



**PROGRAMA DE MESTRADO EM
GESTÃO DE RECURSOS HUMANOS**

**MANUAL DE ORIENTAÇÃO DE
SISTEMAS DE INFORMAÇÃO EM RECURSOS HUMANOS**

ENSINO ONLINE. ENSINO COM FUTURO

2026

**PROGRAMA DE MESTRADO EM
MESTRADO EM GESTÃO DE RECURSOS HUMANOS**

**MANUAL DE ORIENTAÇÃO DE
SISTEMAS DE INFORMAÇÃO EM RECURSOS HUMANOS**

1º ANO

CÓDIGO CFG-PG- ISCED-022

TOTAL HORAS/2º SEMESTRE 200

CRÉDITOS (SNATCA) 6

NÚMERO DE TEMAS 3

Direitos de autor (copyright)

Este manual é propriedade da Universidade Aberta ISCED (UnISCED), à qual se reservam todos os direitos. É proibida a sua duplicação ou reprodução, parcial ou total, sob quaisquer formas ou por quaisquer meios (eletrónico, mecânico, gravação, fotocópia ou outros), sem a permissão expressa da entidade editora UnISCED.

Pela não observância do acima estipulado, o infractor é passível de aplicação de processos judiciais de acordo com a legislação em vigor no país.

Universidade Aberta ISCED (UnISCED)

Faculdade de Economia e Gestão

Rua Carlos Pereira, parcela n.º 148/07, Estoril-Expansão, Cidade da Beira

Telf.: (+258) 84 0943 449

E-mail: faculdade@unisced.edu.mz

Website: <https://unisced.edu.mz/>

Agradecimentos

A Universidade Aberta ISCED (UnISCED) e o autor do presente manual agradecem a colaboração dos seguintes indivíduos e instituições:

Pela coordenação	Vice-Reitoria Académica da UnISCED
Pelo <i>design</i>	Direcção de Desenvolvimento Curricular e Produção de Materiais de Estudo
Financiamento e logística	UnISCED
Pela revisão	Direcção de Desenvolvimento Curricular e Produção de Materiais de Estudo
Ano de publicação	2026
Ano de actualização	2026
Local de publicação	Cidade da Beira

Elaborado por:

Stefan Mussa PhD

Índice

Visão geral	7
Introdução Geral	8
Objectivo geral da disciplina	9
Conteúdo da Disciplina	10
Apoio, dúvidas e reclamações	12
Avaliação	13
Originalidade e Plágio	14
Prefácio	15
Competências a Desenvolver	16
Metodologia de Estudo	17
Unidade I – sistemas de informação	18
1.1 Conceito de Sistemas de Informação	18
1.2 Componentes dos Sistemas de Informação	20
1.3 Tipos de Sistemas de Informação	22
1.4 Sistemas de Informação em Recursos Humanos (SIRH)	24
Conclusão do Capítulo I	27
Perguntas de Avaliação	28
Unidade II – Gestão de dados	30
2.1 Conceito de Gestão de Dados	30
2.2 Ciclo de Vida dos Dados	32
2.3 Bases de Dados	34
2.5 Gestão de Dados em Recursos Humanos	37
2.6 Ética e Proteção de Dados	38
Conclusão do Capítulo II	39
Perguntas de Avaliação	40
Unidade III – Gestão de segurança	43
3.1 Conceito de Segurança da Informação	44
3.3 Riscos e Ameaças Informáticas	46
3.4 Políticas de Segurança da Informação	47

3.5 Segurança da Informação em Recursos Humanos.....	48
3.6 Tecnologias de Segurança	49
3.7 Gestão de Incidentes e Continuidade	50
Conclusão do Capítulo III	51
Perguntas de Avaliação	52
IV-Sistema de Informação em Gestão de Recursos Humanos.....	55
4.1 O SIRH como Parceiro Estratégico da Organização	55
4.2 Integração do SIRH com Outros Sistemas Organizacionais	55
4.3 Inteligência Artificial e Automação no SIRH.....	56
4.4 Transformação Digital da Função de RH através do SIRH	57
4.5 Métricas e KPIs de RH Suportados pelo SIRH	57
4.6 Tendências Emergentes nos SIRH (2025–2030).....	59
4.7 Conclusão do Capítulo IV	60
Perguntas de Avaliação	60
Questões de Escolha Múltipla	60
Questões de Verdadeiro ou Falso	61
Conclusões Gerais do Manual.....	62
Glossário Técnico	63
Referências Bibliográficas	64

Bem Vindo à Disciplina de Sistemas de Informação em Recursos Humanos (SIRH)

O presente manual foi concebido para servir como um recurso didático e científico fundamental para estudantes de Mestrado em Gestão de Recursos Humanos, com foco na disciplina de Sistemas de Informação em Recursos Humanos (SIRH). Numa era de transformação digital acelerada, a gestão eficaz dos recursos humanos é indissociável da utilização estratégica de tecnologias de informação. Este trabalho visa preencher a lacuna entre a teoria académica e a aplicação prática, fornecendo uma base sólida para a compreensão, implementação e gestão de SIRH em contextos organizacionais complexos. A abordagem crítica e a fundamentação científica são pilares deste manual, incentivando os leitores a desenvolverem uma perspetiva analítica e inovadora sobre o papel da tecnologia na gestão de pessoas.

Introdução Geral

No cenário empresarial contemporâneo, a informação tornou-se um ativo estratégico inestimável. A capacidade de recolher, processar, analisar e disseminar dados de forma eficiente é crucial para a tomada de decisões e para a sustentabilidade organizacional. No domínio da Gestão de Recursos Humanos (GRH), esta premissa assume uma importância ainda maior, dada a complexidade e a sensibilidade dos dados relacionados com o capital humano. Os Sistemas de Informação em Recursos Humanos (SIRH) emergem, assim, como ferramentas indispensáveis que suportam as diversas funções da GRH, desde a administração de pessoal até ao desenvolvimento estratégico de talentos.

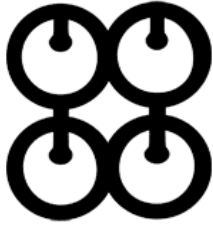
Este manual propõe-se a explorar, de forma aprofundada e rigorosa, os conceitos, as tecnologias e as aplicações dos SIRH, bem como os desafios e as oportunidades que estes representam para as organizações. Com uma linguagem académica formal e uma fundamentação científica robusta, o conteúdo foi estruturado para proporcionar aos estudantes de pós-graduação uma compreensão abrangente e crítica da matéria, preparando-os para enfrentar as exigências de um mercado de trabalho em constante

evolução. Serão abordados temas desde a evolução histórica dos sistemas de informação até às tendências mais recentes, como a Inteligência Artificial, Big Data e People Analytics, sempre com uma perspetiva de aplicação prática e de impacto organizacional.

Objectivo geral da disciplina

- Formular perspectivas sobre a aplicação dos sistemas de informação de recursos humanos nas organizações para operacionalização da estratégia organizacional.

Objectivos Específicos



- Identificar os sistemas de informação e as diferentes tipologias e características associadas;
- Aplicar as ferramentas de suporte à comunicação organizacional e a ambientes colaborativos, com destaque para as ferramentas online;
- Gerir ferramentas de mídias sociais e redes sociais profissionais de organizações.

Conteúdo da Disciplina

Este módulo está estruturado em temas que constam do plano curricular da disciplina. Para cada tema, foram seleccionados materiais que servirão de base teórica para a aprendizagem dos estudantes. Cada tema contém uma sinopse, objectivos, resultados de aprendizagem, materiais de aprendizagem e as actividades de avaliação e auto-avaliação.

No final de cada tema, são incorporados exercícios de auto-avaliação.

Outros recursos

Para além dos materiais recomendados, a UnISCED disponibiliza outros recursos de aprendizagem como recursos educacionais abertos, manuais, artigos científicos, revistas digitais, vídeos tutoriais, actas de congressos e outros seleccionados e disponibilizados na plataforma *Moodle*, Biblioteca Virtual da UnISCED ou outros repositórios virtuais.

Auto-avaliação e tarefas de avaliação

Os exercícios de auto-avaliação para este módulo encontram-se no final de cada tema e também disponíveis na plataforma *Moodle*.

Habilidades de estudo

Durante a formação e desenvolvimento de competências, e com vista a facilitar a aprendizagem e alcançar melhores resultados, o estudante deverá ter empenho, dedicação e disciplina no estudo, isto é, os bons resultados apenas se conseguem com estratégias eficientes e eficazes.

Por isso, é importante saber como, onde e quando estudar. Para o efeito, apresentamos algumas sugestões com as quais esperamos que o caro estudante possa rentabilizar o tempo dedicado aos estudos, procedendo como se segue:

- Estudar regularmente, sendo necessário que faça uma agenda de trabalho/ estudo que lhe garanta um tempo específico para o estudo. Isso significa que não se deve estudar apenas quando tiver tempo.
- Não estude na última hora, seja sistemático e não o faça apenas para responder às avaliações.

- Sempre que necessário e possível, consulte a tutoria para “tirar” dúvidas. A sua interação com a tutoria e outros colegas ou grupo de estudo é uma estratégia poderosa para progredir no curso.

IMPORTANTE: Em observância ao triângulo **modo-espaco-tempo**, respectivamente **como, onde** e **quando** estudar, como foi referido no início deste item, antes de organizar os seus momentos de estudo, reflecta sobre o ambiente de estudo que seria ideal para si:

- ❖ Estudo melhor em casa/biblioteca/café/outro lugar?
- ❖ Estudo melhor à noite/de manhã/de tarde/fins-de-semana/ao longo da semana?
- ❖ Estudo melhor com música/num sítio sossegado/num sítio barulhento?
- ❖ Preciso de intervalo a cada 30 minutos, a cada hora, etc.

Por outro lado, não recomendamos estudar seguidamente por tempo superior a uma hora. Estudar por tempo de uma hora intercalado por 10 (dez) a 15 (quinze) minutos de descanso.

Apoio, dúvidas e reclamações

Para a resolução das dificuldades dos estudantes, a UnISCED dispõe de várias opções de apoio. Para o efeito, é importante saber definir claramente a dificuldade para poder contactar ou usar a opção de apoio mais apropriada e obter, assim, ajuda rápida.

N.º	Opção	Tipo de apoio requerido
1	Fórum de dúvidas no <i>Moodle</i>	Dúvidas de conteúdo, acesso às actividades, explicações.
2	Tutor (Sessão de vídeo-conferência, <i>chat</i> do <i>Moodle</i> e <i>e-mail</i>)	Dúvidas de conteúdo, acesso às actividades, explicações.
3	Coordenador (<i>e-mail</i> ou por telefone)	Problemas de acesso à disciplina ou nas actividades.
5	<i>HelpDesk</i> (telefone)	Questões administrativas, pagamentos, estado das propinas e inscrições.
6	Secretaria <i>Online</i> (<i>pedido de assistência - online</i> na plataforma <i>Moodle</i>)	Resultados, reclamações, pedidos de esclarecimento, estado das propinas.
7	Centro de Recursos (telefone, <i>e-mail</i> ou presencialmente)	Questões gerais, reclamações, pedidos de esclarecimento, estado das propinas, confirmação de pagamentos.

Avaliação

A avaliação do estudante consta, de forma detalhada, do Regulamento de Mestrado e Doutorado em vigor na UnISCED.

Algumas actividades práticas, relatórios e reflexões serão utilizados como instrumentos de avaliação quer formativa quer sumativa.

Durante a realização das avaliações, os estudantes devem ter em consideração a apresentação, a coerência e a coesão textuais, o grau de cientificidade, a forma de conclusão dos assuntos, as recomendações e/ ou sugestões, a identificação das referências bibliográficas utilizadas, o respeito pelos direitos do autor, entre outros.

Os objectivos e critérios de avaliação constam do Regulamento de Mestrado e Doutorado.

Originalidade e Plágio

Os trabalhos académicos e científicos, incluindo avaliações, dissertações e teses, são submetidos a verificação de originalidade através de ferramentas especializadas para a detecção de níveis elevados de similaridade e plágio. Adicionalmente, são analisados com o propósito de identificar a eventual utilização de conteúdos gerados por Inteligência Artificial (IA). A similaridade excessiva, o plágio e o uso não autorizado de materiais produzidos por IA configuram violações da integridade académica na UnISCED e estão sujeitos a sanções nos termos dos regulamentos institucionais aplicáveis.

Prefácio

O presente manual foi concebido para servir como um recurso didático e científico fundamental para estudantes de Mestrado em Gestão de Recursos Humanos, com foco na disciplina de Sistemas de Informação em Recursos Humanos (SIRH). Numa era de transformação digital acelerada, a gestão eficaz dos recursos humanos é indissociável da utilização estratégica de tecnologias de informação. Este trabalho visa preencher a lacuna entre a teoria académica e a aplicação prática, fornecendo uma base sólida para a compreensão, implementação e gestão de SIRH em contextos organizacionais complexos. A abordagem crítica e a fundamentação científica são pilares deste manual, incentivando os leitores a desenvolverem uma perspetiva analítica e inovadora sobre o papel da tecnologia na gestão de pessoas.

Competências a Desenvolver

- Ao final da leitura e estudo deste manual, espera-se que os estudantes desenvolvam as seguintes competências:
- Compreender e aplicar os conceitos fundamentais de Sistemas de Informação e SIRH.
- Analisar criticamente a importância estratégica dos SIRH para a gestão de recursos humanos e para o sucesso organizacional.
- Identificar e avaliar os diferentes tipos e componentes de SIRH, selecionando as soluções mais adequadas para diversas necessidades de RH.
- Gerir dados de RH de forma eficaz, garantindo a sua qualidade, integridade e segurança.
- Aplicar princípios de People Analytics para extrair insights valiosos dos dados de RH e suportar a tomada de decisão.
- Desenvolver e implementar políticas de segurança da informação e proteção de dados em RH, em conformidade com as normas legais e éticas.
- Avaliar e mitigar riscos e ameaças relacionados com a segurança da informação em ambientes de RH.
- Integrar perspectivas estratégicas de RH e tecnologia, contribuindo para a transformação digital das organizações.
- Comunicar de forma clara e rigorosa sobre temas relacionados com SIRH, tanto para públicos técnicos quanto não técnicos.

Metodologia de Estudo

Para otimizar a aprendizagem e o aproveitamento deste manual, sugere-se a seguinte metodologia de estudo:

1. **Leitura Ativa:** Leia cada capítulo com atenção, sublinhando conceitos-chave e fazendo anotações. Procure compreender a interligação entre os diferentes tópicos.
2. **Reflexão Crítica:** Não se limite a assimilar a informação. Questione, analise e reflita sobre as implicações teóricas e práticas dos conceitos apresentados.
3. **Consulta de Referências:** Utilize as referências bibliográficas sugeridas para aprofundar os temas de maior interesse ou para esclarecer dúvidas.
4. **Resolução de Exercícios:** Os exercícios e perguntas de avaliação ao final de cada capítulo são ferramentas essenciais para consolidar o conhecimento e testar a compreensão.
5. **Discussão e Debate:** Participe ativamente em discussões com colegas e professores, compartilhando perspectivas e enriquecendo a sua compreensão.
6. **Aplicação Prática:** Procure relacionar os conceitos teóricos com situações reais do seu contexto profissional ou com estudos de caso apresentados, desenvolvendo a sua capacidade de aplicação.

Unidade I – sistemas de informação

Introdução ao Capítulo I

Este capítulo dedica-se a explorar o universo dos Sistemas de Informação (SI), desde os seus conceitos fundamentais até às suas aplicações mais complexas, com um foco particular nos Sistemas de Informação em Recursos Humanos (SIRH). Numa era caracterizada pela digitalização e pela crescente dependência da tecnologia, compreender a estrutura, o funcionamento e o impacto dos SI é crucial para qualquer profissional, especialmente para aqueles que atuam na gestão de pessoas. Abordaremos a evolução histórica, os componentes essenciais, os diversos tipos de SI e o seu papel transformador nas organizações, culminando numa análise das tendências modernas que moldam o futuro da gestão de informação em RH.

1.1 Conceito de Sistemas de Informação

Definições Clássicas e Modernas

Tradicionalmente, um Sistema de Informação (SI) pode ser definido como um conjunto organizado de pessoas, hardware, software, redes de comunicação e dados que recolhe, transforma e dissemina informação numa organização (Laudon & Laudon, 2020). Esta definição clássica enfatiza os elementos tangíveis e a função primária de processamento de dados. No entanto, com a evolução tecnológica e a crescente complexidade dos ambientes organizacionais, as definições modernas de SI transcendem a mera perspetiva técnica, incorporando a dimensão estratégica e o valor gerado pela informação.

Uma perspetiva mais contemporânea define SI como um conjunto de componentes inter-relacionados que recolhem, processam, armazenam e distribuem informação para apoiar a tomada de decisões, a coordenação, o controlo, a análise e a visualização numa organização (O'Brien & Marakas, 2011). Esta visão destaca o papel dos SI como facilitadores de processos de negócio e como ferramentas estratégicas para alcançar vantagens competitivas. Tannenbaum (1990), por exemplo, definiu um SIRH como um sistema utilizado para adquirir, armazenar, manipular e distribuir informação sobre os recursos humanos de uma organização (Tannenbaum,

1990). Esta definição, embora mais antiga, ainda ressoa na compreensão do propósito fundamental dos SIRH.

Evolução Histórica

A história dos Sistemas de Informação é intrinsecamente ligada à evolução da tecnologia e das necessidades empresariais. Inicialmente, os SI eram rudimentares, focados em tarefas administrativas básicas, como o processamento de salários e a manutenção de registos. Com o advento dos computadores na década de 1950 e 1960, surgiram os primeiros Sistemas de Processamento de Transações (SPT), que automatizavam operações rotineiras e de grande volume. Nas décadas seguintes, a complexidade aumentou, dando origem aos Sistemas de Informação de Gestão (SIG), que forneciam relatórios para apoiar a gestão intermédia, e aos Sistemas de Apoio à Decisão (SAD), que auxiliavam na resolução de problemas não estruturados.

A proliferação da internet e das tecnologias web nos anos 90 e 2000 impulsionou a criação de sistemas mais integrados e acessíveis, como os Enterprise Resource Planning (ERP), que unificaram diversas funções empresariais, incluindo os recursos humanos. Mais recentemente, a ascensão da computação em nuvem (Cloud Computing), da Inteligência Artificial (IA), do Big Data e da People Analytics tem redefinido o panorama dos SI, tornando-os mais inteligentes, preditivos e estratégicos (Marler &

Boudreau, 2017) .

Importância nas Organizações

A importância dos Sistemas de Informação nas organizações modernas é inegável. Eles são o motor que impulsiona a eficiência operacional, a inovação e a capacidade de resposta às dinâmicas do mercado. Os SI permitem:

- ✓ **Otimização de Processos:** Automatizam tarefas repetitivas, reduzem erros e aceleram fluxos de trabalho.
- ✓ **Melhoria da Tomada de Decisão:** Fornecem dados e análises que suportam decisões mais informadas e estratégicas.

- ✓ **Vantagem Competitiva:** Permitem que as organizações inovem em produtos, serviços e modelos de negócio, diferenciando-se da concorrência.
- ✓ **Comunicação e Colaboração:** Facilitam a troca de informações entre departamentos e equipes, promovendo um ambiente de trabalho mais colaborativo.
- ✓ **Gestão do Conhecimento:** Capturam, armazenam e disseminam o conhecimento organizacional, tornando-o acessível e reutilizável.

1.2 Componentes dos Sistemas de Informação



Um Sistema de Informação eficaz é composto por vários elementos interligados que trabalham em conjunto para atingir os objetivos organizacionais. Estes componentes podem ser categorizados da seguinte forma:

Hardware- O hardware refere-se a todos os equipamentos físicos e dispositivos eletrónicos que compõem o SI. Inclui computadores (servidores, desktops, laptops), dispositivos

móveis (smartphones, tablets), periféricos (impressoras, scanners), equipamentos de rede (routers, switches) e dispositivos de armazenamento (discos rígidos, SSDs). A escolha do hardware adequado é crucial para garantir o desempenho, a capacidade e a fiabilidade do sistema.

Software- O software é o conjunto de programas, aplicações e instruções que controlam o hardware e permitem que os utilizadores interajam com o sistema. Divide-se geralmente em:

Software de Sistema: Inclui sistemas operativos (Windows, Linux, macOS) e utilitários que gerenciam os recursos do computador.

Software de Aplicação: Programas desenvolvidos para realizar tarefas específicas, como processadores de texto, folhas de cálculo, sistemas de gestão de bases de dados (SGBD), e aplicações empresariais como ERP e SIRH.

Dados- Os dados são a matéria-prima dos Sistemas de Informação. São factos brutos, números, textos e imagens que, quando processados e organizados, se transformam em informação significativa. A qualidade, a integridade e a segurança dos dados são fundamentais para a fiabilidade e utilidade de qualquer SI. Em RH, os dados incluem informações sobre colaboradores, salários, desempenho, formação, entre outros.

Pessoas- As pessoas são o componente mais crítico de qualquer SI. Incluem os utilizadores finais (colaboradores, gestores), os especialistas em SI (analistas de sistemas, programadores, administradores de bases de dados) e a gestão que define a estratégia e os objetivos do sistema. O sucesso de um SI depende em grande parte da forma como as pessoas o utilizam, interagem e contribuem para a sua evolução.

Processos- Os processos são as etapas e procedimentos que governam a forma como os dados são recolhidos, processados, armazenados e distribuídos. Incluem as regras de negócio, os fluxos de trabalho e as políticas que garantem que o SI opera de forma eficiente e consistente. A otimização dos processos é essencial para maximizar o valor dos SI.

Redes- As redes de comunicação permitem a interconexão entre os diferentes componentes do SI, facilitando a partilha de dados e recursos. Incluem redes locais (LAN), redes de longa distância (WAN), a internet e tecnologias sem fios (Wi-Fi, Bluetooth). A infraestrutura de rede é vital para a acessibilidade e a colaboração dentro e fora da organização.

1.3 Tipos de Sistemas de Informação



Os Sistemas de Informação podem ser classificados de diversas formas, dependendo da sua função, nível organizacional a que servem e tipo de apoio que oferecem. Abaixo, são apresentados alguns dos tipos mais comuns:

Sistemas Operacionais (SPT)

Os Sistemas de Processamento de Transações (SPT) são projetados para processar e registrar as transações diárias de rotina necessárias para conduzir o negócio. Exemplos incluem sistemas de processamento de pedidos, sistemas de folha de pagamento e sistemas de registro de clientes. São cruciais para a eficiência operacional e para a manutenção de registros precisos.

Sistemas de Apoio à Decisão (SAD)

Os Sistemas de Apoio à Decisão (SAD) ajudam os gestores a tomar decisões semi estruturadas e não estruturadas, fornecendo ferramentas de análise de dados e modelos de simulação. Eles combinam dados e modelos analíticos para apoiar a resolução de problemas complexos, como a previsão de vendas ou a análise de investimentos.

Sistemas Estratégicos

Os Sistemas Estratégicos são aqueles que alteram os objetivos, produtos, serviços ou relações ambientais de uma organização para ajudar a obter uma vantagem competitiva. Exemplos incluem sistemas de gestão da cadeia de suprimentos que otimizam a logística ou sistemas de CRM que melhoram o relacionamento com o cliente.

Enterprise Resource Planning (ERP)

Os Enterprise Resource Planning (ERP) são sistemas integrados que consolidam todos os processos de negócio de uma organização (finanças, RH, produção, vendas, etc.) numa única plataforma. O objetivo é otimizar a gestão de recursos, melhorar a comunicação e a eficiência, e fornecer uma visão holística da empresa. Os módulos de RH são uma parte integrante dos sistemas ERP modernos.

Business Intelligence (BI)

Business Intelligence (BI) refere-se a um conjunto de tecnologias e processos que transformam dados brutos em informações significativas e úteis para fins de análise de negócios. Inclui ferramentas de relatórios, dashboards, mineração de dados e análise preditiva, que ajudam as organizações a identificar tendências, padrões e oportunidades de negócio.

Sistemas de Informação em Recursos Humanos (SIRH)

TIPOS DE SISTEMAS DE INFORMAÇÃO EM RH

Os Sistemas de Informação em Recursos Humanos (SIRH) são soluções tecnológicas que apoiam os processos de gestão de pessoas, fornecendo informações precisas para a tomada de decisão estratégica.

TIPO DE SISTEMA	DESCRIÇÃO	PRINCIPAIS FUNÇÕES	EXEMPLOS DE APLICAÇÃO	BENEFÍCIOS PARA A ORGANIZAÇÃO
 1. SISTEMAS OPERACIONAIS DE RH	Sistemas que apoiam as atividades diárias e rotineiras do departamento de RH, registrando e processando dados operacionais.	• Cadastro de colaboradores • Folha de pagamento • Gestão de benefícios • Controle de ponto e assiduidade • Administração de documentos	 Workday HCM SAP SuccessFactors Módulo RH do TOTVS Senior X	✓ Maior eficiência operacional ✓ Redução de erros ✓ Padronização de processos ✓ Agilidade no atendimento
 2. SISTEMAS DE APOIO À DECISÃO EM RH	Sistemas que fornecem informações e relatórios para apoiar gestores na tomada de decisões táticas e estratégicas.	• Relatórios gerenciais • Indicadores de RH (KPIs) • Análises de desempenho • Planejamento de pessoal • Simulações e cenários	 Power BI Tableau Qlik Sense SAP Analytics Cloud	✓ Decisões mais assertivas ✓ Visão analítica do negócio ✓ Monitoramento de resultados ✓ Melhoria contínua
 3. SISTEMAS ESTRATÉGICOS DE RH	Sistemas que apoiam o alinhamento da gestão de pessoas à estratégia organizacional.	• Planejamento estratégico de RH • Gestão de talentos e sucessão • Desenvolvimento organizacional • Cultura e clima organizacional • Gestão por competências	 SAP SuccessFactors Oracle HCM Cloud Cornerstone OnDemand	✓ Alinhamento à estratégia da organização ✓ Desenvolvimento de talentos ✓ Retenção de pessoas-chave ✓ Aumento da competitividade
 4. SISTEMAS DE GESTÃO DO APRENDIZADO (LMS)	Sistemas voltados para o gerenciamento de treinamentos, cursos e desenvolvimento de competências.	• Gestão de treinamentos • E-learning • Trilhas de aprendizagem • Avaliação de aprendizagem • Certificações	 Moodle TalentLMS Docebo SAP Litmos	✓ Desenvolvimento contínuo ✓ Engajamento dos colaboradores ✓ Padronização dos treinamentos ✓ Acompanhamento de resultados
 5. SISTEMAS DE RECRUTAMENTO E SELEÇÃO (ATS)	Sistemas que automatizam e otimizam o processo de recrutamento e seleção de talentos.	• Divulgação de vagas • Triagem de currículos • Gestão de candidatos • Agendamento de entrevistas • Integração com redes sociais	 Greenhouse Breezy HR Gupy LinkedIn Talent Solutions	✓ Processo seletivo mais ágil ✓ Melhor experiência do candidato ✓ Maior qualidade nas contratações ✓ Redução de custos
 6. SISTEMAS DE GESTÃO DE DESEMPENHO E RECOMPENSAS	Sistemas que ajudam a avaliar o desempenho e gerenciar recompensas, metas e reconhecimento.	• Definição de metas (KPIs/OKRs) • Avaliação de desempenho • Planos de desenvolvimento • Programas de reconhecimento • Gestão de recompensas	 Leapsome 15Five Lattice Sage HR	✓ Melhoria do desempenho ✓ Cultura de reconhecimento ✓ Engajamento e motivação ✓ Retenção de talentos



IMPORTANTE: Os tipos de sistemas de informação em RH podem integrar-se entre si, formando um ecossistema tecnológico que gera informações confiáveis e estratégicas para a gestão de pessoas.



Os Sistemas de Informação em Recursos Humanos (SIRH) são sistemas especializados que automatizam e gerenciam as funções de RH. Eles integram dados e processos relacionados com os colaboradores, desde o recrutamento e seleção até à gestão de desempenho, folha de pagamento e desenvolvimento de carreira. Serão explorados em maior detalhe na secção seguinte.

1.4 Sistemas de Informação em Recursos Humanos (SIRH)

Conceito

Um Sistema de Informação em Recursos Humanos (SIRH), também conhecido como Human Resource Information System (HRIS), é uma solução tecnológica que integra e automatiza as funções e processos de gestão de recursos humanos.

Conforme definido por Kavanagh e Johnson (2020), um SIRH é um sistema que permite às organizações recolher, armazenar, manipular, analisar, recuperar e distribuir informações sobre os seus recursos humanos . O seu propósito principal é melhorar a eficiência e a eficácia das operações de RH, bem como apoiar a tomada de decisões estratégicas relacionadas com o capital humano.

Os principais objetivos de um SIRH incluem:

-  **Otimizar a Administração de RH:** Automatizar tarefas rotineiras como processamento de folha de pagamento, gestão de benefícios e manutenção de registos de colaboradores.
-  **Melhorar a Eficiência Operacional:** Reduzir o tempo e os custos associados aos processos de RH, eliminando a necessidade de trabalho manual e em papel.
-  **Fornecer Informação para Tomada de Decisão:** Oferecer dados e relatórios precisos e atualizados para apoiar gestores e líderes de RH em decisões estratégicas.
-  **Garantir a Conformidade:** Ajudar as organizações a cumprir as regulamentações legais e políticas internas relacionadas com RH.
-  **Apoiar o Desenvolvimento de Talentos:** Facilitar a gestão de desempenho, formação, desenvolvimento de carreira e planeamento de sucessão.
-  **Melhorar a Experiência do Colaborador:** Fornecer portais de auto-atendimento que permitem aos colaboradores aceder e atualizar as suas informações pessoais, solicitar férias, etc.

As funções de um SIRH são vastas e abrangem diversas áreas da GRH: **Uma tabela comparativa pode ilustrar as principais funcionalidades:**

Área de RH	Funções do SIRH
Recrutamento e Seleção	Divulgação de vagas, triagem automática de currículos, gestão de candidaturas, agendamento de entrevistas e análise de perfis de candidatos.
Administração de Pessoal	Gestão de contratos, cadastro de colaboradores, controlo de assiduidade, processamento salarial e gestão de benefícios.
Formação e Desenvolvimento	Identificação de necessidades de formação, gestão de programas de capacitação, acompanhamento de desempenho e desenvolvimento de competências.
Avaliação de Desempenho	Definição de metas, monitorização de desempenho, feedback contínuo, avaliações periódicas e geração de relatórios analíticos.
Gestão de Carreiras	Planeamento de sucessão, gestão de talentos, promoções, mobilidade interna e desenvolvimento de planos de carreira.
Saúde e Segurança no Trabalho	Registo de acidentes, monitorização de condições de trabalho, gestão de exames médicos e conformidade com normas de segurança.
Comunicação Interna	Partilha de informações organizacionais, gestão de notificações, portais do colaborador e integração entre departamentos.
People Analytics	Análise de dados de RH, produção de indicadores estratégicos, previsão de tendências e apoio à tomada de decisão.
Gestão Documental	Armazenamento digital de documentos, controlo de acesso, organização de arquivos e automatização documental.
Compliance e Auditoria	Monitorização de conformidade legal, rastreabilidade de processos, auditorias internas e proteção de dados pessoais.

Conclusão do Capítulo I

O Capítulo I forneceu uma visão abrangente sobre os Sistemas de Informação, desde a sua conceptualização e evolução histórica até à sua importância estratégica nas organizações modernas. Foi dada especial atenção aos Sistemas de Informação em Recursos Humanos (SIRH), destacando os seus objetivos, funções e aplicações práticas na automatização e otimização dos processos de RH. A compreensão dos componentes de um SI e dos diversos tipos de sistemas existentes é fundamental para qualquer profissional que deseje alavancar a tecnologia para impulsionar a eficiência e a competitividade. As tendências modernas, como a IA, Big Data e People Analytics, sublinham a necessidade de uma adaptação contínua e de uma visão estratégica na gestão da informação em RH, preparando o terreno para os próximos capítulos que aprofundarão a gestão de dados e a segurança da informação.

Perguntas de Avaliação

Verdadeiro ou Falso

1. Um Sistema de Informação (SI) é composto exclusivamente por hardware e software, sem a intervenção de pessoas ou processos. **(F)**
2. Os Sistemas de Processamento de Transações (SPT) são primariamente utilizados para apoiar decisões estratégicas não estruturadas. **(F)**
3. A definição clássica de SIRH de Tannenbaum (1990) foca-se na aquisição, armazenamento, manipulação, análise, recuperação e distribuição de informações sobre recursos humanos. **(V)**
4. O Cloud Computing é uma tendência moderna que tem diminuído a importância dos SIRH nas organizações. **(F)**
5. Um dos objetivos principais de um SIRH é otimizar a administração de RH e melhorar a eficiência operacional. **(V)**

Escolha Múltipla

1. Qual dos seguintes não é um componente fundamental de um Sistema de Informação?
a) Hardware
b) Software
c) Produtos Finais
d) Pessoas
2. Qual tipo de Sistema de Informação é projetado para consolidar todos os processos de negócio de uma organização numa única plataforma?
a) Sistemas de Apoio à Decisão (SAD)
b) Sistemas de Processamento de Transações (SPT)
c) Enterprise Resource Planning (ERP)
d) Business Intelligence (BI)
3. Qual das seguintes não é uma função típica de um SIRH?
a) Gestão de desempenho
b) Controlo de inventário de matérias-primas
c) Processamento de folha de pagamento
d) Recrutamento e seleção
4. A People Analytics, como tendência moderna em SIRH, visa principalmente:
a) Automatizar tarefas administrativas de RH.
b) Fornecer insights baseados em dados para a tomada de decisão em RH.
c) Gerenciar a segurança física das instalações da empresa.
d) Desenvolver novos produtos e serviços para o mercado.
5. Qual a principal vantagem da implementação de um SIRH nas organizações?
a) Aumento da burocracia e do trabalho manual.
b) Redução da comunicação entre departamentos.
c) Melhoria da eficiência operacional e apoio à tomada de decisão estratégica.
d) Diminuição da conformidade com regulamentações legais.

Guião de correção

Verdadeiro ou Falso: 1. F, 2. F, 3. V, 4. F, 5. V

Escolha Múltipla: 1. c, 2. c, 3. b, 4. b, 5. c

Exercícios Complementares

1. Estudo de Caso: Analise um caso real de implementação de um SIRH numa organização à sua escolha. Discuta os desafios enfrentados, as soluções adotadas e os impactos observados na gestão de RH e no desempenho organizacional.

2. Perguntas para Debate:

De que forma a evolução dos Sistemas de Informação tem moldado o papel do profissional de Recursos Humanos?

Quais são os principais dilemas éticos e de privacidade associados à recolha e utilização de dados de colaboradores em SIRH?

Como as pequenas e médias empresas (PMEs) podem beneficiar da implementação de SIRH, considerando as suas limitações de recursos?

3. Atividades Práticas:

Pesquise e compare três diferentes softwares de SIRH disponíveis no mercado, destacando as suas funcionalidades, vantagens e desvantagens para uma empresa de médio porte.

Desenhe um fluxograma que represente o processo de recrutamento e seleção numa organização, identificando os pontos onde um SIRH pode otimizar cada etapa.

4. Reflexão Crítica: Discuta a afirmação: “A tecnologia por si só não garante o sucesso de um SIRH; a cultura organizacional e a gestão da mudança são igualmente importantes.”

Unidade II – Gestão de dados

Introdução ao Capítulo II

A gestão de dados é a espinha dorsal de qualquer Sistema de Informação em Recursos Humanos (SIRH) eficaz. Num ambiente organizacional onde a informação é um ativo estratégico, a capacidade de gerir dados de forma eficiente, segura e ética é fundamental. Este capítulo explora os conceitos essenciais da gestão de dados, desde

o seu ciclo de vida até à importância da qualidade da informação. Aprofundaremos a aplicação da gestão de dados em Recursos Humanos, com especial destaque para a People Analytics, e discutiremos os desafios éticos e legais associados à proteção de dados pessoais, como a conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD/GDPR).

2.1 Conceito de Gestão de Dados



A Gestão de Dados refere-se ao conjunto de práticas, processos, políticas e tecnologias utilizadas para gerir o ciclo de vida completo dos dados de uma organização, desde a sua criação ou aquisição até ao seu arquivo ou destruição. O objetivo principal é garantir que os dados sejam precisos, acessíveis, seguros e utilizáveis para apoiar as operações e a tomada de decisão.

Os principais objetivos da gestão de dados incluem:

- ✓ **Garantir a Qualidade dos Dados:** Assegurar que os dados são precisos, completos, consistentes e atualizados.
- ✓ **Facilitar o Acesso e a Partilha:** Tornar os dados facilmente acessíveis aos utilizadores autorizados, promovendo a colaboração e a eficiência.
- ✓ **Proteger a Segurança e a Privacidade:** Implementar medidas para proteger os dados contra acessos não autorizados, perdas ou violações, garantindo a conformidade com as regulamentações.

- ✓ **Otimizar o Armazenamento e a Recuperação:** Utilizar tecnologias e arquiteturas eficientes para armazenar e recuperar dados de forma rápida e económica.
- ✓ **Apoiar a Tomada de Decisão:** Fornecer dados fiáveis e relevantes para análises e relatórios, suportando decisões estratégicas e operacionais.

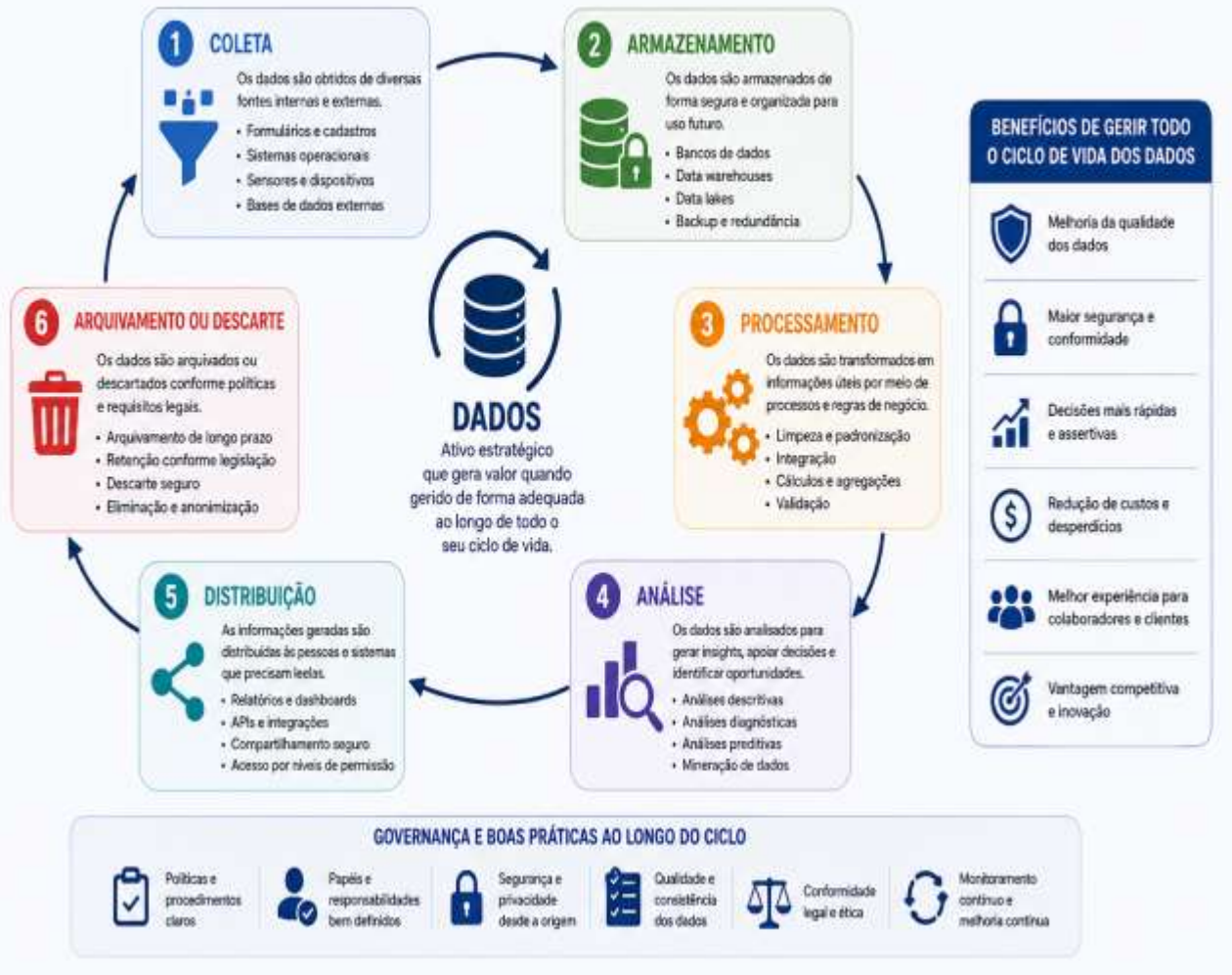
Importância Estratégica

A gestão de dados é estrategicamente importante porque os dados são a base para a inteligência de negócios e a inovação. Organizações que gerem os seus dados de forma eficaz podem identificar tendências, otimizar processos, melhorar a experiência do cliente (ou do colaborador, no caso de RH) e obter uma vantagem competitiva significativa. Em RH, a gestão de dados permite uma compreensão mais profunda da força de trabalho, facilitando a atração, retenção e desenvolvimento de talentos.

2.2 Ciclo de Vida dos Dados

CICLO DE VIDA DOS DADOS

O ciclo de vida dos dados representa as etapas pelas quais os dados passam desde a sua criação até ao seu descarte. Uma gestão eficiente em cada etapa garante qualidade, segurança e valor estratégico para a organização.



O ciclo de vida dos dados descreve as fases pelas quais os dados passam desde a sua criação até à sua eliminação. Compreender este ciclo é essencial para implementar práticas de gestão de dados eficazes.

- 1. Coleta** - A coleta é a fase inicial, onde os dados são gerados ou adquiridos. Em RH, isto pode incluir a recolha de currículos, dados de desempenho, informações de folha de pagamento ou respostas a inquéritos de clima organizacional. É crucial garantir que a coleta seja feita de forma ética, legal e com o consentimento adequado, quando aplicável.

2. **Armazenamento** -Após a coleta, os dados devem ser armazenados de forma segura e organizada. Isto envolve a escolha de tecnologias de armazenamento adequadas, como bases de dados relacionais, data warehouses ou soluções em nuvem, garantindo a integridade e a disponibilidade dos dados.
3. **Processamento** -O processamento envolve a transformação dos dados brutos em informação útil. Isto pode incluir a limpeza de dados (remoção de erros ou duplicados), a integração de dados de diferentes fontes e a aplicação de algoritmos ou modelos analíticos.
4. **Análise** -A análise é a fase onde se extrai valor dos dados. Utilizando ferramentas de Business Intelligence ou People Analytics, os dados são explorados para identificar padrões, tendências e insights que suportem a tomada de decisão.
5. **Distribuição** -A distribuição (ou disseminação) envolve a partilha da informação resultante da análise com os utilizadores relevantes. Isto pode ser feito através de relatórios, dashboards ou alertas automatizados, garantindo que a informação certa chega à pessoa certa no momento certo.
6. **Arquivo**- O arquivo é a fase final do ciclo de vida ativo dos dados. Dados que já não são frequentemente utilizados, mas que precisam ser retidos por motivos legais ou históricos, são movidos para sistemas de armazenamento de longo prazo. Eventualmente, os dados podem ser destruídos de forma segura quando já não forem necessários.

2.3 Bases de Dados

As bases de dados são o núcleo tecnológico da gestão de dados, fornecendo a infraestrutura para armazenar, organizar e recuperar informações de forma eficiente.

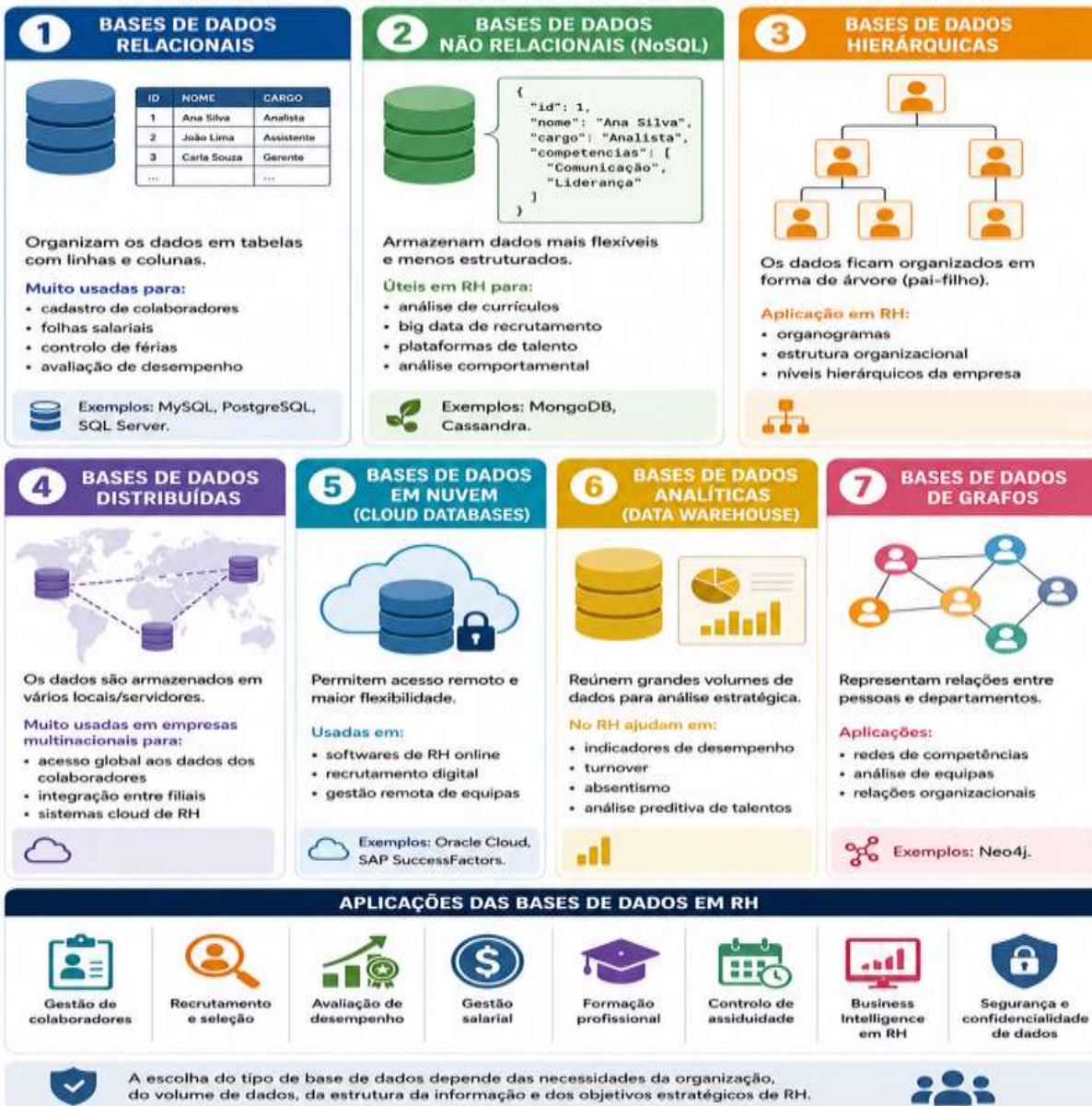
Uma base de dados é uma coleção organizada de dados estruturados, tipicamente armazenados e acedidos eletronicamente a partir de um sistema informático. O software que interage com os utilizadores, as aplicações e a própria base de dados para capturar e analisar os dados é chamado de Sistema de Gestão de Bases de Dados (SGBD)

Tipos de Bases de Dados

Existem vários tipos de bases de dados, cada um adequado a diferentes necessidades e tipos de dados.

TIPOS DE BASES DE DADOS EM RH

Principais tipos de bases de dados utilizadas em Recursos Humanos e suas aplicações



Bases Relacionais -As bases de dados relacionais organizam os dados em tabelas com linhas e colunas, estabelecendo relações entre elas. Utilizam a linguagem SQL (Structured Query Language) para gerir e consultar os dados. São ideais para dados estruturados e transações

complexas, sendo amplamente utilizadas em sistemas ERP e SIRH tradicionais para gerir informações de colaboradores, salários e benefícios.

Bases Não Relacionais (NoSQL) -As bases de dados não relacionais (NoSQL) são projetadas para lidar com grandes volumes de dados não estruturados ou semi-estruturados, como documentos, grafos ou pares chave-valor. Oferecem maior flexibilidade e escalabilidade do que as bases relacionais, sendo frequentemente utilizadas em aplicações web modernas, análise de Big Data e redes sociais.

2.4 Qualidade da Informação

A utilidade de qualquer Sistema de Informação depende intrinsecamente da qualidade dos dados que o alimentam. Dados de má qualidade podem levar a decisões erradas, ineficiências operacionais e perda de confiança no sistema.

- ✓ **Integridade** -A integridade refere-se à precisão e consistência dos dados ao longo do seu ciclo de vida. Garante que os dados não sejam alterados ou corrompidos de forma não autorizada, mantendo a sua fiabilidade.
- ✓ **Consistência** -A consistência assegura que os dados são uniformes em todo o sistema. Por exemplo, o nome de um colaborador deve ser escrito da mesma forma em todos os módulos do SIRH, evitando discrepâncias e confusões.
- ✓ **Confiabilidade**- A confiabilidade indica o grau de confiança que os utilizadores podem ter nos dados. Dados confiáveis são provenientes de fontes seguras, foram processados corretamente e refletem a realidade com precisão.
- ✓ **Atualização**- A atualização (ou tempestividade) refere-se à relevância temporal dos dados. Dados desatualizados podem ser inúteis ou até prejudiciais para a tomada de decisão. É crucial garantir que os dados reflitam a situação atual.
- ✓ **Precisão**- A precisão mede o quão próximos os dados estão do valor real ou verdadeiro. Erros de digitação, falhas de sistema ou informações incorretas fornecidas pelos utilizadores podem comprometer a precisão dos dados.

2.5 Gestão de Dados em Recursos Humanos

A aplicação dos princípios de gestão de dados na área de Recursos Humanos tem transformado a forma como as organizações gerem o seu capital humano.

Dados dos Colaboradores

A gestão eficaz dos dados dos colaboradores é fundamental. Isto inclui informações demográficas, histórico profissional, competências, avaliações de desempenho, dados salariais e informações de contacto. Um SIRH centraliza estes dados, facilitando o acesso e a atualização, e garantindo a consistência da informação.

Indicadores de RH

Os indicadores de RH (KPIs) são métricas quantificáveis utilizadas para avaliar o desempenho e a eficácia das práticas de RH. Exemplos incluem a taxa de rotatividade (turnover), o tempo médio de contratação, o custo por contratação, o índice de absentismo e o retorno sobre o investimento (ROI) em formação. A gestão de dados permite o cálculo preciso e o acompanhamento contínuo destes indicadores.

People Analytics

A People Analytics (ou HR Analytics) é a aplicação de técnicas de análise de dados, estatística e modelagem preditiva aos dados de recursos humanos, com o objetivo de melhorar a tomada de decisão e o desempenho organizacional [4]. Vai além do simples reporte de métricas, procurando identificar correlações, prever tendências e otimizar processos. Por exemplo, a People Analytics pode ser utilizada para identificar os fatores que contribuem para a retenção de talentos ou para prever o sucesso de um candidato numa determinada função.

Gestão Documental

A gestão documental em RH envolve a organização, o armazenamento e a recuperação de documentos relacionados com os colaboradores, como contratos, avaliações, certificados e

registos disciplinares. A digitalização e a gestão eletrónica de documentos melhoram a eficiência, reduzem o espaço físico necessário e facilitam o cumprimento de requisitos legais.

Tomada de Decisão Baseada em Dados

A tomada de decisão baseada em dados (Data-Driven Decision Making) é o objetivo final da gestão de dados em RH. Em vez de depender da intuição ou de suposições, os líderes de RH utilizam dados e análises para fundamentar as suas decisões, desde a contratação e promoção até à definição de políticas de remuneração e desenvolvimento.

2.6 Ética e Proteção de Dados

A recolha e utilização de dados de colaboradores levantam questões éticas e legais significativas, que devem ser geridas com rigor.

Privacidade e Confidencialidade

A privacidade refere-se ao direito dos indivíduos de controlar as suas informações pessoais e de decidir como e com quem são partilhadas. A confidencialidade é a obrigação da organização de proteger essas informações contra acessos não autorizados e de as utilizar apenas para os fins previstos.

Proteção de Dados Pessoais e LGPD/GDPR

A proteção de dados pessoais é regulamentada por leis rigorosas em muitas jurisdições. O Regulamento Geral sobre a Proteção de Dados (RGPD/GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil estabelecem princípios e regras estritas para o tratamento de dados pessoais, incluindo o consentimento, a minimização de dados, a transparência e o direito ao esquecimento. As organizações devem garantir que os seus SIRH e práticas de gestão de dados estão em total conformidade com estas regulamentações.

Responsabilidade Organizacional

A responsabilidade organizacional implica que a empresa é responsável por garantir a segurança, a privacidade e o uso ético dos dados dos seus colaboradores. Isto requer a implementação de

políticas claras, a formação dos colaboradores, a realização de auditorias regulares e a adoção de tecnologias de segurança adequadas.

Conclusão do Capítulo II

A gestão de dados é um pilar fundamental para o sucesso de qualquer iniciativa de Sistemas de Informação em Recursos Humanos. Compreender o ciclo de vida dos dados, a importância da qualidade da informação e as potencialidades da People Analytics permite às organizações transformar dados brutos em insights estratégicos. No entanto, esta capacidade deve ser

exercida com responsabilidade, respeitando os princípios éticos e as regulamentações de proteção de dados, como o GDPR. O equilíbrio entre a inovação tecnológica e a proteção da privacidade é o grande desafio e a principal responsabilidade dos profissionais de RH na era digital.

Perguntas de Avaliação

Verdadeiro ou Falso

1. O ciclo de vida dos dados termina com a fase de análise, não havendo necessidade de arquivamento ou destruição. **(F)**
2. As bases de dados relacionais são ideais para armazenar grandes volumes de dados não estruturados, como publicações em redes sociais. **(F)**

3. A People Analytics foca-se exclusivamente na criação de relatórios descritivos sobre o passado, sem capacidade preditiva. **(F)**
4. A integridade dos dados garante que a informação não seja alterada ou corrompida de forma não autorizada. **(V)**
5. O GDPR (Regulamento Geral sobre a Proteção de Dados) aplica-se apenas a dados de clientes, não abrangendo os dados dos colaboradores de uma organização. **(F)**

Escolha Múltipla

1. Qual das seguintes fases NÃO faz parte do ciclo de vida típico dos dados?

- a) Coleta
- b) Processamento
- c) Intuição**
- d) Arquivo

2. Qual a principal característica que distingue as bases de dados NoSQL das bases de dados relacionais?

- a) Utilizam exclusivamente a linguagem SQL.
- b) São projetadas para lidar com dados não estruturados e oferecem maior flexibilidade.**
- c) Organizam os dados estritamente em tabelas com linhas e colunas.
- d) São menos escaláveis e adequadas apenas para pequenos volumes de dados.

3. A dimensão da qualidade da informação que assegura que os dados refletem a situação atual e não estão obsoletos é a:

- a) Consistência
- b) Precisão
- c) Atualização (Tempestividade)**
- d) Confiabilidade

4. O principal objetivo da People Analytics é:

- a) Substituir os profissionais de RH por algoritmos.
- b) Aplicar técnicas de análise de dados para melhorar a tomada de decisão e o desempenho organizacional.**
- c) Aumentar a quantidade de dados recolhidos sem um propósito específico.
- d) Garantir a conformidade legal com as leis laborais.

5. No contexto da ética e proteção de dados, o princípio da “minimização de dados” significa que:

- a) A organização deve recolher o máximo de dados possível para uso futuro.
- b) A organização deve recolher apenas os dados estritamente necessários para a finalidade pretendida.**
- c) Os dados devem ser armazenados no menor espaço físico possível.
- d) O acesso aos dados deve ser restrito apenas à gestão de topo.

Guião de Correção

Verdadeiro ou Falso: 1. F, 2. F, 3. F, 4. V, 5. F

Escolha Múltipla: 1. c, 2. b, 3. c, 4. b, 5. b

Exercícios Complementares

1. Estudo de Caso: Uma empresa multinacional pretende implementar um projeto de People Analytics para prever o risco de saída (turnover) dos seus colaboradores-chave. Identifique os tipos de dados que a empresa precisaria de recolher, os potenciais desafios na qualidade desses dados e as considerações éticas e legais (GDPR) que devem ser tidas em conta.

2. Perguntas para Debate:

Até que ponto a utilização de algoritmos na tomada de decisão em RH (ex: seleção de candidatos) pode introduzir vieses e discriminação? Como mitigar esses riscos?

Qual o impacto do teletrabalho e dos modelos híbridos na gestão e segurança dos dados dos colaboradores?

3. Atividades Práticas:

Crie um modelo de “Política de Privacidade de Dados para Colaboradores” para uma empresa fictícia, abordando os princípios do GDPR (consentimento, finalidade, direitos dos titulares, etc.).

Utilizando uma folha de cálculo (ex: Excel), crie um pequeno conjunto de dados fictícios de RH (nome, idade, departamento, salário, avaliação de desempenho) e aplique técnicas simples de limpeza de dados (identificar duplicados, corrigir erros de formatação) e crie um dashboard básico com dois indicadores (ex: média salarial por departamento).

4. Reflexão Crítica: Analise a tensão entre a necessidade das organizações de recolher dados para otimizar a gestão de talentos (People Analytics) e o direito à privacidade dos colaboradores. Como encontrar um equilíbrio sustentável?

Unidade III – Gestão de segurança

SEGURANÇA DA INFORMAÇÃO EM RECURSOS HUMANOS

Proteger informações de colaboradores é proteger pessoas, a empresa e o futuro.



OBJETIVO

Garantir a confidencialidade, integridade e disponibilidade das informações de RH, prevenindo acessos não autorizados, uso indevido, vazamentos, perdas e alterações indevidas.



INFORMAÇÕES DE RH QUE DEVEM SER PROTEGIDAS

- Dados pessoais (nome, endereço, data de nascimento, documentos)
- Informações salariais e benefícios
- Avaliações de desempenho
- Dados de saúde e afastamentos
- Histórico profissional e disciplinar
- Contratos e documentos internos
- Credenciais de acesso e informações de sistemas

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO



CONFIDENCIALIDADE

As informações devem ser acessadas apenas por pessoas autorizadas.



INTEGRIDADE

As informações devem ser precisas, completas e protegidas contra alterações indevidas.



DISPONIBILIDADE

As informações devem estar disponíveis para as pessoas autorizadas sempre que necessário.

BOAS PRÁTICAS EM RH



Acesso restrito

Conceder acesso apenas ao que é necessário para cada função.



Políticas e procedimentos

Definir e comunicar regras claras sobre o uso das informações.



Treinamento e conscientização

Capacitar colaboradores sobre segurança e privacidade de dados.



Senhas fortes e autenticação

Utilizar senhas seguras e, sempre que possível, autenticação em duas etapas.



Backup e recuperação

Realizar cópias de segurança regularmente e testar a recuperação de dados.

RISCOS E AMEAÇAS COMUNS



Acesso não autorizado

Acesso indevido por pessoas não autorizadas aos dados de RH.



Phishing e engenharia social

Técnicas para enganar colaboradores e obter informações sensíveis.



Malware e ransomware

Softwares maliciosos que podem roubar, criptografar ou destruir dados.



Perda ou vazamento de dados. Vazamento accidental ou intencional de informações sigilosas.



Erro humano

Falhas por descuido, envio de informações para pessoas ou locais incorretos.

CONFORMIDADE LEGAL

A área de RH deve seguir as leis e normas de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados Pessoais).

- Coleta e uso de dados com finalidade específica
- Consentimento do titular
- Direito de acesso, correção e exclusão de dados
- Relato de incidentes à autoridade competente



CONTROLE DE ACESSO

- Definir perfis de acesso por função
- Revisar acessos periodicamente
- Revogar acessos de colaboradores desligados ou transferidos
- Registrar logs de acesso e atividades



Usuário → Autenticação → Permissão → Acesso permitido



RESPOSTA A INCIDENTES

Em caso de incidente de segurança:

- Identificar e conter o incidente
- Avaliar o impacto
- Comunicar as partes envolvidas
- Registrar o ocorrido
- Adotar medidas corretivas para evitar novos incidentes



Reporte imediatamente qualquer suspeita de incidente ao time de segurança ou ao responsável de TI.

BENEFÍCIOS DA SEGURANÇA DA INFORMAÇÃO EM RH



Protege a privacidade e a confiança dos colaboradores



Evita prejuízos financeiros e legais



Fortalece a imagem e a reputação da empresa



Garante conformidade com leis e normas



Promove uma cultura organizacional ética e responsável



Segurança da informação é responsabilidade de todos!

Ao proteger os dados de RH, protegemos pessoas e construímos um ambiente de trabalho mais seguro e confiável.



Introdução ao Capítulo III

No cenário digital atual, a segurança da informação tornou-se uma preocupação central para todas as organizações, especialmente no que diz respeito aos dados sensíveis de Recursos Humanos. Este capítulo aborda a Gestão de Segurança da Informação de forma técnica, científica e estratégica, explorando os seus conceitos fundamentais, princípios basilares e os riscos e ameaças informáticas que as organizações enfrentam. Analisaremos as políticas e tecnologias de segurança, com um foco particular na segurança da informação em RH, e discutiremos a importância da gestão de incidentes e da continuidade de negócios para proteger os ativos informacionais e garantir a resiliência organizacional.

3.1 Conceito de Segurança da Informação

A Segurança da Informação pode ser definida como a proteção da informação e dos sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de garantir a confidencialidade, integridade e disponibilidade da informação [6]. É um campo multidisciplinar que envolve tecnologia, processos e pessoas, visando salvaguardar os ativos informacionais de uma organização.

Os principais objetivos da segurança da informação são amplamente reconhecidos como a tríade CIA (Confidencialidade, Integridade e Disponibilidade), à qual se adicionam frequentemente a Autenticidade e o Não Repúdio:

- ✓ **Confidencialidade:** Garantir que a informação é acessível apenas por pessoas autorizadas.
- ✓ **Integridade:** Assegurar que a informação é precisa e completa, e que não foi modificada de forma não autorizada.
- ✓ **Disponibilidade:** Garantir que os utilizadores autorizados têm acesso à informação e aos sistemas quando necessário.

Importância Organizacional -A importância da segurança da informação para as organizações é crescente. A violação de dados pode resultar em perdas financeiras significativas, danos à reputação, multas regulatórias (como as impostas pelo GDPR) e perda de confiança dos clientes e colaboradores. Uma gestão de segurança robusta protege os ativos críticos, mantém a continuidade dos negócios e sustenta a vantagem competitiva.

3.2 Princípios da Segurança da Informação

Os princípios da segurança da informação são a base para a implementação de estratégias e políticas eficazes.

Confidencialidade- A confidencialidade é a garantia de que a informação não será divulgada a indivíduos, entidades ou processos não autorizados. Métodos para garantir a confidencialidade incluem criptografia, controlo de acesso e políticas de privacidade. Em RH, isto é crucial para proteger dados sensíveis como salários, informações médicas e avaliações de desempenho.

Integridade- A integridade assegura que a informação é precisa, completa e não foi alterada de forma não autorizada. Mecanismos como hashing, assinaturas digitais e controlo de versões são utilizados para manter a integridade dos dados. É vital para a fiabilidade dos registos de RH e para a tomada de decisões baseadas em dados.

Disponibilidade- A disponibilidade garante que os sistemas e a informação estão acessíveis e operacionais para os utilizadores autorizados quando necessário. Isto envolve a implementação de redundância, backups, planos de recuperação de desastres e manutenção adequada dos sistemas. A interrupção dos sistemas de RH pode paralisar operações críticas como o processamento de salários ou o recrutamento.

Autenticidade- A autenticidade verifica a identidade de um utilizador, processo ou sistema. Garante que a entidade que se apresenta é quem diz ser. Métodos incluem senhas, autenticação multifator e certificados digitais.

Não Repúdio- O não repúdio garante que uma parte não pode negar a autoria de uma ação ou transação. Por exemplo, um colaborador não pode negar ter acedido a um determinado documento se houver registos que comprovem o acesso.

3.3 Riscos e Ameaças Informáticas

As organizações estão constantemente expostas a uma vasta gama de riscos e ameaças informáticas que podem comprometer a segurança da informação.

RISCOS E AMEAÇAS INFORMÁTICAS EM RH

A informação em Recursos Humanos é sensível, estratégica e valiosa. Proteger esses dados é proteger pessoas e o negócio.

O QUE SÃO?
Riscos são possibilidades de algo causar dano à organização. Ameaças são ações ou eventos que exploram vulnerabilidades para causar esses danos.

PRINCIPAIS RISCOS E AMEAÇAS INFORMÁTICAS EM RH

1 PHISHING E ENGENHARIA SOCIAL  E-mails ou mensagens falsas que enganam colaboradores para roubar credenciais ou dados confidenciais.	2 MALWARE E RANSOMWARE  Softwares maliciosos que invadem sistemas, bloqueiam dados e podem exigir resgate para liberação.	3 ACESSO NÃO AUTORIZADO  Invasores ou usuários internos obtêm acesso indevido a informações sensíveis de colaboradores.	4 VAZAMENTO DE DADOS  Divulgação acidental ou intencional de dados pessoais, salariais ou médicos de colaboradores.
5 PERDA OU ROUBO DE DISPOSITIVOS  Dispositivos com informações de RH podem ser perdidos ou roubados, causando vazamento de dados.	6 SENHAS FRACAS OU COMPARTILHADAS  Credenciais fracas ou compartilhadas facilitam o acesso indevido aos sistemas de RH.	7 FALHAS DE SISTEMA E SOFTWARE  Vulnerabilidades e sistemas desatualizados podem ser explorados por atacantes.	8 AMEAÇAS INTERNAS  Ações maliciosas ou negligentes de colaboradores podem comprometer dados e sistemas.

IMPACTOS PARA A ORGANIZAÇÃO

- Prejuízos financeiros e operacionais
- Multas e sanções legais (LGPD)
- Danos à imagem e reputação da empresa
- Perda de confiança dos colaboradores
- Interrupção de processos de RH

PRINCIPAIS PONTOS DE VULNERABILIDADE EM RH

- E-mails e comunicações sem verificação
- Armazenamento inadequado de documentos
- Excesso de acessos e permissões
- Falta de backups ou backups não testados
- Sistemas desatualizados
- Falta de conscientização dos colaboradores

BOAS PRÁTICAS PARA REDUZIR RISCOS E AMEAÇAS

POLÍTICAS DE SEGURANÇA Definir e comunicar regras claras para o uso seguro da informação.	CONTROLE DE ACESSO Conceder acessos apenas ao necessário (princípio do menor privilégio).	TREINAMENTO E CONSCIENTIZAÇÃO Capacitar colaboradores para identificar e evitar ameaças.	ATUALIZAÇÕES REGULARES Manter sistemas e softwares sempre atualizados para corrigir vulnerabilidades.	BACKUPS REGULARES Realizar cópias de segurança e testar restauração dos dados periodicamente.	CONFORMIDADE E PRIVACIDADE Adequar-se à LGPD e outras normas de proteção de dados.
---	---	--	---	---	--

LEMBRE-SE
Segurança da informação em RH não é apenas tecnologia, é também cultura, processos e pessoas. **Proteger dados é valorizar pessoas!**

- ✓ **Malware-** Malware (software malicioso) é um termo genérico que inclui vírus, worms, trojans, ransomware e spyware. Estes programas são projetados para danificar, roubar ou controlar sistemas informáticos, causando interrupções e perdas de dados.
- ✓ **Phishing** - Phishing é uma técnica de engenharia social onde atacantes tentam obter informações sensíveis (como nomes de utilizador, senhas e detalhes de cartão de crédito) disfarçando-se de uma entidade confiável numa comunicação eletrónica. É uma ameaça comum em RH, visando credenciais de acesso a SIRH ou dados de colaboradores.
- ✓ **Engenharia Social-** A engenharia social é a manipulação psicológica de pessoas para que realizem ações ou divulguem informações confidenciais. Vai além do phishing, explorando a confiança e a ingenuidade humana para contornar as defesas de segurança.
- ✓ **Vazamento de Dados-** O vazamento de dados ocorre quando informações sensíveis são expostas a indivíduos não autorizados. Pode ser resultado de ataques cibernéticos, erros humanos, falhas de sistema ou roubo de dispositivos. Em RH, o vazamento de dados de colaboradores pode ter sérias consequências legais e de reputação.
- ✓ **Ataques Cibernéticos-** Os ataques cibernéticos são tentativas deliberadas de comprometer a segurança de sistemas informáticos, redes ou dados. Incluem ataques de negação de serviço (DDoS), invasões de sistemas, exploração de vulnerabilidades e roubo de credenciais.

3.4 Políticas de Segurança da Informação

As políticas de segurança da informação são diretrizes formais que estabelecem as regras e os procedimentos para proteger os ativos informacionais de uma organização.

- ✓ **Normas Organizacionais-** As normas organizacionais definem o comportamento aceitável e as responsabilidades dos colaboradores em relação à segurança da informação. Devem ser claras, concisas e comunicadas a todos os membros da organização. Exemplos incluem políticas de uso aceitável de recursos de TI, políticas de senhas e políticas de classificação de dados.
- ✓ **Governança-** A governança da segurança da informação refere-se à estrutura de liderança, processos e controlos que garantem que a segurança da informação apoia e

alinha-se com os objetivos gerais da organização. Envolve a definição de papéis e responsabilidades, a gestão de riscos e a supervisão do desempenho da segurança.

- ✓ **Compliance-** O compliance (conformidade) é a adesão a leis, regulamentos, normas e padrões internos e externos relacionados com a segurança da informação. Em RH, isto inclui a conformidade com o GDPR, leis de privacidade de dados e regulamentos específicos do setor.
- ✓ **Auditoria-** A auditoria de segurança da informação é um exame sistemático e independente das políticas, procedimentos e sistemas de segurança para determinar se estão a funcionar conforme o esperado e se estão em conformidade com os requisitos. Ajuda a identificar vulnerabilidades e a garantir a eficácia das medidas de segurança.

3.5 Segurança da Informação em Recursos Humanos

A segurança da informação em RH é um domínio crítico, dada a natureza sensível dos dados de colaboradores e a importância de proteger a privacidade.

- ✓ **Segurança de Dados dos Colaboradores-** A segurança de dados dos colaboradores envolve a proteção de informações pessoais, financeiras, de saúde e de desempenho. Os SIRH devem ser configurados com controlos de acesso rigorosos, criptografia de dados e monitorização de atividades para prevenir acessos não autorizados e vazamentos.
- ✓ **Controlo de Acessos-** O controlo de acessos garante que apenas utilizadores autorizados podem aceder a recursos específicos do SIRH. Isto é implementado através de mecanismos como autenticação (verificação de identidade) e autorização (definição de permissões de acesso com base no princípio do menor privilégio).
- ✓ **Segurança em Recrutamento Digital-** O recrutamento digital envolve a recolha e o processamento de grandes volumes de dados de candidatos. A segurança neste processo é vital para proteger a privacidade dos candidatos e evitar fraudes. Inclui a utilização de plataformas seguras, a proteção de dados em trânsito e em repouso, e a eliminação segura de dados de candidatos não selecionados.
- ✓ **Segurança no Teletrabalho-** O teletrabalho introduziu novos desafios de segurança, uma vez que os colaboradores acedem aos sistemas da empresa a partir de redes domésticas

menos seguras e dispositivos pessoais. As organizações devem implementar VPNs, políticas de segurança para dispositivos pessoais, formação em segurança e monitorização remota para mitigar estes riscos.

3.6 Tecnologias de Segurança

Diversas tecnologias são empregadas para fortalecer a postura de segurança da informação.

- ✓ **Criptografia-** A criptografia é o processo de transformar informação em um código para evitar o acesso não autorizado. É utilizada para proteger dados em repouso (armazenados) e em trânsito (transmitidos), garantindo a confidencialidade e a integridade.
- ✓ **Firewalls-** Firewalls são sistemas de segurança de rede que monitorizam e controlam o tráfego de rede de entrada e saída com base em regras de segurança predeterminadas. Atuam como uma barreira entre uma rede interna confiável e redes externas não confiáveis, como a internet.
- ✓ **Backup-** O backup é a cópia de dados para que possam ser recuperados em caso de perda de dados ou falha do sistema. É uma medida essencial para garantir a disponibilidade da informação e a continuidade dos negócios.
- ✓ **Sistemas de Autenticação-** Os sistemas de autenticação verificam a identidade dos utilizadores. Além das senhas, incluem autenticação multifator (MFA), biometria (impressões digitais, reconhecimento facial) e tokens de segurança, aumentando a robustez do controlo de acessos.
- ✓ **Segurança em Cloud-** A segurança em cloud refere-se às políticas, tecnologias e controlos implementados para proteger dados, aplicações e infraestruturas baseadas na nuvem. É uma responsabilidade partilhada entre o fornecedor de serviços cloud e o cliente, exigindo uma gestão cuidadosa das configurações de segurança e conformidade.

3.7 Gestão de Incidentes e Continuidade

Apesar de todas as medidas preventivas, incidentes de segurança podem ocorrer. A capacidade de uma organização de responder eficazmente a estes incidentes e de manter a continuidade dos negócios é crucial.

- ✓ **Gestão de Riscos-** A gestão de riscos é o processo de identificar, avaliar e mitigar os riscos de segurança da informação. Envolve a análise de vulnerabilidades, a avaliação da probabilidade e do impacto de ameaças, e a implementação de controlos para reduzir a exposição a riscos inaceitáveis.
- ✓ **Planos de Contingência-** Os planos de contingência são procedimentos detalhados que descrevem as ações a serem tomadas em resposta a um incidente de segurança ou falha de sistema. O objetivo é minimizar o impacto e restaurar as operações o mais rapidamente possível.
- ✓ **Recuperação de Desastres-** A recuperação de desastres (DR) é um conjunto de políticas e procedimentos para permitir a recuperação ou continuação da infraestrutura tecnológica vital e dos sistemas após um desastre natural ou causado pelo homem. Foca-se na restauração de sistemas e dados.
- ✓ **Continuidade de Negócios-** A continuidade de negócios (BC) é a capacidade de uma organização de continuar a fornecer produtos ou serviços em níveis aceitáveis predefinidos após um incidente disruptivo. Abrange não apenas a recuperação de TI, mas também a recuperação de processos de negócio, instalações e pessoal.

Conclusão do Capítulo III

O Capítulo III sublinhou a importância crítica da gestão de segurança da informação no contexto dos Sistemas de Informação em Recursos Humanos. A proteção dos dados de colaboradores contra ameaças cibernéticas e acessos não autorizados é uma responsabilidade fundamental, que exige a implementação de políticas robustas, tecnologias avançadas e uma cultura organizacional consciente da segurança. A compreensão dos princípios da confidencialidade, integridade e disponibilidade, juntamente com a capacidade de gerir riscos, incidentes e garantir a continuidade dos negócios, são competências indispensáveis para os profissionais de RH e de TI. A segurança da informação não é apenas uma questão técnica, mas um pilar estratégico que sustenta a confiança, a conformidade e a resiliência das organizações na era digital.

Perguntas de Avaliação

Verdadeiro ou Falso

1. A Confidencialidade, Integridade e Disponibilidade (CIA) são os únicos princípios da segurança da informação. **(F)**
2. Phishing é uma técnica de ataque que explora vulnerabilidades de software para instalar malware. **(F)**
3. O controlo de acessos em SIRH deve seguir o princípio do menor privilégio. **(V)**
4. A criptografia é utilizada principalmente para garantir a disponibilidade dos dados. **(F)**
5. A gestão de riscos é um processo reativo, focado apenas na resposta a incidentes após a sua ocorrência. **(F)**

Escolha Múltipla

1. Qual dos seguintes princípios da segurança da informação garante que a informação é acessível apenas por pessoas autorizadas?
a) Integridade
b) Disponibilidade
c) Confidencialidade
d) Não Repúdio
2. Qual tipo de malware é projetado para bloquear o acesso a um sistema informático até que um resgate seja pago?
a) Vírus
b) Worm
c) Ransomware
d) Spyware
3. Qual das seguintes não é uma medida de segurança recomendada para o teletrabalho? a) Utilização de VPNs.
b) Políticas de segurança para dispositivos pessoais.
c) Partilha de senhas para facilitar o acesso.
d) Formação em segurança para colaboradores.
4. O GDPR (Regulamento Geral sobre a Proteção de Dados) é um exemplo de:

a) Tecnologia de segurança.

b) Ameaça informática.

c) Regulamentação de compliance.

d) Princípio de engenharia social.

5. A principal diferença entre Recuperação de Desastres (DR) e Continuidade de Negócios (BC) é **que:**

a) DR foca-se na recuperação de sistemas e dados, enquanto BC abrange a recuperação de todos os processos de negócio.

b) BC foca-se na recuperação de sistemas e dados, enquanto DR abrange a recuperação de todos os processos de negócio.

c) DR e BC são termos sinónimos e podem ser usados indistintamente.

d) DR é uma estratégia preventiva, enquanto BC é uma estratégia reativa.

Guião de correção

Verdadeiro ou Falso: 1. F, 2. F, 3. V, 4. F, 5. F

Escolha Múltipla: 1. c, 2. c, 3. c, 4. c, 5. a

Exercícios Complementares

1. Estudo de Caso: Uma empresa de consultoria de RH sofreu um ataque de ransomware que cifrou todos os seus dados de colaboradores. Discuta as etapas que a empresa deveria seguir no seu plano de gestão de incidentes, as medidas de recuperação de desastres e como poderia ter prevenido o ataque através de políticas de segurança e tecnologias adequadas.

2. Perguntas para Debate:

Como as organizações podem equilibrar a necessidade de segurança robusta com a usabilidade dos sistemas para os colaboradores?

Qual o papel da cultura organizacional na promoção de uma postura de segurança eficaz?

3. Atividades Práticas:

Elabore um pequeno plano de contingência para um cenário de perda de acesso ao SIRH devido a uma falha de energia prolongada, incluindo os passos a seguir e as responsabilidades.

Pesquise sobre as principais certificações de segurança da informação (ex: ISO 27001, CISSP) e discuta a sua relevância para profissionais de RH que lidam com SIRH.

4. Análise Crítica: Analise a afirmação: “A segurança da informação é uma responsabilidade exclusiva do departamento de TI.” Discuta o papel de cada colaborador na segurança da informação da organização.

IV-Sistema de Informação em Gestão de Recursos Humanos

4.1 O SIRH como Parceiro Estratégico da Organização

A transição do SIRH de sistema administrativo para plataforma estratégica constitui uma das transformações mais significativas na história da gestão de recursos humanos. Esta transição não ocorre de forma automática com a implementação de tecnologia sofisticada, mas exige uma reorientação profunda da forma como a função de RH conceptualiza o seu papel e utiliza a informação disponível (Lawler & Boudreau, 2015).

Ulrich e Brockbank (2005) propõem um modelo de RH estratégico assente em cinco papéis complementares: defensor dos colaboradores, desenvolvedor de capital humano, expert funcional, parceiro estratégico e líder de RH. O SIRH é o habilitador tecnológico que permite ao profissional de RH exercer cada um destes papéis com base em evidências, antecipando necessidades organizacionais e propondo soluções fundamentadas em dados. Neste enquadramento, o SIRH deixa de ser uma ferramenta de registo para se tornar uma plataforma de inteligência organizacional.

4.2 Integração do SIRH com Outros Sistemas Organizacionais

Um SIRH moderno não opera em isolamento, mas integra-se com múltiplos sistemas organizacionais numa arquitectura de informação coerente. A qualidade desta integração é determinante para a eliminação de silos de informação e para a criação de uma visão holística e em tempo real do capital humano como factor estratégico.

Sistema a Integrar	Natureza e Benefício da Integração
ERP (SAP, Oracle, Microsoft D365)	Integração financeira: dados de headcount e custos salariais reflectidos em tempo real na contabilidade; planeamento de workforce alinhado com orçamentos.
Sistemas de Business Intelligence (BI)	Alimentação de data warehouses de RH; dashboards estratégicos com KPIs de talento, produtividade e custo; relatórios de gestão integrados.
Plataformas de Colaboração (Teams, Slack)	Integração de fluxos de aprovação HR (férias, despesas); notificações automáticas; onboarding digital colaborativo.
Sistemas de Controlo de Acesso Físico	Sincronização automática de permissões de acesso com o status do colaborador no SIRH; revogação imediata no offboarding.
Plataformas de Learning (LMS)	Sincronização de catálogos de formação; automatização de inscrições baseada em planos de desenvolvimento; registo automático de competências.
Sistemas de Gestão de Desempenho (externos)	Integração de feedbacks e OKRs com o módulo de avaliação; continuidade entre ciclos de avaliação e planos de carreira.

4.3 Inteligência Artificial e Automação no SIRH

A integração de Inteligência Artificial (IA) e automação nos SIRH representa a fronteira mais disruptiva da gestão contemporânea de recursos humanos. As aplicações de IA em RH cobrem um espectro cada vez mais amplo de processos, desde a triagem automática de candidaturas até à previsão de rotatividade e à personalização da experiência do colaborador.

Cappelli (2019) identifica quatro áreas de aplicação prioritárias da IA em RH: triagem automatizada de candidaturas (redução de tempo de análise em 75%); análise preditiva de turnover (antecipação de saídas com meses de antecedência); personalização da formação e desenvolvimento (cursos recomendados com base no perfil e nos objectivos individuais); e automação de respostas a consultas de colaboradores através de chatbots de RH. Contudo, a mesma literatura alerta para os riscos de viés algorítmico: sistemas de IA treinados em dados históricos tendem a replicar e amplificar preconceitos existentes, como demonstrado no caso do

sistema de recrutamento automático da Amazon, descontinuado em 2018 por favorecer sistematicamente candidatos masculinos (Dastin, 2018).

ROBOTIC PROCESS AUTOMATION (RPA) EM RH

A RPA tecnologia que automatiza tarefas repetitivas baseadas em regras através de robots de software tem encontrado aplicações crescentes em processos de RH. O processamento automático de contratos de onboarding, a reconciliação de dados entre sistemas de RH e financeiros, a geração automática de declarações para entidades reguladoras e a automatização do envio de comunicações a candidatos são exemplos de processos de RH altamente adequados à RPA, com ganhos de eficiência tipicamente superiores a 70% (Deloitte, 2021).

4.4 Transformação Digital da Função de RH através do SIRH

A transformação digital da função de RH não se resume à adoção de novas tecnologias, mas implica uma mudança profunda nos modelos de trabalho, nas competências requeridas e na cultura da própria função. Westerman et al. (2014) definem a transformação digital como a integração de tecnologia digital em todas as áreas de uma organização, transformando fundamentalmente o modo como opera e entrega valor. No contexto de RH, esta transformação manifesta-se em três dimensões interligadas.

A primeira dimensão é a digitalização dos processos conversão de processos analógicos em digitais, eliminando papel e automatizando tarefas administrativas. A segunda é a transformação dos processos redesenho fundamental dos processos de RH à luz das possibilidades tecnológicas, e não apenas a sua digitalização superficial. A terceira, e mais profunda, é a transformação do modelo de negócio de RH reposicionamento da função como unidade de criação de valor estratégico, orientada por dados e focada na experiência do colaborador e no impacto organizacional mensurável.

4.5 Métricas e KPIs de RH Suportados pelo SIRH

Uma das principais contribuições estratégicas do SIRH é a capacidade de medir, monitorizar e comunicar o impacto da gestão de pessoas através de indicadores-chave de desempenho (KPIs) rigorosos. Boudreau e Ramstad (2007) argumentam que a função de RH só pode aspirar a um

papel verdadeiramente estratégico quando é capaz de demonstrar, com dados factuais, a sua contribuição para os resultados organizacionais.

Categoria de KPI	Indicador	Fórmula / Descrição
Recrutamento	Time to Fill	Dias entre abertura da vaga e aceitação de oferta. Benchmark: 25–45 dias.
Recrutamento	Cost per Hire	$(\text{Custos internos} + \text{externos}) / \text{N}^{\circ} \text{ contratações}$. Benchmark: 4.000–7.000 USD.
Retenção	Taxa de Turnover Voluntário	$(\text{Saídas voluntárias} / \text{Média colaboradores}) \times 100$. Benchmark: < 10%/ano.
Desempenho	Índice de Engagement	Score de inquérito de engagement. Benchmark: > 70% colaboradores engaged.
Formação	ROI de Formação	$(\text{Benefícios} - \text{Custos formação}) / \text{Custos formação} \times 100$. Modelo Kirkpatrick.
Diversidade	Índice de Paridade de Género	Distribuição % por género em cada nível hierárquico. Objectivo: paridade.
Custo	Custo de RH por Colaborador	$\text{Total custos de RH} / \text{Total colaboradores}$. Benchmark varia por sector.
Saúde Org.	Taxa de Absentismo	$(\text{Dias ausentes} / \text{Dias úteis totais}) \times 100$. Benchmark: < 3,5%/ano.

4.6 Tendências Emergentes nos SIRH (2025–2030)

O futuro dos SIRH é moldado por um conjunto de tendências tecnológicas e organizacionais convergentes que os profissionais de RH devem acompanhar criticamente, avaliando as suas implicações e oportunidades para a gestão estratégica de pessoas.

- Skills-Based HR: migração de modelos baseados em cargos para modelos baseados em competências (skills), com SIRH que mapeiam e recomendam projectos com base no portfólio de competências individuais. Exemplo: plataformas como o Eightfold AI.
- Generative AI em RH: chatbots de RH com LLMs capazes de responder a perguntas complexas de colaboradores, gerar descrições de funções personalizadas e sugerir planos de desenvolvimento individuais.
- Total Workforce Management: gestão integrada de colaboradores efectivos, trabalhadores a prazo, freelancers e robots no mesmo SIRH, reflectindo a crescente diversidade das formas de trabalho.
- Employee Experience Platforms (EXP): plataformas centradas na experiência holística do colaborador, integrando SIRH, ferramentas de colaboração, wellbeing e desenvolvimento numa interface única.
- Blockchain em RH: verificação imutável e descentralizada de credenciais académicas e profissionais, eliminando fraudes em CVs e acelerando processos de recrutamento e onboarding.

4.7 Conclusão do Capítulo IV

O percurso traçado ao longo deste manual evidenciou que os Sistemas de Informação em Gestão de Recursos Humanos constituem muito mais do que ferramentas tecnológicas: são arquiteturas estratégicas que moldam a capacidade das organizações de gerir, desenvolver e reter o seu capital humano. A sua eficácia depende de uma trilogia indissociável: qualidade dos dados que os alimentam, robustez da segurança que os protege e maturidade analítica que transforma informação em decisões de valor.

O profissional de RH do século XXI é, necessariamente, um profissional tecnológico, analítico e estratégico. O domínio dos SIRH dos seus fundamentos teóricos, das suas aplicações práticas, dos seus riscos e das suas implicações éticas é o alicerce sobre o qual se constrói a capacidade de gerir pessoas de forma mais fundamentada, mais justa e mais impactante. É este o horizonte que este manual, enquanto instrumento de formação avançada, procurou iluminar.

Perguntas de Avaliação

Questões de Escolha Múltipla

1. De acordo com Ulrich (1997), qual é o papel do SIRH no contexto do modelo de RH como parceiro estratégico?

- a) Substituir os profissionais de RH por processos automatizados de baixo custo operacional.
- b) Centralizar todas as decisões de RH num sistema automatizado para eliminar subjectividade.
- c) Habilitar o profissional de RH a exercer múltiplos papéis estratégicos com base em evidências e dados. ✓**
- d) Garantir exclusivamente a conformidade legal e regulatória da função de RH.

2. O conceito de Skills-Based HR, enquanto tendência emergente nos SIRH, refere-se a:

- a) A avaliação das competências técnicas de TI dos profissionais de RH para gerir os sistemas.
- b) A migração de modelos organizacionais baseados em cargos para modelos baseados em competências individuais. ✓**
- c) A formação obrigatória de todos os colaboradores em ferramentas de SIRH cloud.
- d) A automatização completa do processo de recrutamento com base em análise de competências por IA.

3 . O KPI 'Cost per Hire' é calculado como:

- a) Custo total do departamento de RH dividido pelo número total de colaboradores.

- b) Salário anual médio dos novos colaboradores dividido pelo número de contratações.
- c) Soma dos custos internos e externos de recrutamento dividida pelo número de contratações. ✓**
- d) Custo de formação de novos colaboradores no primeiro ano de actividade.

4. Qual das seguintes afirmações sobre viés algorítmico em sistemas de IA aplicados ao recrutamento é cientificamente correcta?

- a) Os algoritmos de IA são por natureza objectivos e imparciais, eliminando os preconceitos humanos.
- b) O viés algorítmico só ocorre quando os programadores introduzem preconceitos de forma consciente.
- c) Sistemas de IA treinados em dados históricos tendem a replicar e amplificar preconceitos existentes. ✓**
- d) A legislação europeia RGPD proíbe completamente o uso de IA em processos de recrutamento.

Questões de Verdadeiro ou Falso

1. Os Sistemas de Informação de Recursos Humanos são constituídos exclusivamente por componentes tecnológicos, sendo as pessoas e os processos elementos secundários e substituíveis. (F)
2. O 'Recovery Time Objective' (RTO) define o tempo máximo aceitável de indisponibilidade de um sistema crítico, como um SIRH, após um incidente de segurança ou falha técnica. (V)
3. O RGPD exige que as violações de dados pessoais sejam notificadas à autoridade de protecção de dados competente no prazo máximo de 72 horas após o responsável tomar conhecimento da violação. (V)
4. O modelo de implementação de SIRH em cloud (SaaS) é sempre a opção mais segura e fiável para todas as organizações, independentemente do seu sector de actividade ou dos requisitos regulatórios aplicáveis.(F)
5. O conceito de 'Insider Threat' na segurança de SIRH refere-se exclusivamente a ataques de hackers externos que se fazem passar por colaboradores da organização.(F)
- 6 . A integração de sistemas de controlo de acesso físico com o SIRH permite a revogação automática de permissões de acesso a instalações quando um colaborador é registado como tendo saído da organização no sistema de RH. (V)

Conclusões Gerais do Manual

A elaboração deste Manual Acadêmico e Científico de Sistemas de Informação em Recursos Humanos (SIRH) permitiu uma exploração profunda e integrada da tecnologia no contexto da gestão de pessoas. Ao longo dos três capítulos, ficou evidente que os SIRH não são apenas ferramentas de automatização administrativa, mas sim pilares estratégicos que sustentam a eficiência, a inovação e a vantagem competitiva das organizações modernas.

No Capítulo I, compreendemos a evolução dos Sistemas de Informação e o papel central dos SIRH na otimização das funções de RH. A transição de sistemas puramente transacionais para soluções inteligentes e integradas reflete a necessidade de as organizações gerirem o seu capital humano de forma mais ágil e informada.

O Capítulo II destacou a importância vital da gestão de dados. A qualidade da informação, o ciclo de vida dos dados e a emergência da People Analytics foram identificados como elementos cruciais para transformar dados brutos em insights valiosos, permitindo uma tomada de decisão fundamentada e estratégica. Ao mesmo tempo, a necessidade de ética e proteção de dados, em conformidade com o GDPR, sublinhou a responsabilidade das organizações em proteger a privacidade dos seus colaboradores.

Finalmente, no Capítulo III, abordámos a gestão de segurança da informação como uma necessidade imperativa. A proteção contra ameaças cibernéticas, a implementação de políticas robustas e a preparação para a continuidade de negócios são essenciais para garantir a resiliência organizacional e a confiança dos stakeholders.

Em conclusão, o sucesso na implementação e gestão de um SIRH exige uma abordagem holística que integre tecnologia, processos e pessoas. Os profissionais de Recursos Humanos do futuro devem possuir não apenas competências de gestão de

pessoas, mas também uma literacia digital sólida e uma visão estratégica sobre o papel da informação. Este manual espera ter contribuído para a formação avançada de estudantes de mestrado, preparando-os para liderar a transformação digital em RH com rigor científico e aplicação prática.

Glossário Técnico

Autenticação: Processo de verificação da identidade de um utilizador, sistema ou dispositivo.

Backup: Cópia de segurança de dados para permitir a sua recuperação em caso de perda ou falha.

Big Data: Conjuntos de dados extremamente grandes e complexos que requerem tecnologias avançadas para processamento e análise.

Business Intelligence (BI): Tecnologias e processos que transformam dados brutos em informações úteis para análise de negócios.

Cloud Computing: Entrega de serviços de computação (servidores, armazenamento, bases de dados, etc.) através da internet.

Compliance: Adesão a leis, regulamentos, normas e padrões.

Confidencialidade: Garantia de que a informação é acessível apenas por pessoas autorizadas.

Criptografia: Processo de codificação de informação para evitar o acesso não autorizado.

Data Warehouse: Repositório centralizado de dados integrados de várias fontes, utilizado para análise e relatórios.

Enterprise Resource Planning (ERP): Sistema integrado que gere todos os processos de negócio de uma organização.

Firewall: Sistema de segurança de rede que monitoriza e controla o tráfego com base em regras de segurança.

GDPR (General Data Protection Regulation): Regulamento da União Europeia sobre a proteção de dados e privacidade.

Integridade: Garantia de que a informação é precisa e não foi alterada de forma não autorizada.

People Analytics: Aplicação de técnicas de análise de dados aos recursos humanos para melhorar a tomada de decisão.

Phishing: Técnica de engenharia social para obter informações sensíveis de forma fraudulenta.

Sistemas de Apoio à Decisão (SAD): Sistemas que auxiliam gestores na tomada de decisões complexas.

Sistemas de Informação em Recursos Humanos (SIRH): Soluções tecnológicas que integram e automatizam as funções de RH.

Referências Bibliográficas

- ISO/IEC 27000:2018. (2018). Information technology Security techniques Information security management systems Overview and vocabulary. International Organization for Standardization.
- Kavanagh, M. J., & Johnson, R. D. (2020). Human resource information systems: Basics, applications, and future directions (5.^a ed.). SAGE Publications.
- Laudon, K. C., & Laudon, J. P. (2020). Management information systems: Managing the digital firm (16.^a ed.). Pearson.
- Marler, J. H., & Boudreau, J. W. (2017). An evidence-based review of HR analytics. *The International Journal of Human Resource Management*, 28(1), 3–26. <https://doi.org/10.1080/09585192.2016.1244699>
- O'Brien, J. A., & Marakas, G. M. (2011). Management information systems (10.^a ed.). McGraw-Hill/Irwin.
- Tannenbaum, S. I. (1990). HRIS: User group implications. *Journal of Systems Management*, 41(1), 27–32.
- Barocas, S., & Hardt, M. (2019). Fairness and machine learning: Limitations and opportunities. fairmlbook.org.
- Boudreau, J. W., & Ramstad, P. M. (2007). Beyond HR: The new science of human capital. Harvard Business School Press.
- Cappelli, P. (2019). Your approach to hiring is all wrong. *Harvard Business Review*, 97(3), 48–58.
- Dastin, J. (2018, October 10). Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>
- Date, C. J. (2004). An introduction to database systems (8th ed.). Pearson Addison Wesley.
- Deloitte. (2021). The future of work in technology: Automation, AI and the workforce. Deloitte Insights.
- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. International Organization for Standardization.

Kavanagh, M. J., & Johnson, R. D. (Eds.). (2021). Human resource information systems: Basics, applications, and future directions (5th ed.). SAGE Publications.

Lawler, E. E., & Boudreau, J. W. (2015). Global trends in human resource management: A twenty-year analysis. Stanford University Press.

Marler, J. H., & Boudreau, J. W. (2017). An evidence-based review of HR analytics. *The International Journal of Human Resource Management*, 28(1), 3–26. <https://doi.org/10.1080/09585192.2016.1244699>

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Publishers.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 — Regulamento Geral sobre a Proteção de Dados (RGPD). *Jornal Oficial da União Europeia*, L 119, 1–88.

Ulrich, D. (1997). Human resource champions: The next agenda for adding value and delivering results. Harvard Business School Press.

Ulrich, D., & Brockbank, W. (2005). The HR value proposition. Harvard Business School Press.

Verizon. (2023). 2023 data breach investigations report. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Review Press.