: Start Background Jobs with Any User	BCDEPLOY
Administration: Start Background Jobs with Any User	BEZRUKOV
Administration: Start Background Jobs with Any User	BLOCHING
Administration: Start Background Jobs with Any User	BLUMOEHR
Administration: Start Background Jobs with Any User	BOEHMA
Administration: Start Background Jobs with Any User	BOLLINGER
Administration: Start Background Jobs with Any User	BREINING
Administration: Start Background Jobs with Any User	BRENNER
Administration: Start Background Jobs with Any User	BRUNSG
Administration: Start Background Jobs with Any User	BUCHERT
Administration: Start Background Jobs with Any User	BUCHWALD
Administration: Start Background Jobs with Any User	CCMS
Administration: Start Background Jobs with Any User	CURA
Administration: Start Background Jobs with Any User	DAVISCH
Administration: Start Background Jobs with Any User	DDIC

Text of Criterion	User
Administration: Start Background Jobs with Any User	DDICSUPPORT
Administration: Start Background Jobs with Any User	DIEHL
Administration: Start Background Jobs with Any User	DISANTO
Administration: Start Background Jobs with Any User	DKCADM
Administration: Start Background Jobs with Any User	DROESCHER
Administration: Start Background Jobs with Any User	ECC_UPGR
Administration: Start Background Jobs with Any User	ENTERPRISE
Administration: Start Background Jobs with Any User	EX_DEMO_SUP
Administration: Start Background Jobs with Any User	FISCHER
Administration: Start Background Jobs with Any User	FISCHERB
Administration: Start Background Jobs with Any User	FISCHERK
Administration: Start Background Jobs with Any User	FORTMANN
Administration: Start Background Jobs with Any User	FRICKE
Administration: Start Background Jobs with Any User	GARBRISCH
Administration: Start Background Jobs with Any User	GAUTHIER
Administration: Start Background Jobs with Any User	GENTNERB
Administration: Start Background Jobs with Any User	GIRI
Administration: Start Background Jobs with Any User	GODZIEBA
Administration: Start Background Jobs with Any User	GONSIOR
Administration: Start Background Jobs with Any User	GRAUENHORST
Administration: Start Background Jobs with Any User	HABERSACK
Administration: Start Background Jobs with Any User	HAMID
Administration: Start Background Jobs with Any User	HOCHADEL
Administration: Start Background Jobs with Any User	HOEVERMANN
Administration: Start Background Jobs with Any User	HORSTA
Administration: Start Background Jobs with Any User	HUETT
Administration: Start Background Jobs with Any User	ID3TEST
Administration: Start Background Jobs with Any User	IDADMIN
Administration: Start Background Jobs with Any User	ISM
Administration: Start Background Jobs with Any User	KARASU
Administration: Start Background Jobs with Any User	KATZSCHNER
Administration: Start Background Jobs with Any User	KILIAN
Administration: Start Background Jobs with Any User	KIRST
Administration: Start Background Jobs with Any User	KOCHS

System Audit Report

Text of Criterion	User
Administration: Start Background Jobs with Any User	KOCHUL
Administration: Start Background Jobs with Any User	KRELLJ
Administration: Start Background Jobs with Any User	KUEHN
Administration: Start Background Jobs with Any User	LANGSTON
Administration: Start Background Jobs with Any User	LCHAMDONDOG
Administration: Start Background Jobs with Any User	LEITSCH
Administration: Start Background Jobs with Any User	LEUPOLD
Administration: Start Background Jobs with Any User	LORENZ
Administration: Start Background Jobs with Any User	LORENZC
Administration: Start Background Jobs with Any User	LOTUS
Administration: Start Background Jobs with Any User	LUETKEHOFF
Administration: Start Background Jobs with Any User	MAASSBERG
Administration: Start Background Jobs with Any User	MEERWARTH
Administration: Start Background Jobs with Any User	MICHALSKY
Administration: Start Background Jobs with Any User	MIZUNO
Administration: Start Background Jobs with Any User	MONSNG
Administration: Start Background Jobs with Any User	MONUSA
Administration: Start Background Jobs with Any User	MUELLERUW
Administration: Start Background Jobs with Any User	NATZMER
Administration: Start Background Jobs with Any User	NGDCREF4
Administration: Start Background Jobs with Any User	NIEDEROEST
Administration: Start Background Jobs with Any User	OBERBOERSCHG
Administration: Start Background Jobs with Any User	OERDING
Administration: Start Background Jobs with Any User	OLZOG
Administration: Start Background Jobs with Any User	PALADM
Administration: Start Background Jobs with Any User	PCSETUP
Administration: Start Background Jobs with Any User	PEISL
Administration: Start Background Jobs with Any User	PETER
Administration: Start Background Jobs with Any User	PSS
Administration: Start Background Jobs with Any User	RAMOS
Administration: Start Background Jobs with Any User	RBAEIM4
Administration: Start Background Jobs with Any User	RBANK4
Administration: Start Background Jobs with Any User	RBIHANA4
Administration: Start Background Jobs with Any User	RCIO4

Text of Criterion	User
Administration: Start Background Jobs with Any User	RCLA4
Administration: Start Background Jobs with Any User	RCRM4
Administration: Start Background Jobs with Any User	RCSA4
Administration: Start Background Jobs with Any User	REINELTD
Administration: Start Background Jobs with Any User	RENSEL
Administration: Start Background Jobs with Any User	REPM4
Administration: Start Background Jobs with Any User	RFC_CONV
Administration: Start Background Jobs with Any User	RFIGRC4
Administration: Start Background Jobs with Any User	RFIORI4
Administration: Start Background Jobs with Any User	RHANA4
Administration: Start Background Jobs with Any User	RHCM4
Administration: Start Background Jobs with Any User	RINSHC4
Administration: Start Background Jobs with Any User	RLOB4
Administration: Start Background Jobs with Any User	RMANU4
Administration: Start Background Jobs with Any User	RMOBIL4
Administration: Start Background Jobs with Any User	RPLM4
Administration: Start Background Jobs with Any User	RPS4
Administration: Start Background Jobs with Any User	RRDS4
Administration: Start Background Jobs with Any User	RRETAIL4
Administration: Start Background Jobs with Any User	RSCM4
Administration: Start Background Jobs with Any User	RSRM4
Administration: Start Background Jobs with Any User	RSUSTAIN4
Administration: Start Background Jobs with Any User	RUBENADM
Administration: Start Background Jobs with Any User	RUTTELC4
Administration: Start Background Jobs with Any User	SAP*
Administration: Start Background Jobs with Any User	SAPCPIC
Administration: Start Background Jobs with Any User	SAWKENG
Administration: Start Background Jobs with Any User	SCHULZET
Administration: Start Background Jobs with Any User	SDCAUTO
Administration: Start Background Jobs with Any User	SDCMONI
Administration: Start Background Jobs with Any User	SELVARAJ
Administration: Start Background Jobs with Any User	SE_DEMO_SUP
Administration: Start Background Jobs with Any User	SE_SAPADMIN
Administration: Start Background Jobs with Any User	SIMONSON

Text of Criterion	User
Administration: Start Background Jobs with Any User	SM_ADMIN_SMC
Administration: Start Background Jobs with Any User	STADEL
Administration: Start Background Jobs with Any User	STSADMIN
Administration: Start Background Jobs with Any User	SUPPORT
Administration: Start Background Jobs with Any User	TCSADM
Administration: Start Background Jobs with Any User	TCS_DEMO_2ND
Administration: Start Background Jobs with Any User	TCS_DEMO_SUP
Administration: Start Background Jobs with Any User	TDC
Administration: Start Background Jobs with Any User	TDC_CATT
Administration: Start Background Jobs with Any User	TDC_SAPADMIN
Administration: Start Background Jobs with Any User	TEST
Administration: Start Background Jobs with Any User	TOEWEU
Administration: Start Background Jobs with Any User	TRANS
Administration: Start Background Jobs with Any User	U4UMGMTPSS
Administration: Start Background Jobs with Any User	UPGRADE
Administration: Start Background Jobs with Any User	VEITSHANSC
Administration: Start Background Jobs with Any User	VERNAQ
Administration: Start Background Jobs with Any User	VERNITSKAJAK
Administration: Start Background Jobs with Any User	VP_SAPADMIN
Administration: Start Background Jobs with Any User	WATKINSG
Administration: Start Background Jobs with Any User	WEISSAN
Administration: Start Background Jobs with Any User	WF-BATCH
Administration: Start Background Jobs with Any User	WORSCH
Use Background Jobs	BASIS
Use Background Jobs	BATIPPS
Use Background Jobs	BCDEPLOY
Use Background Jobs	BEZRUKOV
Use Background Jobs	BLOCHING
Use Background Jobs	BLUMOEHR
Use Background Jobs	BOEHMA
Use Background Jobs	BOLLINGER
Use Background Jobs	BREINING
Use Background Jobs	BRENNER
Use Background Jobs	BRUNSG

Text of Criterion	User
Use Background Jobs	BUCHERT
Use Background Jobs	BUCHWALD
Use Background Jobs	CCMS
Use Background Jobs	CURA
Use Background Jobs	DAVISCH
Use Background Jobs	DDIC
Use Background Jobs	DDICSUPPORT
Use Background Jobs	DIEHL
Use Background Jobs	DISANTO
Use Background Jobs	DKCADM
Use Background Jobs	DROESCHER
Use Background Jobs	ECC_UPGR
Use Background Jobs	ENTERPRISE
Use Background Jobs	EX_DEMO_SUP
Use Background Jobs	FISCHER
Use Background Jobs	FISCHERB
Use Background Jobs	FISCHERK
Use Background Jobs	FORTMANN
Use Background Jobs	FRICKE
Use Background Jobs	GARBRISCH
Use Background Jobs	GAUTHIER
Use Background Jobs	GENTNERB
Use Background Jobs	GIRI
Use Background Jobs	GODZIEBA
Use Background Jobs	GONSIOR
Use Background Jobs	GRAUENHORST
Use Background Jobs	HABERSACK
Use Background Jobs	HAMID
Use Background Jobs	HOCHADEL
Use Background Jobs	HOEVERMANN
Use Background Jobs	HORSTA
Use Background Jobs	HUETT
Use Background Jobs	ID3TEST
Use Background Jobs	IDADMIN

System Audit Report

Text of Criterion	User
Use Background Jobs	ISM
Use Background Jobs	KARASU
Use Background Jobs	KATZSCHNER
Use Background Jobs	KILIAN
Use Background Jobs	KIRST
Use Background Jobs	KOCHS
Use Background Jobs	KOCHUL
Use Background Jobs	KRELLJ
Use Background Jobs	KUEHN
Use Background Jobs	LANGSTON
Use Background Jobs	LCHAMDONDOG
Use Background Jobs	LEITSCH
Use Background Jobs	LEUPOLD
Use Background Jobs	LORENZ
Use Background Jobs	LORENZC
Use Background Jobs	LOTUS
Use Background Jobs	LUETKEHOFF
Use Background Jobs	MAASSBERG
Use Background Jobs	MEERWARTH
Use Background Jobs	MICHALSKY
Use Background Jobs	MIZUNO
Use Background Jobs	MONSNG
Use Background Jobs	MONUSA
Use Background Jobs	MUELLERUW
Use Background Jobs	NATZMER
Use Background Jobs	NGDCREF4
Use Background Jobs	NIEDEROEST
Use Background Jobs	OBERBOERSCHG
Use Background Jobs	OERDING
Use Background Jobs	OLZOG
Use Background Jobs	PALADM
Use Background Jobs	PCSETUP
Use Background Jobs	PEISL
Use Background Jobs	PETER

Text of Criterion	User
Use Background Jobs	PSS
Use Background Jobs	RAMOS
Use Background Jobs	RBAEIM4
Use Background Jobs	RBANK4
Use Background Jobs	RBIHANA4
Use Background Jobs	RCIO4
Use Background Jobs	RCLA4
Use Background Jobs	RCRM4
Use Background Jobs	RCSA4
Use Background Jobs	REINELTD
Use Background Jobs	RENSEL
Use Background Jobs	REPM4
Use Background Jobs	RFC_CONV
Use Background Jobs	RFIGRC4
Use Background Jobs	RFIORI4
Use Background Jobs	RHANA4
Use Background Jobs	RHCM4
Use Background Jobs	RINSHC4
Use Background Jobs	RLOB4
Use Background Jobs	RMANU4
Use Background Jobs	RMOBIL4
Use Background Jobs	RPLM4
Use Background Jobs	RPS4
Use Background Jobs	RRDS4
Use Background Jobs	RRETAIL4
Use Background Jobs	RSCM4
Use Background Jobs	RSRM4
Use Background Jobs	RSUSTAIN4
Use Background Jobs	RUBENADM
Use Background Jobs	RUTTELC4
Use Background Jobs	SAP*
Use Background Jobs	SAPCPIC
Use Background Jobs	SAWKENG
Use Background Jobs	SCHULZET

System Audit Report

Text of Criterion	User
Use Background Jobs	SDCAUTO
Use Background Jobs	SDCMONI
Use Background Jobs	SELVARAJ
Use Background Jobs	SE_DEMO_SUP
Use Background Jobs	SE_SAPADMIN
Use Background Jobs	SIMONSON
Use Background Jobs	SMTMSMD
Use Background Jobs	SM_ADMIN_SMC
Use Background Jobs	STADEL
Use Background Jobs	STSADMIN
Use Background Jobs	SUPPORT
Use Background Jobs	TCSADM
Use Background Jobs	TCS_DEMO_2ND
Use Background Jobs	TCS_DEMO_SUP
Use Background Jobs	TDC
Use Background Jobs	TDC_CATT
Use Background Jobs	TDC_SAPADMIN
Use Background Jobs	TEST
Use Background Jobs	TOEWEU
Use Background Jobs	TRANS
Use Background Jobs	U4UMGMTPSS
Use Background Jobs	UPGRADE
Use Background Jobs	VEITSHANSC
Use Background Jobs	VERNAQ
Use Background Jobs	VERNITSKAJAK
Use Background Jobs	VP_SAPADMIN
Use Background Jobs	WATKINSG
Use Background Jobs	WEISSAN
Use Background Jobs	WF-BATCH
Use Background Jobs	WORSCH
Adminsitration: Network, Processes, Update Admin., and so on	BASIS
Adminsitration: Network, Processes, Update Admin., and so on	BATIPPS
Adminsitration: Network, Processes, Update Admin., and so on	BCDEPLOY
Adminsitration: Network, Processes, Update Admin., and so on	BEZRUKOV

System Audit Report

Text of Criterion	User
Adminsitration: Network, Processes, Update Admin., and so on	BLOCHING
Adminsitration: Network, Processes, Update Admin., and so on	BLUMOEHR
Adminsitration: Network, Processes, Update Admin., and so on	BOEHMA
Adminsitration: Network, Processes, Update Admin., and so on	BOLLINGER
Adminsitration: Network, Processes, Update Admin., and so on	BREINING
Adminsitration: Network, Processes, Update Admin., and so on	BRENNER
Adminsitration: Network, Processes, Update Admin., and so on	BRUNSG
Adminsitration: Network, Processes, Update Admin., and so on	BUCHERT
Adminsitration: Network, Processes, Update Admin., and so on	BUCHWALD
Adminsitration: Network, Processes, Update Admin., and so on	CCMS
Adminsitration: Network, Processes, Update Admin., and so on	CURA
Adminsitration: Network, Processes, Update Admin., and so on	DAVISCH
Adminsitration: Network, Processes, Update Admin., and so on	DDIC
Adminsitration: Network, Processes, Update Admin., and so on	DDICSUPPORT
Adminsitration: Network, Processes, Update Admin., and so on	DIEHL
Adminsitration: Network, Processes, Update Admin., and so on	DISANTO
Adminsitration: Network, Processes, Update Admin., and so on	DKCADM
Adminsitration: Network, Processes, Update Admin., and so on	DROESCHER
Adminsitration: Network, Processes, Update Admin., and so on	ECC_UPGR
Adminsitration: Network, Processes, Update Admin., and so on	ENTERPRISE
Adminsitration: Network, Processes, Update Admin., and so on	EX_DEMO_SUP
Adminsitration: Network, Processes, Update Admin., and so on	FINBTR@ID3
Adminsitration: Network, Processes, Update Admin., and so on	FISCHER
Adminsitration: Network, Processes, Update Admin., and so on	FISCHERB
Adminsitration: Network, Processes, Update Admin., and so on	FISCHERK
Adminsitration: Network, Processes, Update Admin., and so on	FORTMANN
Adminsitration: Network, Processes, Update Admin., and so on	FRICKE
Adminsitration: Network, Processes, Update Admin., and so on	GARBRISCH
Adminsitration: Network, Processes, Update Admin., and so on	GAUTHIER
Adminsitration: Network, Processes, Update Admin., and so on	GENTNERB
Adminsitration: Network, Processes, Update Admin., and so on	GIRI
Adminsitration: Network, Processes, Update Admin., and so on	GODZIEBA
Adminsitration: Network, Processes, Update Admin., and so on	GONSIOR
Adminsitration: Network, Processes, Update Admin., and so on	GRAUENHORST

System Audit Report

Text of Criterion	User
Adminsitration: Network, Processes, Update Admin., and so on	HABERSACK
Adminsitration: Network, Processes, Update Admin., and so on	HAMID
Adminsitration: Network, Processes, Update Admin., and so on	HOCHADEL
Adminsitration: Network, Processes, Update Admin., and so on	HOEVERMANN
Adminsitration: Network, Processes, Update Admin., and so on	HORSTA
Adminsitration: Network, Processes, Update Admin., and so on	HUETT
Adminsitration: Network, Processes, Update Admin., and so on	ID3TEST
Adminsitration: Network, Processes, Update Admin., and so on	IDADMIN
Adminsitration: Network, Processes, Update Admin., and so on	ISM
Adminsitration: Network, Processes, Update Admin., and so on	KARASU
Adminsitration: Network, Processes, Update Admin., and so on	KATZSCHNER
Adminsitration: Network, Processes, Update Admin., and so on	KILIAN
Adminsitration: Network, Processes, Update Admin., and so on	KIRST
Adminsitration: Network, Processes, Update Admin., and so on	KOCHS
Adminsitration: Network, Processes, Update Admin., and so on	KOCHUL
Adminsitration: Network, Processes, Update Admin., and so on	KRELLJ
Adminsitration: Network, Processes, Update Admin., and so on	KUEHN
Adminsitration: Network, Processes, Update Admin., and so on	LANGSTON
Adminsitration: Network, Processes, Update Admin., and so on	LCHAMDONDOG
Adminsitration: Network, Processes, Update Admin., and so on	LEITSCH
Adminsitration: Network, Processes, Update Admin., and so on	LEUPOLD
Adminsitration: Network, Processes, Update Admin., and so on	LORENZ
Adminsitration: Network, Processes, Update Admin., and so on	LORENZC
Adminsitration: Network, Processes, Update Admin., and so on	LOTUS
Adminsitration: Network, Processes, Update Admin., and so on	LUETKEHOFF
Adminsitration: Network, Processes, Update Admin., and so on	MAASSBERG
Adminsitration: Network, Processes, Update Admin., and so on	MEERWARTH
Adminsitration: Network, Processes, Update Admin., and so on	MICHALSKY
Adminsitration: Network, Processes, Update Admin., and so on	MIZUNO
Adminsitration: Network, Processes, Update Admin., and so on	MONSNG
Adminsitration: Network, Processes, Update Admin., and so on	MONUSA
Adminsitration: Network, Processes, Update Admin., and so on	MUELLERUW
Adminsitration: Network, Processes, Update Admin., and so on	NATZMER
Adminsitration: Network, Processes, Update Admin., and so on	NGDCREF4

System Audit Report

Text of Criterion	User
Adminsitration: Network, Processes, Update Admin., and so on	NIEDEROEST
Adminsitration: Network, Processes, Update Admin., and so on	OBERBOERSCHG
Adminsitration: Network, Processes, Update Admin., and so on	OERDING
Adminsitration: Network, Processes, Update Admin., and so on	OLZOG
Adminsitration: Network, Processes, Update Admin., and so on	PALADM
Adminsitration: Network, Processes, Update Admin., and so on	PCSETUP
Adminsitration: Network, Processes, Update Admin., and so on	PEISL
Adminsitration: Network, Processes, Update Admin., and so on	PETER
Adminsitration: Network, Processes, Update Admin., and so on	PSS
Adminsitration: Network, Processes, Update Admin., and so on	RAMOS
Adminsitration: Network, Processes, Update Admin., and so on	RBAEIM4
Adminsitration: Network, Processes, Update Admin., and so on	RBANK4
Adminsitration: Network, Processes, Update Admin., and so on	RBIHANA4
Adminsitration: Network, Processes, Update Admin., and so on	RCIO4
Adminsitration: Network, Processes, Update Admin., and so on	RCLA4
Adminsitration: Network, Processes, Update Admin., and so on	RCRM4
Adminsitration: Network, Processes, Update Admin., and so on	RCSA4
Adminsitration: Network, Processes, Update Admin., and so on	REINELTD
Adminsitration: Network, Processes, Update Admin., and so on	RENSEL
Adminsitration: Network, Processes, Update Admin., and so on	REPM4
Adminsitration: Network, Processes, Update Admin., and so on	RFC_CONV
Adminsitration: Network, Processes, Update Admin., and so on	RFIGRC4
Adminsitration: Network, Processes, Update Admin., and so on	RFIORI4
Adminsitration: Network, Processes, Update Admin., and so on	RHANA4
Adminsitration: Network, Processes, Update Admin., and so on	RHCM4
Adminsitration: Network, Processes, Update Admin., and so on	RINSHC4
Adminsitration: Network, Processes, Update Admin., and so on	RLOB4
Adminsitration: Network, Processes, Update Admin., and so on	RMANU4
Adminsitration: Network, Processes, Update Admin., and so on	RMOBIL4
Adminsitration: Network, Processes, Update Admin., and so on	RPLM4
Adminsitration: Network, Processes, Update Admin., and so on	RPS4
Adminsitration: Network, Processes, Update Admin., and so on	RRDS4
Adminsitration: Network, Processes, Update Admin., and so on	RRETAIL4
Adminsitration: Network, Processes, Update Admin., and so on	RSCM4

Text of Criterion	User
Adminsitration: Network, Processes, Update Admin., and so on	RSRM4
Adminsitration: Network, Processes, Update Admin., and so on	RSUSTAIN4
Adminsitration: Network, Processes, Update Admin., and so on	RUBENADM
Adminsitration: Network, Processes, Update Admin., and so on	RUTTELC4
Adminsitration: Network, Processes, Update Admin., and so on	SAP*
Adminsitration: Network, Processes, Update Admin., and so on	SAPCPIC
Adminsitration: Network, Processes, Update Admin., and so on	SAWKENG
Adminsitration: Network, Processes, Update Admin., and so on	SCHULZET
Adminsitration: Network, Processes, Update Admin., and so on	SDCAUTO
Adminsitration: Network, Processes, Update Admin., and so on	SDCMONI
Adminsitration: Network, Processes, Update Admin., and so on	SELVARAJ
Adminsitration: Network, Processes, Update Admin., and so on	SE_DEMO_SUP
Adminsitration: Network, Processes, Update Admin., and so on	SE_SAPADMIN
Adminsitration: Network, Processes, Update Admin., and so on	SIMONSON
Adminsitration: Network, Processes, Update Admin., and so on	SMTMSMD
Adminsitration: Network, Processes, Update Admin., and so on	SM_ADMIN_SMC
Adminsitration: Network, Processes, Update Admin., and so on	SM_SMC
Adminsitration: Network, Processes, Update Admin., and so on	SM_SMD
Adminsitration: Network, Processes, Update Admin., and so on	SOLMANM58001
Adminsitration: Network, Processes, Update Admin., and so on	SOLMANSAM000
Adminsitration: Network, Processes, Update Admin., and so on	STADEL
Adminsitration: Network, Processes, Update Admin., and so on	STSADMIN
Adminsitration: Network, Processes, Update Admin., and so on	SUPPORT
Adminsitration: Network, Processes, Update Admin., and so on	TCSADM
Adminsitration: Network, Processes, Update Admin., and so on	TCS_DEMO_2ND
Adminsitration: Network, Processes, Update Admin., and so on	TCS_DEMO_SUP
Adminsitration: Network, Processes, Update Admin., and so on	TDC
Adminsitration: Network, Processes, Update Admin., and so on	TDC_CATT
Adminsitration: Network, Processes, Update Admin., and so on	TDC_SAPADMIN
Adminsitration: Network, Processes, Update Admin., and so on	TEST
Adminsitration: Network, Processes, Update Admin., and so on	TOEWEU
Adminsitration: Network, Processes, Update Admin., and so on	TRANS
Adminsitration: Network, Processes, Update Admin., and so on	U4UMGMTPSS
Adminsitration: Network, Processes, Update Admin., and so on	UPGRADE

Text of Criterion	User
Adminsitration: Network, Processes, Update Admin., and so on	VEITSHANSC
Adminsitration: Network, Processes, Update Admin., and so on	VERNAQ
Adminsitration: Network, Processes, Update Admin., and so on	VERNITSKAJAK
Adminsitration: Network, Processes, Update Admin., and so on	VP_SAPADMIN
Adminsitration: Network, Processes, Update Admin., and so on	WATKINSG
Adminsitration: Network, Processes, Update Admin., and so on	WEISSAN
Adminsitration: Network, Processes, Update Admin., and so on	WF-BATCH
Adminsitration: Network, Processes, Update Admin., and so on	WORSCH
Execute Logical Operating System Commands	BASIS
Execute Logical Operating System Commands	BATIPPS
Execute Logical Operating System Commands	BCDEPLOY
Execute Logical Operating System Commands	BEZRUKOV
Execute Logical Operating System Commands	BLOCHING
Execute Logical Operating System Commands	BLUMOEHR
Execute Logical Operating System Commands	BOEHMA
Execute Logical Operating System Commands	BOLLINGER
Execute Logical Operating System Commands	BREINING
Execute Logical Operating System Commands	BRENNER
Execute Logical Operating System Commands	BRUNSG
Execute Logical Operating System Commands	BUCHERT
Execute Logical Operating System Commands	BUCHWALD
Execute Logical Operating System Commands	CCMS
Execute Logical Operating System Commands	CURA
Execute Logical Operating System Commands	DAVISCH
Execute Logical Operating System Commands	DDIC
Execute Logical Operating System Commands	DDICSUPPORT
Execute Logical Operating System Commands	DIEHL
Execute Logical Operating System Commands	DISANTO
Execute Logical Operating System Commands	DKCADM
Execute Logical Operating System Commands	DROESCHER
Execute Logical Operating System Commands	ECC_UPGR
Execute Logical Operating System Commands	ENTERPRISE
Execute Logical Operating System Commands	EX_DEMO_SUP
Execute Logical Operating System Commands	FINBTR@ID3

System Audit Report

Text of Criterion	User
Execute Logical Operating System Commands	FISCHER
Execute Logical Operating System Commands	FISCHERB
Execute Logical Operating System Commands	FISCHERK
Execute Logical Operating System Commands	FORTMANN
Execute Logical Operating System Commands	FRICKE
Execute Logical Operating System Commands	GARBRISCH
Execute Logical Operating System Commands	GAUTHIER
Execute Logical Operating System Commands	GENTNERB
Execute Logical Operating System Commands	GIRI
Execute Logical Operating System Commands	GODZIEBA
Execute Logical Operating System Commands	GONSIOR
Execute Logical Operating System Commands	GRAUENHORST
Execute Logical Operating System Commands	HABERSACK
Execute Logical Operating System Commands	HAMID
Execute Logical Operating System Commands	HOCHADEL
Execute Logical Operating System Commands	HOEVERMANN
Execute Logical Operating System Commands	HORSTA
Execute Logical Operating System Commands	HUETT
Execute Logical Operating System Commands	ID3TEST
Execute Logical Operating System Commands	IDADMIN
Execute Logical Operating System Commands	ISM
Execute Logical Operating System Commands	KARASU
Execute Logical Operating System Commands	KATZSCHNER
Execute Logical Operating System Commands	KILIAN
Execute Logical Operating System Commands	KIRST
Execute Logical Operating System Commands	KOCHS
Execute Logical Operating System Commands	KOCHUL
Execute Logical Operating System Commands	KRELLJ
Execute Logical Operating System Commands	KUEHN
Execute Logical Operating System Commands	LANGSTON
Execute Logical Operating System Commands	LCHAMDONDOG
Execute Logical Operating System Commands	LEITSCH
Execute Logical Operating System Commands	LEUPOLD
Execute Logical Operating System Commands	LORENZ

System Audit Report

Text of Criterion	User
Execute Logical Operating System Commands	LORENZC
Execute Logical Operating System Commands	LOTUS
Execute Logical Operating System Commands	LUETKEHOFF
Execute Logical Operating System Commands	MAASSBERG
Execute Logical Operating System Commands	MEERWARTH
Execute Logical Operating System Commands	MICHALSKY
Execute Logical Operating System Commands	MIZUNO
Execute Logical Operating System Commands	MONSNG
Execute Logical Operating System Commands	MONUSA
Execute Logical Operating System Commands	MUELLERUW
Execute Logical Operating System Commands	NATZMER
Execute Logical Operating System Commands	NGDCREF4
Execute Logical Operating System Commands	NIEDEROEST
Execute Logical Operating System Commands	OBERBOERSCHG
Execute Logical Operating System Commands	OERDING
Execute Logical Operating System Commands	OLZOG
Execute Logical Operating System Commands	PALADM
Execute Logical Operating System Commands	PCSETUP
Execute Logical Operating System Commands	PEISL
Execute Logical Operating System Commands	PETER
Execute Logical Operating System Commands	PSS
Execute Logical Operating System Commands	RAMOS
Execute Logical Operating System Commands	RBAEIM4
Execute Logical Operating System Commands	RBANK4
Execute Logical Operating System Commands	RBIHANA4
Execute Logical Operating System Commands	RCIO4
Execute Logical Operating System Commands	RCLA4
Execute Logical Operating System Commands	RCRM4
Execute Logical Operating System Commands	RCSA4
Execute Logical Operating System Commands	REINELTD
Execute Logical Operating System Commands	RENSEL
Execute Logical Operating System Commands	REPM4
Execute Logical Operating System Commands	RFC_CONV
Execute Logical Operating System Commands	RFIGRC4

Text of Criterion	User
Execute Logical Operating System Commands	RFIORI4
Execute Logical Operating System Commands	RHANA4
Execute Logical Operating System Commands	RHCM4
Execute Logical Operating System Commands	RINSHC4
Execute Logical Operating System Commands	RLOB4
Execute Logical Operating System Commands	RMANU4
Execute Logical Operating System Commands	RMOBIL4
Execute Logical Operating System Commands	RPLM4
Execute Logical Operating System Commands	RPS4
Execute Logical Operating System Commands	RRDS4
Execute Logical Operating System Commands	RRETAIL4
Execute Logical Operating System Commands	RSCM4
Execute Logical Operating System Commands	RSRM4
Execute Logical Operating System Commands	RSUSTAIN4
Execute Logical Operating System Commands	RUBENADM
Execute Logical Operating System Commands	RUTTELC4
Execute Logical Operating System Commands	SAP*
Execute Logical Operating System Commands	SAPCPIC
Execute Logical Operating System Commands	SAWKENG
Execute Logical Operating System Commands	SCHULZET
Execute Logical Operating System Commands	SDCAUTO
Execute Logical Operating System Commands	SDCMONI
Execute Logical Operating System Commands	SELVARAJ
Execute Logical Operating System Commands	SE_DEMO_SUP
Execute Logical Operating System Commands	SE_SAPADMIN
Execute Logical Operating System Commands	SIMONSON
Execute Logical Operating System Commands	SMTMSMD
Execute Logical Operating System Commands	SM_SMC
Execute Logical Operating System Commands	SM_SMD
Execute Logical Operating System Commands	SOLMANM58001
Execute Logical Operating System Commands	SOLMANSAM000
Execute Logical Operating System Commands	STADEL
Execute Logical Operating System Commands	STSADMIN
Execute Logical Operating System Commands	SUPPORT

Text of Criterion	User
Execute Logical Operating System Commands	TCSADM
Execute Logical Operating System Commands	TCS_DEMO_2ND
Execute Logical Operating System Commands	TCS_DEMO_SUP
Execute Logical Operating System Commands	TDC
Execute Logical Operating System Commands	TDC_CATT
Execute Logical Operating System Commands	TDC_SAPADMIN
Execute Logical Operating System Commands	TEST
Execute Logical Operating System Commands	TOEWEU
Execute Logical Operating System Commands	TRANS
Execute Logical Operating System Commands	U4UMGMTPSS
Execute Logical Operating System Commands	UPGRADE
Execute Logical Operating System Commands	VEITSHANSC
Execute Logical Operating System Commands	VERNAQ
Execute Logical Operating System Commands	VERNITSKAJAK
Execute Logical Operating System Commands	VP_SAPADMIN
Execute Logical Operating System Commands	WATKINSG
Execute Logical Operating System Commands	WEISSAN
Execute Logical Operating System Commands	WF-BATCH
Execute Logical Operating System Commands	WORSCH
Administration: CCMS Maintenance	BASIS
Administration: CCMS Maintenance	BATIPPS
Administration: CCMS Maintenance	BCDEPLOY
Administration: CCMS Maintenance	BEZRUKOV
Administration: CCMS Maintenance	BLOCHING
Administration: CCMS Maintenance	BLUMOEHR
Administration: CCMS Maintenance	BOEHMA
Administration: CCMS Maintenance	BOLLINGER
Administration: CCMS Maintenance	BREINING
Administration: CCMS Maintenance	BRENNER
Administration: CCMS Maintenance	BRUNSG
Administration: CCMS Maintenance	BUCHERT
Administration: CCMS Maintenance	BUCHWALD
Administration: CCMS Maintenance	CCMS
Administration: CCMS Maintenance	CURA

Text of Criterion	User
Administration: CCMS Maintenance	DAVISCH
Administration: CCMS Maintenance	DDIC
Administration: CCMS Maintenance	DDICSUPPORT
Administration: CCMS Maintenance	DIEHL
Administration: CCMS Maintenance	DISANTO
Administration: CCMS Maintenance	DKCADM
Administration: CCMS Maintenance	DROESCHER
Administration: CCMS Maintenance	ECC_UPGR
Administration: CCMS Maintenance	ENTERPRISE
Administration: CCMS Maintenance	EX_DEMO_SUP
Administration: CCMS Maintenance	FINBTR@ID3
Administration: CCMS Maintenance	FISCHER
Administration: CCMS Maintenance	FISCHERB
Administration: CCMS Maintenance	FISCHERK
Administration: CCMS Maintenance	FORTMANN
Administration: CCMS Maintenance	FRICKE
Administration: CCMS Maintenance	GARBRISCH
Administration: CCMS Maintenance	GAUTHIER
Administration: CCMS Maintenance	GENTNERB
Administration: CCMS Maintenance	GIRI
Administration: CCMS Maintenance	GODZIEBA
Administration: CCMS Maintenance	GONSIOR
Administration: CCMS Maintenance	GRAUENHORST
Administration: CCMS Maintenance	HABERSACK
Administration: CCMS Maintenance	HAMID
Administration: CCMS Maintenance	HOCHADEL
Administration: CCMS Maintenance	HOEVERMANN
Administration: CCMS Maintenance	HORSTA
Administration: CCMS Maintenance	HUETT
Administration: CCMS Maintenance	ID3TEST
Administration: CCMS Maintenance	IDADMIN
Administration: CCMS Maintenance	ISM
Administration: CCMS Maintenance	KARASU
Administration: CCMS Maintenance	KATZSCHNER

System Audit Report

Text of Criterion	User
Administration: CCMS Maintenance	KILIAN
Administration: CCMS Maintenance	KIRST
Administration: CCMS Maintenance	KOCHS
Administration: CCMS Maintenance	KOCHUL
Administration: CCMS Maintenance	KRELLJ
Administration: CCMS Maintenance	KUEHN
Administration: CCMS Maintenance	LANGSTON
Administration: CCMS Maintenance	LCHAMDONDOG
Administration: CCMS Maintenance	LEITSCH
Administration: CCMS Maintenance	LEUPOLD
Administration: CCMS Maintenance	LORENZ
Administration: CCMS Maintenance	LORENZC
Administration: CCMS Maintenance	LOTUS
Administration: CCMS Maintenance	LUETKEHOFF
Administration: CCMS Maintenance	MAASSBERG
Administration: CCMS Maintenance	MEERWARTH
Administration: CCMS Maintenance	MICHALSKY
Administration: CCMS Maintenance	MIZUNO
Administration: CCMS Maintenance	MONSNG
Administration: CCMS Maintenance	MONUSA
Administration: CCMS Maintenance	MUELLERUW
Administration: CCMS Maintenance	NATZMER
Administration: CCMS Maintenance	NGDCREF4
Administration: CCMS Maintenance	NIEDEROEST
Administration: CCMS Maintenance	OBERBOERSCHG
Administration: CCMS Maintenance	OERDING
Administration: CCMS Maintenance	OLZOG
Administration: CCMS Maintenance	PALADM
Administration: CCMS Maintenance	PCSETUP
Administration: CCMS Maintenance	PEISL
Administration: CCMS Maintenance	PETER
Administration: CCMS Maintenance	PSS
Administration: CCMS Maintenance	RAMOS
Administration: CCMS Maintenance	RBAEIM4

Text of Criterion	User
Administration: CCMS Maintenance	RBANK4
Administration: CCMS Maintenance	RBIHANA4
Administration: CCMS Maintenance	RCIO4
Administration: CCMS Maintenance	RCLA4
Administration: CCMS Maintenance	RCRM4
Administration: CCMS Maintenance	RCSA4
Administration: CCMS Maintenance	REINELTD
Administration: CCMS Maintenance	RENSEL
Administration: CCMS Maintenance	REPM4
Administration: CCMS Maintenance	RFC_CONV
Administration: CCMS Maintenance	RFIGRC4
Administration: CCMS Maintenance	RFIORI4
Administration: CCMS Maintenance	RHANA4
Administration: CCMS Maintenance	RHCM4
Administration: CCMS Maintenance	RINSHC4
Administration: CCMS Maintenance	RLOB4
Administration: CCMS Maintenance	RMANU4
Administration: CCMS Maintenance	RMOBIL4
Administration: CCMS Maintenance	RPLM4
Administration: CCMS Maintenance	RPS4
Administration: CCMS Maintenance	RRDS4
Administration: CCMS Maintenance	RRETAIL4
Administration: CCMS Maintenance	RSCM4
Administration: CCMS Maintenance	RSRM4
Administration: CCMS Maintenance	RSUSTAIN4
Administration: CCMS Maintenance	RUBENADM
Administration: CCMS Maintenance	RUTTELC4
Administration: CCMS Maintenance	SAP*
Administration: CCMS Maintenance	SAPCPIC
Administration: CCMS Maintenance	SAWKENG
Administration: CCMS Maintenance	SCHULZET
Administration: CCMS Maintenance	SDCAUTO
Administration: CCMS Maintenance	SDCMONI
Administration: CCMS Maintenance	SELVARAJ

System Audit Report

Text of Criterion	User
Administration: CCMS Maintenance	SE_DEMO_SUP
Administration: CCMS Maintenance	SE_SAPADMIN
Administration: CCMS Maintenance	SIMONSON
Administration: CCMS Maintenance	SMTMSMD
Administration: CCMS Maintenance	SM_ADMIN_SMC
Administration: CCMS Maintenance	SM_SMC
Administration: CCMS Maintenance	SM_SMD
Administration: CCMS Maintenance	SOLMANM58001
Administration: CCMS Maintenance	SOLMANSAM000
Administration: CCMS Maintenance	STADEL
Administration: CCMS Maintenance	STSADMIN
Administration: CCMS Maintenance	SUPPORT
Administration: CCMS Maintenance	TCSADM
Administration: CCMS Maintenance	TCS_DEMO_2ND
Administration: CCMS Maintenance	TCS_DEMO_SUP
Administration: CCMS Maintenance	TDC
Administration: CCMS Maintenance	TDC_CATT
Administration: CCMS Maintenance	TDC_SAPADMIN
Administration: CCMS Maintenance	TEST
Administration: CCMS Maintenance	TOEWEU
Administration: CCMS Maintenance	TRANS
Administration: CCMS Maintenance	U4UMGMTPSS
Administration: CCMS Maintenance	UPGRADE
Administration: CCMS Maintenance	VEITSHANSC
Administration: CCMS Maintenance	VERNAQ
Administration: CCMS Maintenance	VERNITSKAJAK
Administration: CCMS Maintenance	VP_SAPADMIN
Administration: CCMS Maintenance	WATKINSG
Administration: CCMS Maintenance	WEISSAN
Administration: CCMS Maintenance	WF-BATCH
Administration: CCMS Maintenance	WORSCH
Administration: Operations on Secured Print Requests	BASIS
Administration: Operations on Secured Print Requests	BATIPPS
Administration: Operations on Secured Print Requests	BCDEPLOY

System Audit Report

Text of Criterion	User
Administration: Operations on Secured Print Requests	BEZRUKOV
Administration: Operations on Secured Print Requests	BLOCHING
Administration: Operations on Secured Print Requests	BLUMOEHR
Administration: Operations on Secured Print Requests	BOEHMA
Administration: Operations on Secured Print Requests	BOLLINGER
Administration: Operations on Secured Print Requests	BREINING
Administration: Operations on Secured Print Requests	BRENNER
Administration: Operations on Secured Print Requests	BRUNSG
Administration: Operations on Secured Print Requests	BUCHERT
Administration: Operations on Secured Print Requests	BUCHWALD
Administration: Operations on Secured Print Requests	CCMS
Administration: Operations on Secured Print Requests	COMPARE
Administration: Operations on Secured Print Requests	CURA
Administration: Operations on Secured Print Requests	DAVISCH
Administration: Operations on Secured Print Requests	DDIC
Administration: Operations on Secured Print Requests	DDICSUPPORT
Administration: Operations on Secured Print Requests	DIEHL
Administration: Operations on Secured Print Requests	DISANTO
Administration: Operations on Secured Print Requests	DKCADM
Administration: Operations on Secured Print Requests	DROESCHER
Administration: Operations on Secured Print Requests	ECC_UPGR
Administration: Operations on Secured Print Requests	ENTERPRISE
Administration: Operations on Secured Print Requests	EX_DEMO_SUP
Administration: Operations on Secured Print Requests	FISCHER
Administration: Operations on Secured Print Requests	FISCHERB
Administration: Operations on Secured Print Requests	FISCHERK
Administration: Operations on Secured Print Requests	FORTMANN
Administration: Operations on Secured Print Requests	FRICKE
Administration: Operations on Secured Print Requests	GARBRISCH
Administration: Operations on Secured Print Requests	GAUTHIER
Administration: Operations on Secured Print Requests	GENTNERB
Administration: Operations on Secured Print Requests	GIRI
Administration: Operations on Secured Print Requests	GODZIEBA
Administration: Operations on Secured Print Requests	GONSIOR

System Audit Report

Text of Criterion	User
Administration: Operations on Secured Print Requests	GRAUENHORST
Administration: Operations on Secured Print Requests	HABERSACK
Administration: Operations on Secured Print Requests	HAMID
Administration: Operations on Secured Print Requests	HOCHADEL
Administration: Operations on Secured Print Requests	HOEVERMANN
Administration: Operations on Secured Print Requests	HORSTA
Administration: Operations on Secured Print Requests	HUETT
Administration: Operations on Secured Print Requests	ID3TEST
Administration: Operations on Secured Print Requests	IDADMIN
Administration: Operations on Secured Print Requests	ISM
Administration: Operations on Secured Print Requests	KARASU
Administration: Operations on Secured Print Requests	KATZSCHNER
Administration: Operations on Secured Print Requests	KILIAN
Administration: Operations on Secured Print Requests	KIRST
Administration: Operations on Secured Print Requests	KOCHS
Administration: Operations on Secured Print Requests	KOCHUL
Administration: Operations on Secured Print Requests	KRELLJ
Administration: Operations on Secured Print Requests	KUEHN
Administration: Operations on Secured Print Requests	LANGSTON
Administration: Operations on Secured Print Requests	LCHAMDONDOG
Administration: Operations on Secured Print Requests	LEITSCH
Administration: Operations on Secured Print Requests	LEUPOLD
Administration: Operations on Secured Print Requests	LORENZ
Administration: Operations on Secured Print Requests	LORENZC
Administration: Operations on Secured Print Requests	LOTUS
Administration: Operations on Secured Print Requests	LUETKEHOFF
Administration: Operations on Secured Print Requests	MAASSBERG
Administration: Operations on Secured Print Requests	MEERWARTH
Administration: Operations on Secured Print Requests	MICHALSKY
Administration: Operations on Secured Print Requests	MIZUNO
Administration: Operations on Secured Print Requests	MONSNG
Administration: Operations on Secured Print Requests	MONUSA
Administration: Operations on Secured Print Requests	MUELLERUW
Administration: Operations on Secured Print Requests	NATZMER

System Audit Report

Text of Criterion	User
Administration: Operations on Secured Print Requests	NGDCREF4
Administration: Operations on Secured Print Requests	NIEDEROEST
Administration: Operations on Secured Print Requests	OBERBOERSCHG
Administration: Operations on Secured Print Requests	OERDING
Administration: Operations on Secured Print Requests	OLZOG
Administration: Operations on Secured Print Requests	PALADM
Administration: Operations on Secured Print Requests	PCSETUP
Administration: Operations on Secured Print Requests	PEISL
Administration: Operations on Secured Print Requests	PETER
Administration: Operations on Secured Print Requests	PSS
Administration: Operations on Secured Print Requests	RAMOS
Administration: Operations on Secured Print Requests	RBAEIM4
Administration: Operations on Secured Print Requests	RBANK4
Administration: Operations on Secured Print Requests	RBIHANA4
Administration: Operations on Secured Print Requests	RCIO4
Administration: Operations on Secured Print Requests	RCLA4
Administration: Operations on Secured Print Requests	RCRM4
Administration: Operations on Secured Print Requests	RCSA4
Administration: Operations on Secured Print Requests	REINELTD
Administration: Operations on Secured Print Requests	RENSEL
Administration: Operations on Secured Print Requests	REPM4
Administration: Operations on Secured Print Requests	RFIGRC4
Administration: Operations on Secured Print Requests	RFIORI4
Administration: Operations on Secured Print Requests	RHANA4
Administration: Operations on Secured Print Requests	RHCM4
Administration: Operations on Secured Print Requests	RINSHC4
Administration: Operations on Secured Print Requests	RLOB4
Administration: Operations on Secured Print Requests	RMANU4
Administration: Operations on Secured Print Requests	RMOBIL4
Administration: Operations on Secured Print Requests	RPLM4
Administration: Operations on Secured Print Requests	RPS4
Administration: Operations on Secured Print Requests	RRDS4
Administration: Operations on Secured Print Requests	RRETAIL4
Administration: Operations on Secured Print Requests	RSCM4

System Audit Report

Text of Criterion	User
Administration: Operations on Secured Print Requests	RSRM4
Administration: Operations on Secured Print Requests	RSUSTAIN4
Administration: Operations on Secured Print Requests	RUBENADM
Administration: Operations on Secured Print Requests	RUTTELC4
Administration: Operations on Secured Print Requests	SAP*
Administration: Operations on Secured Print Requests	SAPCPIC
Administration: Operations on Secured Print Requests	SAWKENG
Administration: Operations on Secured Print Requests	SCHULZET
Administration: Operations on Secured Print Requests	SDCAUTO
Administration: Operations on Secured Print Requests	SDCMONI
Administration: Operations on Secured Print Requests	SELVARAJ
Administration: Operations on Secured Print Requests	SE_DEMO_SUP
Administration: Operations on Secured Print Requests	SE_SAPADMIN
Administration: Operations on Secured Print Requests	SIMONSON
Administration: Operations on Secured Print Requests	STADEL
Administration: Operations on Secured Print Requests	STSADMIN
Administration: Operations on Secured Print Requests	SUPPORT
Administration: Operations on Secured Print Requests	TCSADM
Administration: Operations on Secured Print Requests	TCS_DEMO_2ND
Administration: Operations on Secured Print Requests	TCS_DEMO_SUP
Administration: Operations on Secured Print Requests	TDC
Administration: Operations on Secured Print Requests	TDC_CATT
Administration: Operations on Secured Print Requests	TDC_SAPADMIN
Administration: Operations on Secured Print Requests	TEST
Administration: Operations on Secured Print Requests	TOEWEU
Administration: Operations on Secured Print Requests	TRANS
Administration: Operations on Secured Print Requests	U4UMGMTPSS
Administration: Operations on Secured Print Requests	UPGRADE
Administration: Operations on Secured Print Requests	VEITSHANSC
Administration: Operations on Secured Print Requests	VERNAQ
Administration: Operations on Secured Print Requests	VERNITSKAJAK
Administration: Operations on Secured Print Requests	VP_SAPADMIN
Administration: Operations on Secured Print Requests	WATKINSG
Administration: Operations on Secured Print Requests	WEISSAN

System Audit Report

Text of Criterion	User
Administration: Operations on Secured Print Requests	WF-BATCH
Administration: Operations on Secured Print Requests	WORSCH
Administration: Print on All Printers	ANZEIGER
Administration: Print on All Printers	ARCHIVE
Administration: Print on All Printers	BASIS
Administration: Print on All Printers	BATIPPS
Administration: Print on All Printers	BCDEPLOY
Administration: Print on All Printers	BEZRUKOV
Administration: Print on All Printers	BLOCHING
Administration: Print on All Printers	BLUMOEHR
Administration: Print on All Printers	BOEHMA
Administration: Print on All Printers	BOLLINGER
Administration: Print on All Printers	BREINING
Administration: Print on All Printers	BRENNER
Administration: Print on All Printers	BRUNSG
Administration: Print on All Printers	BUCHERT
Administration: Print on All Printers	BUCHWALD
Administration: Print on All Printers	CCMS
Administration: Print on All Printers	COMPARE
Administration: Print on All Printers	CURA
Administration: Print on All Printers	DAVISCH
Administration: Print on All Printers	DDIC
Administration: Print on All Printers	DDICSUPPORT
Administration: Print on All Printers	DIEHL
Administration: Print on All Printers	DISANTO
Administration: Print on All Printers	DKCADM
Administration: Print on All Printers	DROESCHER
Administration: Print on All Printers	ECC_UPGR
Administration: Print on All Printers	ENTERPRISE
Administration: Print on All Printers	EX_DEMO_SUP
Administration: Print on All Printers	FISCHER
Administration: Print on All Printers	FISCHERB
Administration: Print on All Printers	FISCHERK
Administration: Print on All Printers	FORTMANN

Text of Criterion	User
Administration: Print on All Printers	FRICKE
Administration: Print on All Printers	GARBRISCH
Administration: Print on All Printers	GAUTHIER
Administration: Print on All Printers	GENTNERB
Administration: Print on All Printers	GIRI
Administration: Print on All Printers	GODZIEBA
Administration: Print on All Printers	GONSIOR
Administration: Print on All Printers	GRAUENHORST
Administration: Print on All Printers	HABERSACK
Administration: Print on All Printers	HAMID
Administration: Print on All Printers	HOCHADEL
Administration: Print on All Printers	HOEVERMANN
Administration: Print on All Printers	HORSTA
Administration: Print on All Printers	HUETT
Administration: Print on All Printers	ID3TEST
Administration: Print on All Printers	IDADMIN
Administration: Print on All Printers	ISM
Administration: Print on All Printers	KARASU
Administration: Print on All Printers	KATZSCHNER
Administration: Print on All Printers	KILIAN
Administration: Print on All Printers	KIRST
Administration: Print on All Printers	KOCHS
Administration: Print on All Printers	KOCHUL
Administration: Print on All Printers	KRELLJ
Administration: Print on All Printers	KUEHN
Administration: Print on All Printers	LANGSTON
Administration: Print on All Printers	LCHAMDONDOG
Administration: Print on All Printers	LEITSCH
Administration: Print on All Printers	LEUPOLD
Administration: Print on All Printers	LORENZ
Administration: Print on All Printers	LORENZC
Administration: Print on All Printers	LOTUS
Administration: Print on All Printers	LUETKEHOFF
Administration: Print on All Printers	MAASSBERG

System Audit Report

Text of Criterion	User
Administration: Print on All Printers	MEERWARTH
Administration: Print on All Printers	MICHALSKY
Administration: Print on All Printers	MIZUNO
Administration: Print on All Printers	MONSNG
Administration: Print on All Printers	MONUSA
Administration: Print on All Printers	MUELLERUW
Administration: Print on All Printers	NATZMER
Administration: Print on All Printers	NGDCREF4
Administration: Print on All Printers	NIEDEROEST
Administration: Print on All Printers	OBERBOERSCHG
Administration: Print on All Printers	OERDING
Administration: Print on All Printers	OLZOG
Administration: Print on All Printers	PALADM
Administration: Print on All Printers	PCSETUP
Administration: Print on All Printers	PEISL
Administration: Print on All Printers	PETER
Administration: Print on All Printers	PSS
Administration: Print on All Printers	RAMOS
Administration: Print on All Printers	RBAEIM4
Administration: Print on All Printers	RBANK4
Administration: Print on All Printers	RBIHANA4
Administration: Print on All Printers	RCIO4
Administration: Print on All Printers	RCLA4
Administration: Print on All Printers	RCRM4
Administration: Print on All Printers	RCSA4
Administration: Print on All Printers	REINELTD
Administration: Print on All Printers	RENSEL
Administration: Print on All Printers	REPM4
Administration: Print on All Printers	RFC_CONV
Administration: Print on All Printers	RFIGRC4
Administration: Print on All Printers	RFIORI4
Administration: Print on All Printers	RHANA4
Administration: Print on All Printers	RHCM4
Administration: Print on All Printers	RINSHC4

Text of Criterion	User
Administration: Print on All Printers	RLOB4
Administration: Print on All Printers	RMANU4
Administration: Print on All Printers	RMOBIL4
Administration: Print on All Printers	RPLM4
Administration: Print on All Printers	RPS4
Administration: Print on All Printers	RRDS4
Administration: Print on All Printers	RRETAIL4
Administration: Print on All Printers	RSCM4
Administration: Print on All Printers	RSRM4
Administration: Print on All Printers	RSUSTAIN4
Administration: Print on All Printers	RUBENADM
Administration: Print on All Printers	RUTTELC4
Administration: Print on All Printers	SAP*
Administration: Print on All Printers	SAPCPIC
Administration: Print on All Printers	SAPSUPPORT
Administration: Print on All Printers	SAWKENG
Administration: Print on All Printers	SCHULZET
Administration: Print on All Printers	SDCAUTO
Administration: Print on All Printers	SDCMONI
Administration: Print on All Printers	SELVARAJ
Administration: Print on All Printers	SE_DEMO_SUP
Administration: Print on All Printers	SE_SAPADMIN
Administration: Print on All Printers	SIMONSON
Administration: Print on All Printers	STADEL
Administration: Print on All Printers	STSADMIN
Administration: Print on All Printers	SUPPORT
Administration: Print on All Printers	S_A.SHOW
Administration: Print on All Printers	TCSADM
Administration: Print on All Printers	TCS_DEMO_2ND
Administration: Print on All Printers	TCS_DEMO_SUP
Administration: Print on All Printers	TDC
Administration: Print on All Printers	TDC_CATT
Administration: Print on All Printers	TDC_SAPADMIN
Administration: Print on All Printers	TEST

Text of Criterion	User
Administration: Print on All Printers	TOEWEU
Administration: Print on All Printers	TRANS
Administration: Print on All Printers	U4UMGMTPSS
Administration: Print on All Printers	UPGRADE
Administration: Print on All Printers	VEITSHANSC
Administration: Print on All Printers	VERNAQ
Administration: Print on All Printers	VERNITSKAJAK
Administration: Print on All Printers	VP_SAPADMIN
Administration: Print on All Printers	WATKINSG
Administration: Print on All Printers	WEISSAN
Administration: Print on All Printers	WF-BATCH
Administration: Print on All Printers	WORSCH
Administration: Operations on Other TemSe Objects	BASIS
Administration: Operations on Other TemSe Objects	BATIPPS
Administration: Operations on Other TemSe Objects	BCDEPLOY
Administration: Operations on Other TemSe Objects	BEZRUKOV
Administration: Operations on Other TemSe Objects	BLOCHING
Administration: Operations on Other TemSe Objects	BLUMOEHR
Administration: Operations on Other TemSe Objects	BOEHMA
Administration: Operations on Other TemSe Objects	BOLLINGER
Administration: Operations on Other TemSe Objects	BREINING
Administration: Operations on Other TemSe Objects	BRENNER
Administration: Operations on Other TemSe Objects	BRUNSG
Administration: Operations on Other TemSe Objects	BUCHERT
Administration: Operations on Other TemSe Objects	BUCHWALD
Administration: Operations on Other TemSe Objects	CCMS
Administration: Operations on Other TemSe Objects	CURA
Administration: Operations on Other TemSe Objects	DAVISCH
Administration: Operations on Other TemSe Objects	DDIC
Administration: Operations on Other TemSe Objects	DDICSUPPORT
Administration: Operations on Other TemSe Objects	DIEHL
Administration: Operations on Other TemSe Objects	DISANTO
Administration: Operations on Other TemSe Objects	DKCADM
Administration: Operations on Other TemSe Objects	DROESCHER

System Audit Report

Text of Criterion	User
Administration: Operations on Other TemSe Objects	ECC_UPGR
Administration: Operations on Other TemSe Objects	ENTERPRISE
Administration: Operations on Other TemSe Objects	EX_DEMO_SUP
Administration: Operations on Other TemSe Objects	FISCHER
Administration: Operations on Other TemSe Objects	FISCHERB
Administration: Operations on Other TemSe Objects	FISCHERK
Administration: Operations on Other TemSe Objects	FORTMANN
Administration: Operations on Other TemSe Objects	FRICKE
Administration: Operations on Other TemSe Objects	GARBRISCH
Administration: Operations on Other TemSe Objects	GAUTHIER
Administration: Operations on Other TemSe Objects	GENTNERB
Administration: Operations on Other TemSe Objects	GIRI
Administration: Operations on Other TemSe Objects	GODZIEBA
Administration: Operations on Other TemSe Objects	GONSIOR
Administration: Operations on Other TemSe Objects	GRAUENHORST
Administration: Operations on Other TemSe Objects	HABERSACK
Administration: Operations on Other TemSe Objects	HAMID
Administration: Operations on Other TemSe Objects	HOCHADEL
Administration: Operations on Other TemSe Objects	HOEVERMANN
Administration: Operations on Other TemSe Objects	HORSTA
Administration: Operations on Other TemSe Objects	HUETT
Administration: Operations on Other TemSe Objects	ID3TEST
Administration: Operations on Other TemSe Objects	IDADMIN
Administration: Operations on Other TemSe Objects	ISM
Administration: Operations on Other TemSe Objects	KARASU
Administration: Operations on Other TemSe Objects	KATZSCHNER
Administration: Operations on Other TemSe Objects	KILIAN
Administration: Operations on Other TemSe Objects	KIRST
Administration: Operations on Other TemSe Objects	KOCHS
Administration: Operations on Other TemSe Objects	KOCHUL
Administration: Operations on Other TemSe Objects	KRELLJ
Administration: Operations on Other TemSe Objects	KUEHN
Administration: Operations on Other TemSe Objects	LANGSTON
Administration: Operations on Other TemSe Objects	LCHAMDONDOG

System Audit Report

Text of Criterion	User
Administration: Operations on Other TemSe Objects	LEITSCH
Administration: Operations on Other TemSe Objects	LEUPOLD
Administration: Operations on Other TemSe Objects	LORENZ
Administration: Operations on Other TemSe Objects	LORENZC
Administration: Operations on Other TemSe Objects	LOTUS
Administration: Operations on Other TemSe Objects	LUETKEHOFF
Administration: Operations on Other TemSe Objects	MAASSBERG
Administration: Operations on Other TemSe Objects	MEERWARTH
Administration: Operations on Other TemSe Objects	MICHALSKY
Administration: Operations on Other TemSe Objects	MIZUNO
Administration: Operations on Other TemSe Objects	MONSNG
Administration: Operations on Other TemSe Objects	MONUSA
Administration: Operations on Other TemSe Objects	MUELLERUW
Administration: Operations on Other TemSe Objects	NATZMER
Administration: Operations on Other TemSe Objects	NGDCREF4
Administration: Operations on Other TemSe Objects	NIEDEROEST
Administration: Operations on Other TemSe Objects	OBERBOERSCHG
Administration: Operations on Other TemSe Objects	OERDING
Administration: Operations on Other TemSe Objects	OLZOG
Administration: Operations on Other TemSe Objects	PALADM
Administration: Operations on Other TemSe Objects	PCSETUP
Administration: Operations on Other TemSe Objects	PEISL
Administration: Operations on Other TemSe Objects	PETER
Administration: Operations on Other TemSe Objects	PSS
Administration: Operations on Other TemSe Objects	RAMOS
Administration: Operations on Other TemSe Objects	RBAEIM4
Administration: Operations on Other TemSe Objects	RBANK4
Administration: Operations on Other TemSe Objects	RBIHANA4
Administration: Operations on Other TemSe Objects	RCIO4
Administration: Operations on Other TemSe Objects	RCLA4
Administration: Operations on Other TemSe Objects	RCRM4
Administration: Operations on Other TemSe Objects	RCSA4
Administration: Operations on Other TemSe Objects	REINELTD
Administration: Operations on Other TemSe Objects	RENSEL

Text of Criterion	User
Administration: Operations on Other TemSe Objects	REPM4
Administration: Operations on Other TemSe Objects	RFIGRC4
Administration: Operations on Other TemSe Objects	RFIORI4
Administration: Operations on Other TemSe Objects	RHANA4
Administration: Operations on Other TemSe Objects	RHCM4
Administration: Operations on Other TemSe Objects	RINSHC4
Administration: Operations on Other TemSe Objects	RLOB4
Administration: Operations on Other TemSe Objects	RMANU4
Administration: Operations on Other TemSe Objects	RMOBIL4
Administration: Operations on Other TemSe Objects	RPLM4
Administration: Operations on Other TemSe Objects	RPS4
Administration: Operations on Other TemSe Objects	RRDS4
Administration: Operations on Other TemSe Objects	RRETAIL4
Administration: Operations on Other TemSe Objects	RSCM4
Administration: Operations on Other TemSe Objects	RSRM4
Administration: Operations on Other TemSe Objects	RSUSTAIN4
Administration: Operations on Other TemSe Objects	RUBENADM
Administration: Operations on Other TemSe Objects	RUTTELC4
Administration: Operations on Other TemSe Objects	SAP*
Administration: Operations on Other TemSe Objects	SAPCPIC
Administration: Operations on Other TemSe Objects	SAWKENG
Administration: Operations on Other TemSe Objects	SCHULZET
Administration: Operations on Other TemSe Objects	SDCAUTO
Administration: Operations on Other TemSe Objects	SDCMONI
Administration: Operations on Other TemSe Objects	SELVARAJ
Administration: Operations on Other TemSe Objects	SE_DEMO_SUP
Administration: Operations on Other TemSe Objects	SE_SAPADMIN
Administration: Operations on Other TemSe Objects	SIMONSON
Administration: Operations on Other TemSe Objects	STADEL
Administration: Operations on Other TemSe Objects	STSADMIN
Administration: Operations on Other TemSe Objects	SUPPORT
Administration: Operations on Other TemSe Objects	TCSADM
Administration: Operations on Other TemSe Objects	TCS_DEMO_2ND
Administration: Operations on Other TemSe Objects	TCS_DEMO_SUP

Text of Criterion	User
Administration: Operations on Other TemSe Objects	TDC
Administration: Operations on Other TemSe Objects	TDC_CATT
Administration: Operations on Other TemSe Objects	TDC_SAPADMIN
Administration: Operations on Other TemSe Objects	TEST
Administration: Operations on Other TemSe Objects	TOEWEU
Administration: Operations on Other TemSe Objects	TRANS
Administration: Operations on Other TemSe Objects	U4UMGMTPSS
Administration: Operations on Other TemSe Objects	UPGRADE
Administration: Operations on Other TemSe Objects	VEITSHANSC
Administration: Operations on Other TemSe Objects	VERNAQ
Administration: Operations on Other TemSe Objects	VERNITSKAJAK
Administration: Operations on Other TemSe Objects	VP_SAPADMIN
Administration: Operations on Other TemSe Objects	WATKINSG
Administration: Operations on Other TemSe Objects	WEISSAN
Administration: Operations on Other TemSe Objects	WF-BATCH
Administration: Operations on Other TemSe Objects	WORSCH
Adminsitration: Authorization Maintenance	BASIS
Adminsitration: Authorization Maintenance	BATIPPS
Adminsitration: Authorization Maintenance	BCDEPLOY
Adminsitration: Authorization Maintenance	BEZRUKOV
Adminsitration: Authorization Maintenance	BLOCHING
Adminsitration: Authorization Maintenance	BLUMOEHR
Adminsitration: Authorization Maintenance	BOEHMA
Adminsitration: Authorization Maintenance	BOLLINGER
Adminsitration: Authorization Maintenance	BREINING
Adminsitration: Authorization Maintenance	BRENNER
Adminsitration: Authorization Maintenance	BRUNSG
Adminsitration: Authorization Maintenance	BUCHERT
Adminsitration: Authorization Maintenance	BUCHWALD
Adminsitration: Authorization Maintenance	CCMS
Adminsitration: Authorization Maintenance	CURA
Adminsitration: Authorization Maintenance	DAVISCH
Adminsitration: Authorization Maintenance	DDIC
Adminsitration: Authorization Maintenance	DDICSUPPORT

System Audit Report

Text of Criterion	User
Adminsitration: Authorization Maintenance	DIEHL
Adminsitration: Authorization Maintenance	DISANTO
Adminsitration: Authorization Maintenance	DKCADM
Adminsitration: Authorization Maintenance	DROESCHER
Adminsitration: Authorization Maintenance	ECC_UPGR
Adminsitration: Authorization Maintenance	ENTERPRISE
Adminsitration: Authorization Maintenance	EX_DEMO_SUP
Adminsitration: Authorization Maintenance	FISCHER
Adminsitration: Authorization Maintenance	FISCHERB
Adminsitration: Authorization Maintenance	FISCHERK
Adminsitration: Authorization Maintenance	FORTMANN
Adminsitration: Authorization Maintenance	FRICKE
Adminsitration: Authorization Maintenance	GARBRISCH
Adminsitration: Authorization Maintenance	GAUTHIER
Adminsitration: Authorization Maintenance	GENTNERB
Adminsitration: Authorization Maintenance	GIRI
Adminsitration: Authorization Maintenance	GODZIEBA
Adminsitration: Authorization Maintenance	GONSIOR
Adminsitration: Authorization Maintenance	GRAUENHORST
Adminsitration: Authorization Maintenance	HABERSACK
Adminsitration: Authorization Maintenance	HAMID
Adminsitration: Authorization Maintenance	HOCHADEL
Adminsitration: Authorization Maintenance	HOEVERMANN
Adminsitration: Authorization Maintenance	HORSTA
Adminsitration: Authorization Maintenance	HUETT
Adminsitration: Authorization Maintenance	ID3TEST
Adminsitration: Authorization Maintenance	IDADMIN
Adminsitration: Authorization Maintenance	ISM
Adminsitration: Authorization Maintenance	KARASU
Adminsitration: Authorization Maintenance	KATZSCHNER
Adminsitration: Authorization Maintenance	KILIAN
Adminsitration: Authorization Maintenance	KIRST
Adminsitration: Authorization Maintenance	KOCHS
Adminsitration: Authorization Maintenance	KOCHUL

System Audit Report

Text of Criterion	User
Adminsitration: Authorization Maintenance	KRELLJ
Adminsitration: Authorization Maintenance	KUEHN
Adminsitration: Authorization Maintenance	LANGSTON
Adminsitration: Authorization Maintenance	LCHAMDONDOG
Adminsitration: Authorization Maintenance	LEITSCH
Adminsitration: Authorization Maintenance	LEUPOLD
Adminsitration: Authorization Maintenance	LORENZ
Adminsitration: Authorization Maintenance	LORENZC
Adminsitration: Authorization Maintenance	LOTUS
Adminsitration: Authorization Maintenance	LUETKEHOFF
Adminsitration: Authorization Maintenance	MAASSBERG
Adminsitration: Authorization Maintenance	MEERWARTH
Adminsitration: Authorization Maintenance	MICHALSKY
Adminsitration: Authorization Maintenance	MIZUNO
Adminsitration: Authorization Maintenance	MONSNG
Adminsitration: Authorization Maintenance	MONUSA
Adminsitration: Authorization Maintenance	MUELLERUW
Adminsitration: Authorization Maintenance	NATZMER
Adminsitration: Authorization Maintenance	NGDCREF4
Adminsitration: Authorization Maintenance	NIEDEROEST
Adminsitration: Authorization Maintenance	OBERBOERSCHG
Adminsitration: Authorization Maintenance	OERDING
Adminsitration: Authorization Maintenance	OLZOG
Adminsitration: Authorization Maintenance	PALADM
Adminsitration: Authorization Maintenance	PCSETUP
Adminsitration: Authorization Maintenance	PEISL
Adminsitration: Authorization Maintenance	PETER
Adminsitration: Authorization Maintenance	PSS
Adminsitration: Authorization Maintenance	RAMOS
Adminsitration: Authorization Maintenance	RBAEIM4
Adminsitration: Authorization Maintenance	RBANK4
Adminsitration: Authorization Maintenance	RBIHANA4
Adminsitration: Authorization Maintenance	RCIO4
Adminsitration: Authorization Maintenance	RCLA4

Text of Criterion	User
Adminsitration: Authorization Maintenance	RCRM4
Adminsitration: Authorization Maintenance	RCSA4
Adminsitration: Authorization Maintenance	REINELTD
Adminsitration: Authorization Maintenance	RENSEL
Adminsitration: Authorization Maintenance	REPM4
Adminsitration: Authorization Maintenance	RFIGRC4
Adminsitration: Authorization Maintenance	RFIORI4
Adminsitration: Authorization Maintenance	RHANA4
Adminsitration: Authorization Maintenance	RHCM4
Adminsitration: Authorization Maintenance	RINSHC4
Adminsitration: Authorization Maintenance	RLOB4
Adminsitration: Authorization Maintenance	RMANU4
Adminsitration: Authorization Maintenance	RMOBIL4
Adminsitration: Authorization Maintenance	RPLM4
Adminsitration: Authorization Maintenance	RPS4
Adminsitration: Authorization Maintenance	RRDS4
Adminsitration: Authorization Maintenance	RRETAIL4
Adminsitration: Authorization Maintenance	RSCM4
Adminsitration: Authorization Maintenance	RSRM4
Adminsitration: Authorization Maintenance	RSUSTAIN4
Adminsitration: Authorization Maintenance	RUBENADM
Adminsitration: Authorization Maintenance	RUTTELC4
Adminsitration: Authorization Maintenance	SAP*
Adminsitration: Authorization Maintenance	SAPCPIC
Adminsitration: Authorization Maintenance	SAWKENG
Adminsitration: Authorization Maintenance	SCHULZET
Adminsitration: Authorization Maintenance	SDCAUTO
Adminsitration: Authorization Maintenance	SDCMONI
Adminsitration: Authorization Maintenance	SELVARAJ
Adminsitration: Authorization Maintenance	SE_DEMO_SUP
Adminsitration: Authorization Maintenance	SE_SAPADMIN
Adminsitration: Authorization Maintenance	SIMONSON
Adminsitration: Authorization Maintenance	SM_ADMIN_SMC
Adminsitration: Authorization Maintenance	STADEL

Text of Criterion	User
Adminsitration: Authorization Maintenance	STSADMIN
Adminsitration: Authorization Maintenance	SUPPORT
Adminsitration: Authorization Maintenance	TCSADM
Adminsitration: Authorization Maintenance	TCS_DEMO_2ND
Adminsitration: Authorization Maintenance	TCS_DEMO_SUP
Adminsitration: Authorization Maintenance	TDC
Adminsitration: Authorization Maintenance	TDC_CATT
Adminsitration: Authorization Maintenance	TDC_SAPADMIN
Adminsitration: Authorization Maintenance	TEST
Adminsitration: Authorization Maintenance	TOEWEU
Adminsitration: Authorization Maintenance	TRANS
Adminsitration: Authorization Maintenance	U4UMGMTPSS
Adminsitration: Authorization Maintenance	UPGRADE
Adminsitration: Authorization Maintenance	VEITSHANSC
Adminsitration: Authorization Maintenance	VERNAQ
Adminsitration: Authorization Maintenance	VERNITSKAJAK
Adminsitration: Authorization Maintenance	VP_SAPADMIN
Adminsitration: Authorization Maintenance	WATKINSG
Adminsitration: Authorization Maintenance	WEISSAN
Adminsitration: Authorization Maintenance	WF-BATCH
Adminsitration: Authorization Maintenance	WORSCH
Auditing: Display Authorizations	ANZEIGER
Auditing: Display Authorizations	BASIS
Auditing: Display Authorizations	BATIPPS
Auditing: Display Authorizations	BCDEPLOY
Auditing: Display Authorizations	BEZRUKOV
Auditing: Display Authorizations	BLOCHING
Auditing: Display Authorizations	BLUMOEHR
Auditing: Display Authorizations	BOEHMA
Auditing: Display Authorizations	BOLLINGER
Auditing: Display Authorizations	BREINING
Auditing: Display Authorizations	BRENNER
Auditing: Display Authorizations	BRUNSG
Auditing: Display Authorizations	BUCHERT

System Audit Report

Text of Criterion		User
Auditing:	Display Authorizations	BUCHWALD
Auditing:	Display Authorizations	CCMS
Auditing:	Display Authorizations	COMPARE
Auditing:	Display Authorizations	CURA
Auditing:	Display Authorizations	DAVISCH
Auditing:	Display Authorizations	DDIC
Auditing:	Display Authorizations	DDICSUPPORT
Auditing:	Display Authorizations	DIEHL
Auditing:	Display Authorizations	DISANTO
Auditing:	Display Authorizations	DKCADM
Auditing:	Display Authorizations	DROESCHER
Auditing:	Display Authorizations	ECC_UPGR
Auditing:	Display Authorizations	ENTERPRISE
Auditing:	Display Authorizations	EX_DEMO_SUP
Auditing:	Display Authorizations	FISCHER
Auditing:	Display Authorizations	FISCHERB
Auditing:	Display Authorizations	FISCHERK
Auditing:	Display Authorizations	FORTMANN
Auditing:	Display Authorizations	FRICKE
Auditing:	Display Authorizations	GARBRISCH
Auditing:	Display Authorizations	GAUTHIER
Auditing:	Display Authorizations	GENTNERB
Auditing:	Display Authorizations	GIRI
Auditing:	Display Authorizations	GODZIEBA
Auditing:	Display Authorizations	GONSIOR
Auditing:	Display Authorizations	GRAUENHORST
Auditing:	Display Authorizations	HABERSACK
Auditing:	Display Authorizations	HAMID
Auditing:	Display Authorizations	HOCHADEL
Auditing:	Display Authorizations	HOEVERMANN
Auditing:	Display Authorizations	HORSTA
Auditing:	Display Authorizations	HUETT
Auditing:	Display Authorizations	ID3TEST
Auditing:	Display Authorizations	IDADMIN

System Audit Report

Text of Criterion		User
Auditing:	Display Authorizations	ISM
Auditing:	Display Authorizations	KARASU
Auditing:	Display Authorizations	KATZSCHNER
Auditing:	Display Authorizations	KILIAN
Auditing:	Display Authorizations	KIRST
Auditing:	Display Authorizations	KOCHS
Auditing:	Display Authorizations	KOCHUL
Auditing:	Display Authorizations	KRELLJ
Auditing:	Display Authorizations	KUEHN
Auditing:	Display Authorizations	LANGSTON
Auditing:	Display Authorizations	LCHAMDONDOG
Auditing:	Display Authorizations	LEITSCH
Auditing:	Display Authorizations	LEUPOLD
Auditing:	Display Authorizations	LORENZ
Auditing:	Display Authorizations	LORENZC
Auditing:	Display Authorizations	LOTUS
Auditing:	Display Authorizations	LUETKEHOFF
Auditing:	Display Authorizations	MAASSBERG
Auditing:	Display Authorizations	MEERWARTH
Auditing:	Display Authorizations	MICHALSKY
Auditing:	Display Authorizations	MIZUNO
Auditing:	Display Authorizations	MONSNG
Auditing:	Display Authorizations	MONUSA
Auditing:	Display Authorizations	MUELLERUW
Auditing:	Display Authorizations	NATZMER
Auditing:	Display Authorizations	NGDCREF4
Auditing:	Display Authorizations	NIEDEROEST
Auditing:	Display Authorizations	OBERBOERSCHG
Auditing:	Display Authorizations	OERDING
Auditing:	Display Authorizations	OLZOG
Auditing:	Display Authorizations	PALADM
Auditing:	Display Authorizations	PCSETUP
Auditing:	Display Authorizations	PEISL
Auditing:	Display Authorizations	PETER

Text of Criterion		User
Auditing:	Display Authorizations	PITTEN
Auditing:	Display Authorizations	PSS
Auditing:	Display Authorizations	RAMOS
Auditing:	Display Authorizations	RBAEIM4
Auditing:	Display Authorizations	RBANK4
Auditing:	Display Authorizations	RBIHANA4
Auditing:	Display Authorizations	RCIO4
Auditing:	Display Authorizations	RCLA4
Auditing:	Display Authorizations	RCRM4
Auditing:	Display Authorizations	RCSA4
Auditing:	Display Authorizations	REINELTD
Auditing:	Display Authorizations	RENSEL
Auditing:	Display Authorizations	REPM4
Auditing:	Display Authorizations	RFIGRC4
Auditing:	Display Authorizations	RFIORI4
Auditing:	Display Authorizations	RHANA4
Auditing:	Display Authorizations	RHCM4
Auditing:	Display Authorizations	RINSHC4
Auditing:	Display Authorizations	RLOB4
Auditing:	Display Authorizations	RMANU4
Auditing:	Display Authorizations	RMOBIL4
Auditing:	Display Authorizations	RPLM4
Auditing:	Display Authorizations	RPS4
Auditing:	Display Authorizations	RRDS4
Auditing:	Display Authorizations	RRETAIL4
Auditing:	Display Authorizations	RSCM4
Auditing:	Display Authorizations	RSRM4
Auditing:	Display Authorizations	RSUSTAIN4
Auditing:	Display Authorizations	RUBENADM
Auditing:	Display Authorizations	RUTTELC4
Auditing:	Display Authorizations	SAP*
Auditing:	Display Authorizations	SAPCPIC
Auditing:	Display Authorizations	SAPSUPPORT
Auditing:	Display Authorizations	SAWKENG

System Audit Report

Text of Criterion	User
Auditing: Display Authorizations	SCHULZET
Auditing: Display Authorizations	SDCAUTO
Auditing: Display Authorizations	SDCMONI
Auditing: Display Authorizations	SELVARAJ
Auditing: Display Authorizations	SE_DEMO_SUP
Auditing: Display Authorizations	SE_SAPADMIN
Auditing: Display Authorizations	SIMONSON
Auditing: Display Authorizations	SM_ADMIN_SMC
Auditing: Display Authorizations	STADEL
Auditing: Display Authorizations	STSADMIN
Auditing: Display Authorizations	SUPPORT
Auditing: Display Authorizations	S_A.SHOW
Auditing: Display Authorizations	TCSADM
Auditing: Display Authorizations	TCS_DEMO_2ND
Auditing: Display Authorizations	TCS_DEMO_SUP
Auditing: Display Authorizations	TDC
Auditing: Display Authorizations	TDC_CATT
Auditing: Display Authorizations	TDC_SAPADMIN
Auditing: Display Authorizations	TEST
Auditing: Display Authorizations	TOEWEU
Auditing: Display Authorizations	TRANS
Auditing: Display Authorizations	U4UMGMTPSS
Auditing: Display Authorizations	UPGRADE
Auditing: Display Authorizations	VEITSHANSC
Auditing: Display Authorizations	VERNAQ
Auditing: Display Authorizations	VERNITSKAJAK
Auditing: Display Authorizations	VP_SAPADMIN
Auditing: Display Authorizations	WATKINSG
Auditing: Display Authorizations	WEISSAN
Auditing: Display Authorizations	WF-BATCH
Auditing: Display Authorizations	WORSCH
Administration: Profile Maintenance	BASIS
Administration: Profile Maintenance	BATIPPS
Administration: Profile Maintenance	BCDEPLOY

System Audit Report

Text of Criterion	User
Administration: Profile Maintenance	BEZRUKOV
Administration: Profile Maintenance	BLOCHING
Administration: Profile Maintenance	BLUMOEHR
Administration: Profile Maintenance	BOEHMA
Administration: Profile Maintenance	BOLLINGER
Administration: Profile Maintenance	BREINING
Administration: Profile Maintenance	BRENNER
Administration: Profile Maintenance	BRUNSG
Administration: Profile Maintenance	BUCHERT
Administration: Profile Maintenance	BUCHWALD
Administration: Profile Maintenance	CCMS
Administration: Profile Maintenance	CURA
Administration: Profile Maintenance	DAVISCH
Administration: Profile Maintenance	DDIC
Administration: Profile Maintenance	DDICSUPPORT
Administration: Profile Maintenance	DIEHL
Administration: Profile Maintenance	DISANTO
Administration: Profile Maintenance	DKCADM
Administration: Profile Maintenance	DROESCHER
Administration: Profile Maintenance	ECC_UPGR
Administration: Profile Maintenance	ENTERPRISE
Administration: Profile Maintenance	EX_DEMO_SUP
Administration: Profile Maintenance	FISCHER
Administration: Profile Maintenance	FISCHERB
Administration: Profile Maintenance	FISCHERK
Administration: Profile Maintenance	FORTMANN
Administration: Profile Maintenance	FRICKE
Administration: Profile Maintenance	GARBRISCH
Administration: Profile Maintenance	GAUTHIER
Administration: Profile Maintenance	GENTNERB
Administration: Profile Maintenance	GIRI
Administration: Profile Maintenance	GODZIEBA
Administration: Profile Maintenance	GONSIOR
Administration: Profile Maintenance	GRAUENHORST

System Audit Report

Text of Criterion	User
Administration: Profile Maintenance	HABERSACK
Administration: Profile Maintenance	HAMID
Administration: Profile Maintenance	HOCHADEL
Administration: Profile Maintenance	HOEVERMANN
Administration: Profile Maintenance	HORSTA
Administration: Profile Maintenance	HUETT
Administration: Profile Maintenance	ID3TEST
Administration: Profile Maintenance	IDADMIN
Administration: Profile Maintenance	ISM
Administration: Profile Maintenance	KARASU
Administration: Profile Maintenance	KATZSCHNER
Administration: Profile Maintenance	KILIAN
Administration: Profile Maintenance	KIRST
Administration: Profile Maintenance	KOCHS
Administration: Profile Maintenance	KOCHUL
Administration: Profile Maintenance	KRELLJ
Administration: Profile Maintenance	KUEHN
Administration: Profile Maintenance	LANGSTON
Administration: Profile Maintenance	LCHAMDONDOG
Administration: Profile Maintenance	LEITSCH
Administration: Profile Maintenance	LEUPOLD
Administration: Profile Maintenance	LORENZ
Administration: Profile Maintenance	LORENZC
Administration: Profile Maintenance	LOTUS
Administration: Profile Maintenance	LUETKEHOFF
Administration: Profile Maintenance	MAASSBERG
Administration: Profile Maintenance	MEERWARTH
Administration: Profile Maintenance	MICHALSKY
Administration: Profile Maintenance	MIZUNO
Administration: Profile Maintenance	MONSNG
Administration: Profile Maintenance	MONUSA
Administration: Profile Maintenance	MUELLERUW
Administration: Profile Maintenance	NATZMER
Administration: Profile Maintenance	NGDCREF4

Text of Criterion	User
Administration: Profile Maintenance	NIEDEROEST
Administration: Profile Maintenance	OBERBOERSCHG
Administration: Profile Maintenance	OERDING
Administration: Profile Maintenance	OLZOG
Administration: Profile Maintenance	PALADM
Administration: Profile Maintenance	PCSETUP
Administration: Profile Maintenance	PEISL
Administration: Profile Maintenance	PETER
Administration: Profile Maintenance	PSS
Administration: Profile Maintenance	RAMOS
Administration: Profile Maintenance	RBAEIM4
Administration: Profile Maintenance	RBANK4
Administration: Profile Maintenance	RBIHANA4
Administration: Profile Maintenance	RCIO4
Administration: Profile Maintenance	RCLA4
Administration: Profile Maintenance	RCRM4
Administration: Profile Maintenance	RCSA4
Administration: Profile Maintenance	REINELTD
Administration: Profile Maintenance	RENSEL
Administration: Profile Maintenance	REPM4
Administration: Profile Maintenance	RFIGRC4
Administration: Profile Maintenance	RFIORI4
Administration: Profile Maintenance	RHANA4
Administration: Profile Maintenance	RHCM4
Administration: Profile Maintenance	RINSHC4
Administration: Profile Maintenance	RLOB4
Administration: Profile Maintenance	RMANU4
Administration: Profile Maintenance	RMOBIL4
Administration: Profile Maintenance	RPLM4
Administration: Profile Maintenance	RPS4
Administration: Profile Maintenance	RRDS4
Administration: Profile Maintenance	RRETAIL4
Administration: Profile Maintenance	RSCM4
Administration: Profile Maintenance	RSRM4

Text of Criterion	User
Administration: Profile Maintenance	RSUSTAIN4
Administration: Profile Maintenance	RUBENADM
Administration: Profile Maintenance	RUTTELC4
Administration: Profile Maintenance	SAP*
Administration: Profile Maintenance	SAPCPIC
Administration: Profile Maintenance	SAWKENG
Administration: Profile Maintenance	SCHULZET
Administration: Profile Maintenance	SDCAUTO
Administration: Profile Maintenance	SDCMONI
Administration: Profile Maintenance	SELVARAJ
Administration: Profile Maintenance	SE_DEMO_SUP
Administration: Profile Maintenance	SE_SAPADMIN
Administration: Profile Maintenance	SIMONSON
Administration: Profile Maintenance	SM_ADMIN_SMC
Administration: Profile Maintenance	STADEL
Administration: Profile Maintenance	STSADMIN
Administration: Profile Maintenance	SUPPORT
Administration: Profile Maintenance	TCSADM
Administration: Profile Maintenance	TCS_DEMO_2ND
Administration: Profile Maintenance	TCS_DEMO_SUP
Administration: Profile Maintenance	TDC
Administration: Profile Maintenance	TDC_CATT
Administration: Profile Maintenance	TDC_SAPADMIN
Administration: Profile Maintenance	TEST
Administration: Profile Maintenance	TOEWEU
Administration: Profile Maintenance	TRANS
Administration: Profile Maintenance	U4UMGMTPSS
Administration: Profile Maintenance	UPGRADE
Administration: Profile Maintenance	VEITSHANSC
Administration: Profile Maintenance	VERNAQ
Administration: Profile Maintenance	VERNITSKAJAK
Administration: Profile Maintenance	VP_SAPADMIN
Administration: Profile Maintenance	WATKINSG
Administration: Profile Maintenance	WEISSAN

System Audit Report

Text of Criterion	User
Administration: Profile Maintenance	WF-BATCH
Administration: Profile Maintenance	WORSCH
Auditing: Display Profiles	ANZEIGER
Auditing: Display Profiles	BASIS
Auditing: Display Profiles	BATIPPS
Auditing: Display Profiles	BCDEPLOY
Auditing: Display Profiles	BEZRUKOV
Auditing: Display Profiles	BLOCHING
Auditing: Display Profiles	BLUMOEHR
Auditing: Display Profiles	BOEHMA
Auditing: Display Profiles	BOLLINGER
Auditing: Display Profiles	BREINING
Auditing: Display Profiles	BRENNER
Auditing: Display Profiles	BRUNSG
Auditing: Display Profiles	BUCHERT
Auditing: Display Profiles	BUCHWALD
Auditing: Display Profiles	CCMS
Auditing: Display Profiles	COMPARE
Auditing: Display Profiles	CURA
Auditing: Display Profiles	DAVISCH
Auditing: Display Profiles	DDIC
Auditing: Display Profiles	DDICSUPPORT
Auditing: Display Profiles	DIEHL
Auditing: Display Profiles	DISANTO
Auditing: Display Profiles	DKCADM
Auditing: Display Profiles	DROESCHER
Auditing: Display Profiles	ECC_UPGR
Auditing: Display Profiles	ENTERPRISE
Auditing: Display Profiles	EX_DEMO_SUP
Auditing: Display Profiles	FISCHER
Auditing: Display Profiles	FISCHERB
Auditing: Display Profiles	FISCHERK
Auditing: Display Profiles	FORTMANN
Auditing: Display Profiles	FRICKE

System Audit Report

Text of Criterion		User
Auditing:	Display Profiles	GARBRISCH
Auditing:	Display Profiles	GAUTHIER
Auditing:	Display Profiles	GENTNERB
Auditing:	Display Profiles	GIRI
Auditing:	Display Profiles	GODZIEBA
Auditing:	Display Profiles	GONSIOR
Auditing:	Display Profiles	GRAUENHORST
Auditing:	Display Profiles	HABERSACK
Auditing:	Display Profiles	HAMID
Auditing:	Display Profiles	HOCHADEL
Auditing:	Display Profiles	HOEVERMANN
Auditing:	Display Profiles	HORSTA
Auditing:	Display Profiles	HUETT
Auditing:	Display Profiles	ID3TEST
Auditing:	Display Profiles	IDADMIN
Auditing:	Display Profiles	ISM
Auditing:	Display Profiles	KARASU
Auditing:	Display Profiles	KATZSCHNER
Auditing:	Display Profiles	KILIAN
Auditing:	Display Profiles	KIRST
Auditing:	Display Profiles	KOCHS
Auditing:	Display Profiles	KOCHUL
Auditing:	Display Profiles	KRELLJ
Auditing:	Display Profiles	KUEHN
Auditing:	Display Profiles	LANGSTON
Auditing:	Display Profiles	LCHAMDONDOG
Auditing:	Display Profiles	LEITSCH
Auditing:	Display Profiles	LEUPOLD
Auditing:	Display Profiles	LORENZ
Auditing:	Display Profiles	LORENZC
Auditing:	Display Profiles	LOTUS
Auditing:	Display Profiles	LUETKEHOFF
Auditing:	Display Profiles	MAASSBERG
Auditing:	Display Profiles	MEERWARTH

System Audit Report

Text of Criterion		User
Auditing:	Display Profiles	MICHALSKY
Auditing:	Display Profiles	MIZUNO
Auditing:	Display Profiles	MONSNG
Auditing:	Display Profiles	MONUSA
Auditing:	Display Profiles	MUELLERUW
Auditing:	Display Profiles	NATZMER
Auditing:	Display Profiles	NGDCREF4
Auditing:	Display Profiles	NIEDEROEST
Auditing:	Display Profiles	OBERBOERSCHG
Auditing:	Display Profiles	OERDING
Auditing:	Display Profiles	OLZOG
Auditing:	Display Profiles	PALADM
Auditing:	Display Profiles	PCSETUP
Auditing:	Display Profiles	PEISL
Auditing:	Display Profiles	PETER
Auditing:	Display Profiles	PITTEN
Auditing:	Display Profiles	PSS
Auditing:	Display Profiles	RAMOS
Auditing:	Display Profiles	RBAEIM4
Auditing:	Display Profiles	RBANK4
Auditing:	Display Profiles	RBIHANA4
Auditing:	Display Profiles	RCIO4
Auditing:	Display Profiles	RCLA4
Auditing:	Display Profiles	RCRM4
Auditing:	Display Profiles	RCSA4
Auditing:	Display Profiles	REINELTD
Auditing:	Display Profiles	RENSEL
Auditing:	Display Profiles	REPM4
Auditing:	Display Profiles	RFIGRC4
Auditing:	Display Profiles	RFIORI4
Auditing:	Display Profiles	RHANA4
Auditing:	Display Profiles	RHCM4
Auditing:	Display Profiles	RINSHC4
Auditing:	Display Profiles	RLOB4

System Audit Report

Text of Criterion		User
Auditing:	Display Profiles	RMANU4
Auditing:	Display Profiles	RMOBIL4
Auditing:	Display Profiles	RPLM4
Auditing:	Display Profiles	RPS4
Auditing:	Display Profiles	RRDS4
Auditing:	Display Profiles	RRETAIL4
Auditing:	Display Profiles	RSCM4
Auditing:	Display Profiles	RSRM4
Auditing:	Display Profiles	RSUSTAIN4
Auditing:	Display Profiles	RUBENADM
Auditing:	Display Profiles	RUTTELC4
Auditing:	Display Profiles	SAP*
Auditing:	Display Profiles	SAPCPIC
Auditing:	Display Profiles	SAPSUPPORT
Auditing:	Display Profiles	SAWKENG
Auditing:	Display Profiles	SCHULZET
Auditing:	Display Profiles	SDCAUTO
Auditing:	Display Profiles	SDCMONI
Auditing:	Display Profiles	SELVARAJ
Auditing:	Display Profiles	SE_DEMO_SUP
Auditing:	Display Profiles	SE_SAPADMIN
Auditing:	Display Profiles	SIMONSON
Auditing:	Display Profiles	SM_ADMIN_SMC
Auditing:	Display Profiles	STADEL
Auditing:	Display Profiles	STSADMIN
Auditing:	Display Profiles	SUPPORT
Auditing:	Display Profiles	S_A.SHOW
Auditing:	Display Profiles	TCSADM
Auditing:	Display Profiles	TCS_DEMO_2ND
Auditing:	Display Profiles	TCS_DEMO_SUP
Auditing:	Display Profiles	TDC
Auditing:	Display Profiles	TDC_CATT
Auditing:	Display Profiles	TDC_SAPADMIN
Auditing:	Display Profiles	TEST

System Audit Report

Text of Criterion	User
Auditing: Display Profiles	TOEWEU
Auditing: Display Profiles	TRANS
Auditing: Display Profiles	U4UMGMTPSS
Auditing: Display Profiles	UPGRADE
Auditing: Display Profiles	VEITSHANSC
Auditing: Display Profiles	VERNAQ
Auditing: Display Profiles	VERNITSKAJAK
Auditing: Display Profiles	VP_SAPADMIN
Auditing: Display Profiles	WATKINSG
Auditing: Display Profiles	WEISSAN
Auditing: Display Profiles	WF-BATCH
Auditing: Display Profiles	WORSCH
Administration: User Maintenance	BASIS
Administration: User Maintenance	BATIPPS
Administration: User Maintenance	BCDEPLOY
Administration: User Maintenance	BEZRUKOV
Administration: User Maintenance	BLOCHING
Administration: User Maintenance	BLUMOEHR
Administration: User Maintenance	BOEHMA
Administration: User Maintenance	BOLLINGER
Administration: User Maintenance	BREINING
Administration: User Maintenance	BRENNER
Administration: User Maintenance	BRUNSG
Administration: User Maintenance	BUCHERT
Administration: User Maintenance	BUCHWALD
Administration: User Maintenance	CCMS
Administration: User Maintenance	CURA
Administration: User Maintenance	DAVISCH
Administration: User Maintenance	DDIC
Administration: User Maintenance	DDICSUPPORT
Administration: User Maintenance	DIEHL
Administration: User Maintenance	DISANTO
Administration: User Maintenance	DKCADM
Administration: User Maintenance	DROESCHER

Text of Criterion	User
Administration: User Maintenance	ECC_UPGR
Administration: User Maintenance	ENTERPRISE
Administration: User Maintenance	EX_DEMO_SUP
Administration: User Maintenance	FISCHER
Administration: User Maintenance	FISCHERB
Administration: User Maintenance	FISCHERK
Administration: User Maintenance	FORTMANN
Administration: User Maintenance	FRICKE
Administration: User Maintenance	GARBRISCH
Administration: User Maintenance	GAUTHIER
Administration: User Maintenance	GENTNERB
Administration: User Maintenance	GIRI
Administration: User Maintenance	GODZIEBA
Administration: User Maintenance	GONSIOR
Administration: User Maintenance	GRAUENHORST
Administration: User Maintenance	HABERSACK
Administration: User Maintenance	HAMID
Administration: User Maintenance	HOCHADEL
Administration: User Maintenance	HOEVERMANN
Administration: User Maintenance	HORSTA
Administration: User Maintenance	HUETT
Administration: User Maintenance	ID3TEST
Administration: User Maintenance	IDADMIN
Administration: User Maintenance	ISM
Administration: User Maintenance	KARASU
Administration: User Maintenance	KATZSCHNER
Administration: User Maintenance	KILIAN
Administration: User Maintenance	KIRST
Administration: User Maintenance	KOCHS
Administration: User Maintenance	KOCHUL
Administration: User Maintenance	KRELLJ
Administration: User Maintenance	KUEHN
Administration: User Maintenance	LANGSTON
Administration: User Maintenance	LCHAMDONDOG

System Audit Report

Text of Criterion	User
Administration: User Maintenance	LEITSCH
Administration: User Maintenance	LEUPOLD
Administration: User Maintenance	LORENZ
Administration: User Maintenance	LORENZC
Administration: User Maintenance	LOTUS
Administration: User Maintenance	LUETKEHOFF
Administration: User Maintenance	MAASSBERG
Administration: User Maintenance	MEERWARTH
Administration: User Maintenance	MICHALSKY
Administration: User Maintenance	MIZUNO
Administration: User Maintenance	MONSNG
Administration: User Maintenance	MONUSA
Administration: User Maintenance	MUELLERUW
Administration: User Maintenance	NATZMER
Administration: User Maintenance	NGDCREF4
Administration: User Maintenance	NIEDEROEST
Administration: User Maintenance	OBERBOERSCHG
Administration: User Maintenance	OERDING
Administration: User Maintenance	OLZOG
Administration: User Maintenance	PALADM
Administration: User Maintenance	PCSETUP
Administration: User Maintenance	PEISL
Administration: User Maintenance	PETER
Administration: User Maintenance	PSS
Administration: User Maintenance	RAMOS
Administration: User Maintenance	RBAEIM4
Administration: User Maintenance	RBANK4
Administration: User Maintenance	RBIHANA4
Administration: User Maintenance	RCIO4
Administration: User Maintenance	RCLA4
Administration: User Maintenance	RCRM4
Administration: User Maintenance	RCSA4
Administration: User Maintenance	REINELTD
Administration: User Maintenance	RENSEL

Text of Criterion	User
Administration: User Maintenance	REPM4
Administration: User Maintenance	RFC_CONV
Administration: User Maintenance	RFIGRC4
Administration: User Maintenance	RFIORI4
Administration: User Maintenance	RHANA4
Administration: User Maintenance	RHCM4
Administration: User Maintenance	RINSHC4
Administration: User Maintenance	RLOB4
Administration: User Maintenance	RMANU4
Administration: User Maintenance	RMOBIL4
Administration: User Maintenance	RPLM4
Administration: User Maintenance	RPS4
Administration: User Maintenance	RRDS4
Administration: User Maintenance	RRETAIL4
Administration: User Maintenance	RSCM4
Administration: User Maintenance	RSRM4
Administration: User Maintenance	RSUSTAIN4
Administration: User Maintenance	RUBENADM
Administration: User Maintenance	RUTTELC4
Administration: User Maintenance	SAP*
Administration: User Maintenance	SAPCPIC
Administration: User Maintenance	SAWKENG
Administration: User Maintenance	SCHULZET
Administration: User Maintenance	SDCAUTO
Administration: User Maintenance	SDCMONI
Administration: User Maintenance	SELVARAJ
Administration: User Maintenance	SE_DEMO_SUP
Administration: User Maintenance	SE_SAPADMIN
Administration: User Maintenance	SIMONSON
Administration: User Maintenance	SM_ADMIN_SMC
Administration: User Maintenance	STADEL
Administration: User Maintenance	STSADMIN
Administration: User Maintenance	SUPPORT
Administration: User Maintenance	TCSADM

System Audit Report

Text of Criterion	User
Administration: User Maintenance	TCS_DEMO_2ND
Administration: User Maintenance	TCS_DEMO_SUP
Administration: User Maintenance	TDC
Administration: User Maintenance	TDC_CATT
Administration: User Maintenance	TDC_SAPADMIN
Administration: User Maintenance	TEST
Administration: User Maintenance	TOEWEU
Administration: User Maintenance	TRANS
Administration: User Maintenance	U4UMGMTPSS
Administration: User Maintenance	UPGRADE
Administration: User Maintenance	VEITSHANSC
Administration: User Maintenance	VERNAQ
Administration: User Maintenance	VERNITSKAJAK
Administration: User Maintenance	VP_SAPADMIN
Administration: User Maintenance	WATKINSG
Administration: User Maintenance	WEISSAN
Administration: User Maintenance	WF-BATCH
Administration: User Maintenance	WORSCH
Auditing: Display Users	ANZEIGER
Auditing: Display Users	BASIS
Auditing: Display Users	BATIPPS
Auditing: Display Users	BCDEPLOY
Auditing: Display Users	BEZRUKOV
Auditing: Display Users	BLOCHING
Auditing: Display Users	BLUMOEHR
Auditing: Display Users	BOEHMA
Auditing: Display Users	BOLLINGER
Auditing: Display Users	BREINING
Auditing: Display Users	BRENNER
Auditing: Display Users	BRUNSG
Auditing: Display Users	BUCHERT
Auditing: Display Users	BUCHWALD
Auditing: Display Users	CCMS
Auditing: Display Users	COMPARE

System Audit Report

Text of Criterion		User
Auditing:	Display Users	CURA
Auditing:	Display Users	DAVISCH
Auditing:	Display Users	DDIC
Auditing:	Display Users	DDICSUPPORT
Auditing:	Display Users	DIEHL
Auditing:	Display Users	DISANTO
Auditing:	Display Users	DKCADM
Auditing:	Display Users	DROESCHER
Auditing:	Display Users	ECC_UPGR
Auditing:	Display Users	ENTERPRISE
Auditing:	Display Users	EX_DEMO_SUP
Auditing:	Display Users	FISCHER
Auditing:	Display Users	FISCHERB
Auditing:	Display Users	FISCHERK
Auditing:	Display Users	FORTMANN
Auditing:	Display Users	FRICKE
Auditing:	Display Users	GARBRISCH
Auditing:	Display Users	GAUTHIER
Auditing:	Display Users	GENTNERB
Auditing:	Display Users	GIRI
Auditing:	Display Users	GODZIEBA
Auditing:	Display Users	GONSIOR
Auditing:	Display Users	GRAUENHORST
Auditing:	Display Users	HABERSACK
Auditing:	Display Users	HAMID
Auditing:	Display Users	HOCHADEL
Auditing:	Display Users	HOEVERMANN
Auditing:	Display Users	HORSTA
Auditing:	Display Users	HUETT
Auditing:	Display Users	ID3TEST
Auditing:	Display Users	IDADMIN
Auditing:	Display Users	ISM
Auditing:	Display Users	KARASU
Auditing:	Display Users	KATZSCHNER

System Audit Report

Text of Criterion		User
Auditing:	Display Users	KILIAN
Auditing:	Display Users	KIRST
Auditing:	Display Users	KOCHS
Auditing:	Display Users	KOCHUL
Auditing:	Display Users	KRELLJ
Auditing:	Display Users	KUEHN
Auditing:	Display Users	LANGSTON
Auditing:	Display Users	LCHAMDONDOG
Auditing:	Display Users	LEITSCH
Auditing:	Display Users	LEUPOLD
Auditing:	Display Users	LORENZ
Auditing:	Display Users	LORENZC
Auditing:	Display Users	LOTUS
Auditing:	Display Users	LUETKEHOFF
Auditing:	Display Users	MAASSBERG
Auditing:	Display Users	MEERWARTH
Auditing:	Display Users	MICHALSKY
Auditing:	Display Users	MIZUNO
Auditing:	Display Users	MONSNG
Auditing:	Display Users	MONUSA
Auditing:	Display Users	MUELLERUW
Auditing:	Display Users	NATZMER
Auditing:	Display Users	NGDCREF3C
Auditing:	Display Users	NGDCREF4
Auditing:	Display Users	NIEDEROEST
Auditing:	Display Users	OBERBOERSCHG
Auditing:	Display Users	OERDING
Auditing:	Display Users	OLZOG
Auditing:	Display Users	PALADM
Auditing:	Display Users	PCSETUP
Auditing:	Display Users	PEISL
Auditing:	Display Users	PETER
Auditing:	Display Users	PSS
Auditing:	Display Users	RAMOS

System Audit Report

Text of Criterion		User
Auditing:	Display Users	RBAEIM3C
Auditing:	Display Users	RBAEIM4
Auditing:	Display Users	RBANK3C
Auditing:	Display Users	RBANK4
Auditing:	Display Users	RBIHANA3C
Auditing:	Display Users	RBIHANA4
Auditing:	Display Users	RCIO3C
Auditing:	Display Users	RCIO4
Auditing:	Display Users	RCLA4
Auditing:	Display Users	RCRM3C
Auditing:	Display Users	RCRM4
Auditing:	Display Users	RCSA3C
Auditing:	Display Users	RCSA4
Auditing:	Display Users	REINELTD
Auditing:	Display Users	RENSEL
Auditing:	Display Users	REPM3C
Auditing:	Display Users	REPM4
Auditing:	Display Users	RFIGRC3C
Auditing:	Display Users	RFIGRC4
Auditing:	Display Users	RFIORI3C
Auditing:	Display Users	RFIORI4
Auditing:	Display Users	RHANA3C
Auditing:	Display Users	RHANA4
Auditing:	Display Users	RHCM3C
Auditing:	Display Users	RHCM4
Auditing:	Display Users	RINSHC3C
Auditing:	Display Users	RINSHC4
Auditing:	Display Users	RLOB3C
Auditing:	Display Users	RLOB4
Auditing:	Display Users	RMANU3C
Auditing:	Display Users	RMANU4
Auditing:	Display Users	RMOBIL3C
Auditing:	Display Users	RMOBIL4
Auditing:	Display Users	RPLM3C

System Audit Report

Text of Criterion		User
Auditing:	Display Users	RPLM4
Auditing:	Display Users	RPS3C
Auditing:	Display Users	RPS4
Auditing:	Display Users	RRDS3C
Auditing:	Display Users	RRDS4
Auditing:	Display Users	RRETAIL3C
Auditing:	Display Users	RRETAIL4
Auditing:	Display Users	RSCM3C
Auditing:	Display Users	RSCM4
Auditing:	Display Users	RSRM3C
Auditing:	Display Users	RSRM4
Auditing:	Display Users	RSUSTAIN3C
Auditing:	Display Users	RSUSTAIN4
Auditing:	Display Users	RUBENADM
Auditing:	Display Users	RUTTELC3C
Auditing:	Display Users	RUTTELC4
Auditing:	Display Users	SAP*
Auditing:	Display Users	SAPCPIC
Auditing:	Display Users	SAPSUPPORT
Auditing:	Display Users	SAWKENG
Auditing:	Display Users	SCHULZET
Auditing:	Display Users	SDCAUTO
Auditing:	Display Users	SDCMONI
Auditing:	Display Users	SELVARAJ
Auditing:	Display Users	SE_DEMO_SUP
Auditing:	Display Users	SE_MON
Auditing:	Display Users	SE_SAPADMIN
Auditing:	Display Users	SIMONSON
Auditing:	Display Users	SMTMSMD
Auditing:	Display Users	SM_ADMIN_SMC
Auditing:	Display Users	SM_SMC
Auditing:	Display Users	SM_SMD
Auditing:	Display Users	SOLMANM58001
Auditing:	Display Users	SOLMANSAM000

System Audit Report

Text of Criterion		User
Auditing:	Display Users	STADEL
Auditing:	Display Users	STSADMIN
Auditing:	Display Users	SUPPORT
Auditing:	Display Users	S_A.SHOW
Auditing:	Display Users	TCSADM
Auditing:	Display Users	TCS_DEMO_2ND
Auditing:	Display Users	TCS_DEMO_SUP
Auditing:	Display Users	TDC
Auditing:	Display Users	TDC_CATT
Auditing:	Display Users	TDC_SAPADMIN
Auditing:	Display Users	TEST
Auditing:	Display Users	TOEWEU
Auditing:	Display Users	TRANS
Auditing:	Display Users	U4UMGMTPSS
Auditing:	Display Users	UPGRADE
Auditing:	Display Users	VEITSHANSC
Auditing:	Display Users	VERNAQ
Auditing:	Display Users	VERNITSKAJAK
Auditing:	Display Users	VP_SAPADMIN
Auditing:	Display Users	WATKINSG
Auditing:	Display Users	WEISSAN
Auditing:	Display Users	WF-BATCH
Auditing:	Display Users	WORSCH
Customizing:	Table Maintenance	BASIS
Customizing:	Table Maintenance	BATIPPS
Customizing:	Table Maintenance	BCDEPLOY
Customizing:	Table Maintenance	BEZRUKOV
Customizing:	Table Maintenance	BLOCHING
Customizing:	Table Maintenance	BLUMOEHR
Customizing:	Table Maintenance	BOEHMA
Customizing:	Table Maintenance	BOLLINGER
Customizing:	Table Maintenance	BREINING
Customizing:	Table Maintenance	BRENNER
Customizing:	Table Maintenance	BRUNSG

System Audit Report

Text of Criterion	User
Customizing: Table Maintenance	BUCHERT
Customizing: Table Maintenance	BUCHWALD
Customizing: Table Maintenance	CCMS
Customizing: Table Maintenance	COMPARE
Customizing: Table Maintenance	CURA
Customizing: Table Maintenance	DAVISCH
Customizing: Table Maintenance	DDIC
Customizing: Table Maintenance	DDICSUPPORT
Customizing: Table Maintenance	DIEHL
Customizing: Table Maintenance	DISANTO
Customizing: Table Maintenance	DKCADM
Customizing: Table Maintenance	DROESCHER
Customizing: Table Maintenance	ECC_UPGR
Customizing: Table Maintenance	ENTERPRISE
Customizing: Table Maintenance	EX_DEMO_SUP
Customizing: Table Maintenance	FISCHER
Customizing: Table Maintenance	FISCHERB
Customizing: Table Maintenance	FISCHERK
Customizing: Table Maintenance	FORTMANN
Customizing: Table Maintenance	FRICKE
Customizing: Table Maintenance	GARBRISCH
Customizing: Table Maintenance	GAUTHIER
Customizing: Table Maintenance	GENTNERB
Customizing: Table Maintenance	GIRI
Customizing: Table Maintenance	GODZIEBA
Customizing: Table Maintenance	GONSIOR
Customizing: Table Maintenance	GRAUENHORST
Customizing: Table Maintenance	HABERSACK
Customizing: Table Maintenance	HAMID
Customizing: Table Maintenance	HOCHADEL
Customizing: Table Maintenance	HOEVERMANN
Customizing: Table Maintenance	HORSTA
Customizing: Table Maintenance	HUETT
Customizing: Table Maintenance	ID3TEST

System Audit Report

Text of Criterion	User
Customizing: Table Maintenance	IDADMIN
Customizing: Table Maintenance	ISM
Customizing: Table Maintenance	KARASU
Customizing: Table Maintenance	KATZSCHNER
Customizing: Table Maintenance	KILIAN
Customizing: Table Maintenance	KIRST
Customizing: Table Maintenance	KOCHS
Customizing: Table Maintenance	KOCHUL
Customizing: Table Maintenance	KRELLJ
Customizing: Table Maintenance	KUEHN
Customizing: Table Maintenance	LANGSTON
Customizing: Table Maintenance	LCHAMDONDOG
Customizing: Table Maintenance	LEITSCH
Customizing: Table Maintenance	LEUPOLD
Customizing: Table Maintenance	LORENZ
Customizing: Table Maintenance	LORENZC
Customizing: Table Maintenance	LOTUS
Customizing: Table Maintenance	LUETKEHOFF
Customizing: Table Maintenance	MAASSBERG
Customizing: Table Maintenance	MEERWARTH
Customizing: Table Maintenance	MICHALSKY
Customizing: Table Maintenance	MIZUNO
Customizing: Table Maintenance	MONSNG
Customizing: Table Maintenance	MONUSA
Customizing: Table Maintenance	MUELLERUW
Customizing: Table Maintenance	NATZMER
Customizing: Table Maintenance	NGDCREF4
Customizing: Table Maintenance	NIEDEROEST
Customizing: Table Maintenance	OBERBOERSCHG
Customizing: Table Maintenance	OERDING
Customizing: Table Maintenance	OLZOG
Customizing: Table Maintenance	PALADM
Customizing: Table Maintenance	PCSETUP
Customizing: Table Maintenance	PEISL

System Audit Report

Text of Criterion	User
Customizing: Table Maintenance	PETER
Customizing: Table Maintenance	PSS
Customizing: Table Maintenance	RAMOS
Customizing: Table Maintenance	RBAEIM4
Customizing: Table Maintenance	RBANK4
Customizing: Table Maintenance	RBIHANA4
Customizing: Table Maintenance	RCIO4
Customizing: Table Maintenance	RCLA4
Customizing: Table Maintenance	RCRM4
Customizing: Table Maintenance	RCSA4
Customizing: Table Maintenance	REINELTD
Customizing: Table Maintenance	RENSEL
Customizing: Table Maintenance	REPM4
Customizing: Table Maintenance	RFC_CONV
Customizing: Table Maintenance	RFIGRC4
Customizing: Table Maintenance	RFIORI4
Customizing: Table Maintenance	RHANA4
Customizing: Table Maintenance	RHCM4
Customizing: Table Maintenance	RINSHC4
Customizing: Table Maintenance	RLOB4
Customizing: Table Maintenance	RMANU4
Customizing: Table Maintenance	RMOBIL4
Customizing: Table Maintenance	RPLM4
Customizing: Table Maintenance	RPS4
Customizing: Table Maintenance	RRDS4
Customizing: Table Maintenance	RRETAIL4
Customizing: Table Maintenance	RSCM4
Customizing: Table Maintenance	RSRM4
Customizing: Table Maintenance	RSUSTAIN4
Customizing: Table Maintenance	RUBENADM
Customizing: Table Maintenance	RUTTELC4
Customizing: Table Maintenance	SAP*
Customizing: Table Maintenance	SAPCPIC
Customizing: Table Maintenance	SAWKENG

System Audit Report

Text of Criterion		User
Customizing:	Table Maintenance	SCHULZET
Customizing:	Table Maintenance	SDCAUTO
Customizing:	Table Maintenance	SDCMONI
Customizing:	Table Maintenance	SELVARAJ
Customizing:	Table Maintenance	SE_DEMO_SUP
Customizing:	Table Maintenance	SE_SAPADMIN
Customizing:	Table Maintenance	SIMONSON
Customizing:	Table Maintenance	SM_ADMIN_SMC
Customizing:	Table Maintenance	STADEL
Customizing:	Table Maintenance	STSADMIN
Customizing:	Table Maintenance	SUPPORT
Customizing:	Table Maintenance	TCSADM
Customizing:	Table Maintenance	TCS_DEMO_2ND
Customizing:	Table Maintenance	TCS_DEMO_SUP
Customizing:	Table Maintenance	TDC
Customizing:	Table Maintenance	TDC_CATT
Customizing:	Table Maintenance	TDC_SAPADMIN
Customizing:	Table Maintenance	TEST
Customizing:	Table Maintenance	TOEWEU
Customizing:	Table Maintenance	TRANS
Customizing:	Table Maintenance	U4UMGMTPSS
Customizing:	Table Maintenance	UPGRADE
Customizing:	Table Maintenance	VEITSHANSC
Customizing:	Table Maintenance	VERNAQ
Customizing:	Table Maintenance	VERNITSKAJAK
Customizing:	Table Maintenance	VP_SAPADMIN
Customizing:	Table Maintenance	WATKINSG
Customizing:	Table Maintenance	WEISSAN
Customizing:	Table Maintenance	WF-BATCH
Customizing:	Table Maintenance	WORSCH
Customizing:	Cross-Client Table Maintenance	BASIS
Customizing:	Cross-Client Table Maintenance	BATIPPS
Customizing:	Cross-Client Table Maintenance	BCDEPLOY
Customizing:	Cross-Client Table Maintenance	BEZRUKOV

Text of Criterion	User
Customizing: Cross-Client Table Maintenance	BLOCHING
Customizing: Cross-Client Table Maintenance	BLUMOEHR
Customizing: Cross-Client Table Maintenance	BOEHMA
Customizing: Cross-Client Table Maintenance	BOLLINGER
Customizing: Cross-Client Table Maintenance	BREINING
Customizing: Cross-Client Table Maintenance	BRENNER
Customizing: Cross-Client Table Maintenance	BRUNSG
Customizing: Cross-Client Table Maintenance	BUCHERT
Customizing: Cross-Client Table Maintenance	BUCHWALD
Customizing: Cross-Client Table Maintenance	CCMS
Customizing: Cross-Client Table Maintenance	COMPARE
Customizing: Cross-Client Table Maintenance	CURA
Customizing: Cross-Client Table Maintenance	DAVISCH
Customizing: Cross-Client Table Maintenance	DDIC
Customizing: Cross-Client Table Maintenance	DDICSUPPORT
Customizing: Cross-Client Table Maintenance	DIEHL
Customizing: Cross-Client Table Maintenance	DISANTO
Customizing: Cross-Client Table Maintenance	DKCADM
Customizing: Cross-Client Table Maintenance	DROESCHER
Customizing: Cross-Client Table Maintenance	ECC_UPGR
Customizing: Cross-Client Table Maintenance	ENTERPRISE
Customizing: Cross-Client Table Maintenance	EX_DEMO_SUP
Customizing: Cross-Client Table Maintenance	FISCHER
Customizing: Cross-Client Table Maintenance	FISCHERB
Customizing: Cross-Client Table Maintenance	FISCHERK
Customizing: Cross-Client Table Maintenance	FORTMANN
Customizing: Cross-Client Table Maintenance	FRICKE
Customizing: Cross-Client Table Maintenance	GARBRISCH
Customizing: Cross-Client Table Maintenance	GAUTHIER
Customizing: Cross-Client Table Maintenance	GENTNERB
Customizing: Cross-Client Table Maintenance	GIRI
Customizing: Cross-Client Table Maintenance	GODZIEBA
Customizing: Cross-Client Table Maintenance	GONSIOR
Customizing: Cross-Client Table Maintenance	GRAUENHORST

System Audit Report

Text of Criterion	User
Customizing: Cross-Client Table Maintenance	HABERSACK
Customizing: Cross-Client Table Maintenance	HAMID
Customizing: Cross-Client Table Maintenance	HOCHADEL
Customizing: Cross-Client Table Maintenance	HOEVERMANN
Customizing: Cross-Client Table Maintenance	HORSTA
Customizing: Cross-Client Table Maintenance	HUETT
Customizing: Cross-Client Table Maintenance	ID3TEST
Customizing: Cross-Client Table Maintenance	IDADMIN
Customizing: Cross-Client Table Maintenance	ISM
Customizing: Cross-Client Table Maintenance	KARASU
Customizing: Cross-Client Table Maintenance	KATZSCHNER
Customizing: Cross-Client Table Maintenance	KILIAN
Customizing: Cross-Client Table Maintenance	KIRST
Customizing: Cross-Client Table Maintenance	KOCHS
Customizing: Cross-Client Table Maintenance	KOCHUL
Customizing: Cross-Client Table Maintenance	KRELLJ
Customizing: Cross-Client Table Maintenance	KUEHN
Customizing: Cross-Client Table Maintenance	LANGSTON
Customizing: Cross-Client Table Maintenance	LCHAMDONDOG
Customizing: Cross-Client Table Maintenance	LEITSCH
Customizing: Cross-Client Table Maintenance	LEUPOLD
Customizing: Cross-Client Table Maintenance	LORENZ
Customizing: Cross-Client Table Maintenance	LORENZC
Customizing: Cross-Client Table Maintenance	LOTUS
Customizing: Cross-Client Table Maintenance	LUETKEHOFF
Customizing: Cross-Client Table Maintenance	MAASSBERG
Customizing: Cross-Client Table Maintenance	MEERWARTH
Customizing: Cross-Client Table Maintenance	MICHALSKY
Customizing: Cross-Client Table Maintenance	MIZUNO
Customizing: Cross-Client Table Maintenance	MONSNG
Customizing: Cross-Client Table Maintenance	MONUSA
Customizing: Cross-Client Table Maintenance	MUELLERUW
Customizing: Cross-Client Table Maintenance	NATZMER
Customizing: Cross-Client Table Maintenance	NGDCREF4

System Audit Report

Text of Criterion		User
Customizing:	Cross-Client Table Maintenance	NIEDEROEST
Customizing:	Cross-Client Table Maintenance	OBERBOERSCHG
Customizing:	Cross-Client Table Maintenance	OERDING
Customizing:	Cross-Client Table Maintenance	OLZOG
Customizing:	Cross-Client Table Maintenance	PALADM
Customizing:	Cross-Client Table Maintenance	PCSETUP
Customizing:	Cross-Client Table Maintenance	PEISL
Customizing:	Cross-Client Table Maintenance	PETER
Customizing:	Cross-Client Table Maintenance	PITTEN
Customizing:	Cross-Client Table Maintenance	PSS
Customizing:	Cross-Client Table Maintenance	RAMOS
Customizing:	Cross-Client Table Maintenance	RBAEIM4
Customizing:	Cross-Client Table Maintenance	RBANK4
Customizing:	Cross-Client Table Maintenance	RBIHANA4
Customizing:	Cross-Client Table Maintenance	RCIO4
Customizing:	Cross-Client Table Maintenance	RCLA4
Customizing:	Cross-Client Table Maintenance	RCRM4
Customizing:	Cross-Client Table Maintenance	RCSA4
Customizing:	Cross-Client Table Maintenance	REINELTD
Customizing:	Cross-Client Table Maintenance	RENSEL
Customizing:	Cross-Client Table Maintenance	REPM4
Customizing:	Cross-Client Table Maintenance	RFC_CONV
Customizing:	Cross-Client Table Maintenance	RFIGRC4
Customizing:	Cross-Client Table Maintenance	RFIORI4
Customizing:	Cross-Client Table Maintenance	RHANA4
Customizing:	Cross-Client Table Maintenance	RHCM4
Customizing:	Cross-Client Table Maintenance	RINSHC4
Customizing:	Cross-Client Table Maintenance	RLOB4
Customizing:	Cross-Client Table Maintenance	RMANU4
Customizing:	Cross-Client Table Maintenance	RMOBIL4
Customizing:	Cross-Client Table Maintenance	RPLM4
Customizing:	Cross-Client Table Maintenance	RPS4
Customizing:	Cross-Client Table Maintenance	RRDS4
Customizing:	Cross-Client Table Maintenance	RRETAIL4

System Audit Report

Text of Criterion	User
Customizing: Cross-Client Table Maintenance	RSCM4
Customizing: Cross-Client Table Maintenance	RSRM4
Customizing: Cross-Client Table Maintenance	RSUSTAIN4
Customizing: Cross-Client Table Maintenance	RUBENADM
Customizing: Cross-Client Table Maintenance	RUTTELC4
Customizing: Cross-Client Table Maintenance	SAP*
Customizing: Cross-Client Table Maintenance	SAPCPIC
Customizing: Cross-Client Table Maintenance	SAWKENG
Customizing: Cross-Client Table Maintenance	SCHULZET
Customizing: Cross-Client Table Maintenance	SDCAUTO
Customizing: Cross-Client Table Maintenance	SDCMONI
Customizing: Cross-Client Table Maintenance	SELVARAJ
Customizing: Cross-Client Table Maintenance	SE_DEMO_SUP
Customizing: Cross-Client Table Maintenance	SE_SAPADMIN
Customizing: Cross-Client Table Maintenance	SIMONSON
Customizing: Cross-Client Table Maintenance	SMTMSMD
Customizing: Cross-Client Table Maintenance	SM_ADMIN_SMC
Customizing: Cross-Client Table Maintenance	SM_SMC
Customizing: Cross-Client Table Maintenance	SM_SMD
Customizing: Cross-Client Table Maintenance	SOLMANM58001
Customizing: Cross-Client Table Maintenance	SOLMANSAM000
Customizing: Cross-Client Table Maintenance	STADEL
Customizing: Cross-Client Table Maintenance	STSADMIN
Customizing: Cross-Client Table Maintenance	SUPPORT
Customizing: Cross-Client Table Maintenance	TCSADM
Customizing: Cross-Client Table Maintenance	TCS_DEMO_2ND
Customizing: Cross-Client Table Maintenance	TCS_DEMO_SUP
Customizing: Cross-Client Table Maintenance	TDC
Customizing: Cross-Client Table Maintenance	TDC_CATT
Customizing: Cross-Client Table Maintenance	TDC_SAPADMIN
Customizing: Cross-Client Table Maintenance	TEST
Customizing: Cross-Client Table Maintenance	TOEWEU
Customizing: Cross-Client Table Maintenance	TRANS
Customizing: Cross-Client Table Maintenance	U4UMGMTPSS

System Audit Report

Text of Criterion		User
Customizing:	Cross-Client Table Maintenance	UPGRADE
Customizing:	Cross-Client Table Maintenance	VEITSHANSC
Customizing:	Cross-Client Table Maintenance	VERNAQ
Customizing:	Cross-Client Table Maintenance	VERNITSKAJAK
Customizing:	Cross-Client Table Maintenance	VP_SAPADMIN
Customizing:	Cross-Client Table Maintenance	WATKINSG
Customizing:	Cross-Client Table Maintenance	WEISSAN
Customizing:	Cross-Client Table Maintenance	WF-BATCH
Customizing:	Cross-Client Table Maintenance	WORSCH
Customizing:	Table Maintenance of All Basic Tables	BASIS
Customizing:	Table Maintenance of All Basic Tables	BATIPPS
Customizing:	Table Maintenance of All Basic Tables	BCDEPLOY
Customizing:	Table Maintenance of All Basic Tables	BEZRUKOV
Customizing:	Table Maintenance of All Basic Tables	BLOCHING
Customizing:	Table Maintenance of All Basic Tables	BLUMOEHR
Customizing:	Table Maintenance of All Basic Tables	BOEHMA
Customizing:	Table Maintenance of All Basic Tables	BOLLINGER
Customizing:	Table Maintenance of All Basic Tables	BREINING
Customizing:	Table Maintenance of All Basic Tables	BRENNER
Customizing:	Table Maintenance of All Basic Tables	BRUNSG
Customizing:	Table Maintenance of All Basic Tables	BUCHERT
Customizing:	Table Maintenance of All Basic Tables	BUCHWALD
Customizing:	Table Maintenance of All Basic Tables	CCMS
Customizing:	Table Maintenance of All Basic Tables	COMPARE
Customizing:	Table Maintenance of All Basic Tables	CURA
Customizing:	Table Maintenance of All Basic Tables	DAVISCH
Customizing:	Table Maintenance of All Basic Tables	DDIC
Customizing:	Table Maintenance of All Basic Tables	DDICSUPPORT
Customizing:	Table Maintenance of All Basic Tables	DIEHL
Customizing:	Table Maintenance of All Basic Tables	DISANTO
Customizing:	Table Maintenance of All Basic Tables	DKCADM
Customizing:	Table Maintenance of All Basic Tables	DROESCHER
Customizing:	Table Maintenance of All Basic Tables	ECC_UPGR
Customizing:	Table Maintenance of All Basic Tables	ENTERPRISE

System Audit Report

Text of Criterion		User
Customizing:	Table Maintenance of All Basic Tables	EX_DEMO_SUP
Customizing:	Table Maintenance of All Basic Tables	FISCHER
Customizing:	Table Maintenance of All Basic Tables	FISCHERB
Customizing:	Table Maintenance of All Basic Tables	FISCHERK
Customizing:	Table Maintenance of All Basic Tables	FORTMANN
Customizing:	Table Maintenance of All Basic Tables	FRICKE
Customizing:	Table Maintenance of All Basic Tables	GARBRISCH
Customizing:	Table Maintenance of All Basic Tables	GAUTHIER
Customizing:	Table Maintenance of All Basic Tables	GENTNERB
Customizing:	Table Maintenance of All Basic Tables	GIRI
Customizing:	Table Maintenance of All Basic Tables	GODZIEBA
Customizing:	Table Maintenance of All Basic Tables	GONSIOR
Customizing:	Table Maintenance of All Basic Tables	GRAUENHORST
Customizing:	Table Maintenance of All Basic Tables	HABERSACK
Customizing:	Table Maintenance of All Basic Tables	HAMID
Customizing:	Table Maintenance of All Basic Tables	HOCHADEL
Customizing:	Table Maintenance of All Basic Tables	HOEVERMANN
Customizing:	Table Maintenance of All Basic Tables	HORSTA
Customizing:	Table Maintenance of All Basic Tables	HUETT
Customizing:	Table Maintenance of All Basic Tables	ID3TEST
Customizing:	Table Maintenance of All Basic Tables	IDADMIN
Customizing:	Table Maintenance of All Basic Tables	ISM
Customizing:	Table Maintenance of All Basic Tables	KARASU
Customizing:	Table Maintenance of All Basic Tables	KATZSCHNER
Customizing:	Table Maintenance of All Basic Tables	KILIAN
Customizing:	Table Maintenance of All Basic Tables	KIRST
Customizing:	Table Maintenance of All Basic Tables	KOCHS
Customizing:	Table Maintenance of All Basic Tables	KOCHUL
Customizing:	Table Maintenance of All Basic Tables	KRELLJ
Customizing:	Table Maintenance of All Basic Tables	KUEHN
Customizing:	Table Maintenance of All Basic Tables	LANGSTON
Customizing:	Table Maintenance of All Basic Tables	LCHAMDONDOG
Customizing:	Table Maintenance of All Basic Tables	LEITSCH
Customizing:	Table Maintenance of All Basic Tables	LEUPOLD

System Audit Report

Text of Criterion		User
Customizing:	Table Maintenance of All Basic Tables	LORENZ
Customizing:	Table Maintenance of All Basic Tables	LORENZC
Customizing:	Table Maintenance of All Basic Tables	LOTUS
Customizing:	Table Maintenance of All Basic Tables	LUETKEHOFF
Customizing:	Table Maintenance of All Basic Tables	MAASSBERG
Customizing:	Table Maintenance of All Basic Tables	MEERWARTH
Customizing:	Table Maintenance of All Basic Tables	MICHALSKY
Customizing:	Table Maintenance of All Basic Tables	MIZUNO
Customizing:	Table Maintenance of All Basic Tables	MONSNG
Customizing:	Table Maintenance of All Basic Tables	MONUSA
Customizing:	Table Maintenance of All Basic Tables	MUELLERUW
Customizing:	Table Maintenance of All Basic Tables	NATZMER
Customizing:	Table Maintenance of All Basic Tables	NGDCREF4
Customizing:	Table Maintenance of All Basic Tables	NIEDEROEST
Customizing:	Table Maintenance of All Basic Tables	OBERBOERSCHG
Customizing:	Table Maintenance of All Basic Tables	OERDING
Customizing:	Table Maintenance of All Basic Tables	OLZOG
Customizing:	Table Maintenance of All Basic Tables	PALADM
Customizing:	Table Maintenance of All Basic Tables	PCSETUP
Customizing:	Table Maintenance of All Basic Tables	PEISL
Customizing:	Table Maintenance of All Basic Tables	PETER
Customizing:	Table Maintenance of All Basic Tables	PSS
Customizing:	Table Maintenance of All Basic Tables	RAMOS
Customizing:	Table Maintenance of All Basic Tables	RBAEIM4
Customizing:	Table Maintenance of All Basic Tables	RBANK4
Customizing:	Table Maintenance of All Basic Tables	RBIHANA4
Customizing:	Table Maintenance of All Basic Tables	RCIO4
Customizing:	Table Maintenance of All Basic Tables	RCLA4
Customizing:	Table Maintenance of All Basic Tables	RCRM4
Customizing:	Table Maintenance of All Basic Tables	RCSA4
Customizing:	Table Maintenance of All Basic Tables	REINELTD
Customizing:	Table Maintenance of All Basic Tables	RENSEL
Customizing:	Table Maintenance of All Basic Tables	REPM4
Customizing:	Table Maintenance of All Basic Tables	RFC_CONV

Text of Criterion		User
Customizing:	Table Maintenance of All Basic Tables	RFIGRC4
Customizing:	Table Maintenance of All Basic Tables	RFIORI4
Customizing:	Table Maintenance of All Basic Tables	RHANA4
Customizing:	Table Maintenance of All Basic Tables	RHCM4
Customizing:	Table Maintenance of All Basic Tables	RINSHC4
Customizing:	Table Maintenance of All Basic Tables	RLOB4
Customizing:	Table Maintenance of All Basic Tables	RMANU4
Customizing:	Table Maintenance of All Basic Tables	RMOBIL4
Customizing:	Table Maintenance of All Basic Tables	RPLM4
Customizing:	Table Maintenance of All Basic Tables	RPS4
Customizing:	Table Maintenance of All Basic Tables	RRDS4
Customizing:	Table Maintenance of All Basic Tables	RRETAIL4
Customizing:	Table Maintenance of All Basic Tables	RSCM4
Customizing:	Table Maintenance of All Basic Tables	RSRM4
Customizing:	Table Maintenance of All Basic Tables	RSUSTAIN4
Customizing:	Table Maintenance of All Basic Tables	RUBENADM
Customizing:	Table Maintenance of All Basic Tables	RUTTELC4
Customizing:	Table Maintenance of All Basic Tables	SAP*
Customizing:	Table Maintenance of All Basic Tables	SAPCPIC
Customizing:	Table Maintenance of All Basic Tables	SAWKENG
Customizing:	Table Maintenance of All Basic Tables	SCHULZET
Customizing:	Table Maintenance of All Basic Tables	SDCAUTO
Customizing:	Table Maintenance of All Basic Tables	SDCMONI
Customizing:	Table Maintenance of All Basic Tables	SELVARAJ
Customizing:	Table Maintenance of All Basic Tables	SE_DEMO_SUP
Customizing:	Table Maintenance of All Basic Tables	SE_SAPADMIN
Customizing:	Table Maintenance of All Basic Tables	SIMONSON
Customizing:	Table Maintenance of All Basic Tables	SM_ADMIN_SMC
Customizing:	Table Maintenance of All Basic Tables	STADEL
Customizing:	Table Maintenance of All Basic Tables	STSADMIN
Customizing:	Table Maintenance of All Basic Tables	SUPPORT
Customizing:	Table Maintenance of All Basic Tables	TCSADM
Customizing:	Table Maintenance of All Basic Tables	TCS_DEMO_2ND
Customizing:	Table Maintenance of All Basic Tables	TCS_DEMO_SUP

Text of Criterion	User
Customizing: Table Maintenance of All Basic Tables	TDC
Customizing: Table Maintenance of All Basic Tables	TDC_CATT
Customizing: Table Maintenance of All Basic Tables	TDC_SAPADMIN
Customizing: Table Maintenance of All Basic Tables	TEST
Customizing: Table Maintenance of All Basic Tables	TOEWEU
Customizing: Table Maintenance of All Basic Tables	TRANS
Customizing: Table Maintenance of All Basic Tables	U4UMGMTPSS
Customizing: Table Maintenance of All Basic Tables	UPGRADE
Customizing: Table Maintenance of All Basic Tables	VEITSHANSC
Customizing: Table Maintenance of All Basic Tables	VERNAQ
Customizing: Table Maintenance of All Basic Tables	VERNITSKAJAK
Customizing: Table Maintenance of All Basic Tables	VP_SAPADMIN
Customizing: Table Maintenance of All Basic Tables	WATKINSG
Customizing: Table Maintenance of All Basic Tables	WEISSAN
Customizing: Table Maintenance of All Basic Tables	WF-BATCH
Customizing: Table Maintenance of All Basic Tables	WORSCH
Development: Program and ABAP Dictionary Maintenance	BASIS
Development: Program and ABAP Dictionary Maintenance	BATIPPS
Development: Program and ABAP Dictionary Maintenance	BCDEPLOY
Development: Program and ABAP Dictionary Maintenance	BEZRUKOV
Development: Program and ABAP Dictionary Maintenance	BLOCHING
Development: Program and ABAP Dictionary Maintenance	BLUMOEHR
Development: Program and ABAP Dictionary Maintenance	BOEHMA
Development: Program and ABAP Dictionary Maintenance	BOLLINGER
Development: Program and ABAP Dictionary Maintenance	BREINING
Development: Program and ABAP Dictionary Maintenance	BRENNER
Development: Program and ABAP Dictionary Maintenance	BRUNSG
Development: Program and ABAP Dictionary Maintenance	BUCHERT
Development: Program and ABAP Dictionary Maintenance	BUCHWALD
Development: Program and ABAP Dictionary Maintenance	CCMS
Development: Program and ABAP Dictionary Maintenance	CURA
Development: Program and ABAP Dictionary Maintenance	DAVISCH
Development: Program and ABAP Dictionary Maintenance	DDIC
Development: Program and ABAP Dictionary Maintenance	DDICSUPPORT

Text of Criterion	User
Development: Program and ABAP Dictionary Maintenance	DIEHL
Development: Program and ABAP Dictionary Maintenance	DISANTO
Development: Program and ABAP Dictionary Maintenance	DKCADM
Development: Program and ABAP Dictionary Maintenance	DROESCHER
Development: Program and ABAP Dictionary Maintenance	ECC_UPGR
Development: Program and ABAP Dictionary Maintenance	ENTERPRISE
Development: Program and ABAP Dictionary Maintenance	EX_DEMO_SUP
Development: Program and ABAP Dictionary Maintenance	FISCHER
Development: Program and ABAP Dictionary Maintenance	FISCHERB
Development: Program and ABAP Dictionary Maintenance	FISCHERK
Development: Program and ABAP Dictionary Maintenance	FORTMANN
Development: Program and ABAP Dictionary Maintenance	FRICKE
Development: Program and ABAP Dictionary Maintenance	GARBRISCH
Development: Program and ABAP Dictionary Maintenance	GAUTHIER
Development: Program and ABAP Dictionary Maintenance	GENTNERB
Development: Program and ABAP Dictionary Maintenance	GIRI
Development: Program and ABAP Dictionary Maintenance	GODZIEBA
Development: Program and ABAP Dictionary Maintenance	GONSIOR
Development: Program and ABAP Dictionary Maintenance	GRAUENHORST
Development: Program and ABAP Dictionary Maintenance	HABERSACK
Development: Program and ABAP Dictionary Maintenance	HAMID
Development: Program and ABAP Dictionary Maintenance	HOCHADEL
Development: Program and ABAP Dictionary Maintenance	HOEVERMANN
Development: Program and ABAP Dictionary Maintenance	HORSTA
Development: Program and ABAP Dictionary Maintenance	HUETT
Development: Program and ABAP Dictionary Maintenance	ID3TEST
Development: Program and ABAP Dictionary Maintenance	IDADMIN
Development: Program and ABAP Dictionary Maintenance	ISM
Development: Program and ABAP Dictionary Maintenance	KARASU
Development: Program and ABAP Dictionary Maintenance	KATZSCHNER
Development: Program and ABAP Dictionary Maintenance	KILIAN
Development: Program and ABAP Dictionary Maintenance	KIRST
Development: Program and ABAP Dictionary Maintenance	KOCHS
Development: Program and ABAP Dictionary Maintenance	KOCHUL

System Audit Report

Text of Criterion		User
Development:	Program and ABAP Dictionary Maintenance	KRELLJ
Development:	Program and ABAP Dictionary Maintenance	KUEHN
Development:	Program and ABAP Dictionary Maintenance	LANGSTON
Development:	Program and ABAP Dictionary Maintenance	LCHAMDONDOG
Development:	Program and ABAP Dictionary Maintenance	LEITSCH
Development:	Program and ABAP Dictionary Maintenance	LEUPOLD
Development:	Program and ABAP Dictionary Maintenance	LORENZ
Development:	Program and ABAP Dictionary Maintenance	LORENZC
Development:	Program and ABAP Dictionary Maintenance	LOTUS
Development:	Program and ABAP Dictionary Maintenance	LUETKEHOFF
Development:	Program and ABAP Dictionary Maintenance	MAASSBERG
Development:	Program and ABAP Dictionary Maintenance	MEERWARTH
Development:	Program and ABAP Dictionary Maintenance	MICHALSKY
Development:	Program and ABAP Dictionary Maintenance	MIZUNO
Development:	Program and ABAP Dictionary Maintenance	MONSNG
Development:	Program and ABAP Dictionary Maintenance	MONUSA
Development:	Program and ABAP Dictionary Maintenance	MUELLERUW
Development:	Program and ABAP Dictionary Maintenance	NATZMER
Development:	Program and ABAP Dictionary Maintenance	NGDCREF4
Development:	Program and ABAP Dictionary Maintenance	NIEDEROEST
Development:	Program and ABAP Dictionary Maintenance	OBERBOERSCHG
Development:	Program and ABAP Dictionary Maintenance	OERDING
Development:	Program and ABAP Dictionary Maintenance	OLZOG
Development:	Program and ABAP Dictionary Maintenance	PALADM
Development:	Program and ABAP Dictionary Maintenance	PCSETUP
Development:	Program and ABAP Dictionary Maintenance	PEISL
Development:	Program and ABAP Dictionary Maintenance	PETER
Development:	Program and ABAP Dictionary Maintenance	PSS
Development:	Program and ABAP Dictionary Maintenance	RAMOS
Development:	Program and ABAP Dictionary Maintenance	RBAEIM4
Development:	Program and ABAP Dictionary Maintenance	RBANK4
Development:	Program and ABAP Dictionary Maintenance	RBIHANA4
Development:	Program and ABAP Dictionary Maintenance	RCIO4
Development:	Program and ABAP Dictionary Maintenance	RCLA4

Text of Criterion	User
Development: Program and ABAP Dictionary Maintenance	RCRM4
Development: Program and ABAP Dictionary Maintenance	RCSA4
Development: Program and ABAP Dictionary Maintenance	REINELTD
Development: Program and ABAP Dictionary Maintenance	RENSEL
Development: Program and ABAP Dictionary Maintenance	REPM4
Development: Program and ABAP Dictionary Maintenance	RFIGRC4
Development: Program and ABAP Dictionary Maintenance	RFIORI4
Development: Program and ABAP Dictionary Maintenance	RHANA4
Development: Program and ABAP Dictionary Maintenance	RHCM4
Development: Program and ABAP Dictionary Maintenance	RINSHC4
Development: Program and ABAP Dictionary Maintenance	RLOB4
Development: Program and ABAP Dictionary Maintenance	RMANU4
Development: Program and ABAP Dictionary Maintenance	RMOBIL4
Development: Program and ABAP Dictionary Maintenance	RPLM4
Development: Program and ABAP Dictionary Maintenance	RPS4
Development: Program and ABAP Dictionary Maintenance	RRDS4
Development: Program and ABAP Dictionary Maintenance	RRETAIL4
Development: Program and ABAP Dictionary Maintenance	RSCM4
Development: Program and ABAP Dictionary Maintenance	RSRM4
Development: Program and ABAP Dictionary Maintenance	RSUSTAIN4
Development: Program and ABAP Dictionary Maintenance	RUBENADM
Development: Program and ABAP Dictionary Maintenance	RUTTELC4
Development: Program and ABAP Dictionary Maintenance	SAP*
Development: Program and ABAP Dictionary Maintenance	SAPCPIC
Development: Program and ABAP Dictionary Maintenance	SAWKENG
Development: Program and ABAP Dictionary Maintenance	SCHULZET
Development: Program and ABAP Dictionary Maintenance	SDCAUTO
Development: Program and ABAP Dictionary Maintenance	SDCMONI
Development: Program and ABAP Dictionary Maintenance	SELVARAJ
Development: Program and ABAP Dictionary Maintenance	SE_DEMO_SUP
Development: Program and ABAP Dictionary Maintenance	SE_SAPADMIN
Development: Program and ABAP Dictionary Maintenance	SIMONSON
Development: Program and ABAP Dictionary Maintenance	STADEL
Development: Program and ABAP Dictionary Maintenance	STSADMIN

Text of Criterion		User
Development:	Program and ABAP Dictionary Maintenance	SUPPORT
Development:	Program and ABAP Dictionary Maintenance	TCSADM
Development:	Program and ABAP Dictionary Maintenance	TCS_DEMO_2ND
Development:	Program and ABAP Dictionary Maintenance	TCS_DEMO_SUP
Development:	Program and ABAP Dictionary Maintenance	TDC
Development:	Program and ABAP Dictionary Maintenance	TDC_CATT
Development:	Program and ABAP Dictionary Maintenance	TDC_SAPADMIN
Development:	Program and ABAP Dictionary Maintenance	TEST
Development:	Program and ABAP Dictionary Maintenance	TOEWEU
Development:	Program and ABAP Dictionary Maintenance	TRANS
Development:	Program and ABAP Dictionary Maintenance	U4UMGMTPSS
Development:	Program and ABAP Dictionary Maintenance	UPGRADE
Development:	Program and ABAP Dictionary Maintenance	VEITSHANSC
Development:	Program and ABAP Dictionary Maintenance	VERNAQ
Development:	Program and ABAP Dictionary Maintenance	VERNITSKAJAK
Development:	Program and ABAP Dictionary Maintenance	VP_SAPADMIN
Development:	Program and ABAP Dictionary Maintenance	WATKINSG
Development:	Program and ABAP Dictionary Maintenance	WEISSAN
Development:	Program and ABAP Dictionary Maintenance	WF-BATCH
Development:	Program and ABAP Dictionary Maintenance	WORSCH
Development:	Transport System	BASIS
Development:	Transport System	BATIPPS
Development:	Transport System	BCDEPLOY
Development:	Transport System	BEZRUKOV
Development:	Transport System	BLOCHING
Development:	Transport System	BLUMOEHR
Development:	Transport System	BOEHMA
Development:	Transport System	BOLLINGER
Development:	Transport System	BREINING
Development:	Transport System	BRENNER
Development:	Transport System	BRUNSG
Development:	Transport System	BUCHERT
Development:	Transport System	BUCHWALD
Development:	Transport System	CCMS

System Audit Report

Text of Criterion	User
Development: Transport System	CURA
Development: Transport System	DAVISCH
Development: Transport System	DDIC
Development: Transport System	DDICSUPPORT
Development: Transport System	DIEHL
Development: Transport System	DISANTO
Development: Transport System	DKCADM
Development: Transport System	DROESCHER
Development: Transport System	ECC_UPGR
Development: Transport System	ENTERPRISE
Development: Transport System	EX_DEMO_SUP
Development: Transport System	FISCHER
Development: Transport System	FISCHERB
Development: Transport System	FISCHERK
Development: Transport System	FORTMANN
Development: Transport System	FRICKE
Development: Transport System	GARBRISCH
Development: Transport System	GAUTHIER
Development: Transport System	GENTNERB
Development: Transport System	GIRI
Development: Transport System	GODZIEBA
Development: Transport System	GONSIOR
Development: Transport System	GRAUENHORST
Development: Transport System	HABERSACK
Development: Transport System	HAMID
Development: Transport System	HOCHADEL
Development: Transport System	HOEVERMANN
Development: Transport System	HORSTA
Development: Transport System	HUETT
Development: Transport System	ID3TEST
Development: Transport System	IDADMIN
Development: Transport System	ISM
Development: Transport System	KARASU
Development: Transport System	KATZSCHNER

System Audit Report

Text of Criterion	User
Development: Transport System	KILIAN
Development: Transport System	KIRST
Development: Transport System	KOCHS
Development: Transport System	KOCHUL
Development: Transport System	KRELLJ
Development: Transport System	KUEHN
Development: Transport System	LANGSTON
Development: Transport System	LCHAMDONDOG
Development: Transport System	LEITSCH
Development: Transport System	LEUPOLD
Development: Transport System	LORENZ
Development: Transport System	LORENZC
Development: Transport System	LOTUS
Development: Transport System	LUETKEHOFF
Development: Transport System	MAASSBERG
Development: Transport System	MEERWARTH
Development: Transport System	MICHALSKY
Development: Transport System	MIZUNO
Development: Transport System	MONSNG
Development: Transport System	MONUSA
Development: Transport System	MUELLERUW
Development: Transport System	NATZMER
Development: Transport System	NGDCREF4
Development: Transport System	NIEDEROEST
Development: Transport System	OBERBOERSCHG
Development: Transport System	OERDING
Development: Transport System	OLZOG
Development: Transport System	PALADM
Development: Transport System	PCSETUP
Development: Transport System	PEISL
Development: Transport System	PETER
Development: Transport System	PSS
Development: Transport System	RAMOS
Development: Transport System	RBAEIM4

System Audit Report

Text of Criterion	User
Development: Transport System	RBANK4
Development: Transport System	RBIHANA4
Development: Transport System	RCIO4
Development: Transport System	RCLA4
Development: Transport System	RCRM4
Development: Transport System	RCSA4
Development: Transport System	REINELTD
Development: Transport System	RENSEL
Development: Transport System	REPM4
Development: Transport System	RFIGRC4
Development: Transport System	RFIORI4
Development: Transport System	RHANA4
Development: Transport System	RHCM4
Development: Transport System	RINSHC4
Development: Transport System	RLOB4
Development: Transport System	RMANU4
Development: Transport System	RMOBIL4
Development: Transport System	RPLM4
Development: Transport System	RPS4
Development: Transport System	RRDS4
Development: Transport System	RRETAIL4
Development: Transport System	RSCM4
Development: Transport System	RSRM4
Development: Transport System	RSUSTAIN4
Development: Transport System	RUBENADM
Development: Transport System	RUTTELC4
Development: Transport System	SAP*
Development: Transport System	SAPCPIC
Development: Transport System	SAWKENG
Development: Transport System	SCHULZET
Development: Transport System	SDCAUTO
Development: Transport System	SDCMONI
Development: Transport System	SELVARAJ
Development: Transport System	SE_DEMO_SUP

System Audit Report

Text of Criterion	User
Development: Transport System	SE_SAPADMIN
Development: Transport System	SIMONSON
Development: Transport System	SMTMSMD
Development: Transport System	STADEL
Development: Transport System	STSADMIN
Development: Transport System	SUPPORT
Development: Transport System	TCSADM
Development: Transport System	TCS_DEMO_2ND
Development: Transport System	TCS_DEMO_SUP
Development: Transport System	TDC
Development: Transport System	TDC_CATT
Development: Transport System	TDC_SAPADMIN
Development: Transport System	TEST
Development: Transport System	TOEWEU
Development: Transport System	TRANS
Development: Transport System	U4UMGMTPSS
Development: Transport System	UPGRADE
Development: Transport System	VEITSHANSC
Development: Transport System	VERNAQ
Development: Transport System	VERNITSKAJAK
Development: Transport System	VP_SAPADMIN
Development: Transport System	WATKINSG
Development: Transport System	WEISSAN
Development: Transport System	WF-BATCH
Development: Transport System	WORSCH

Página intencionalmente deixada em branco.