

MESG

MESTRADO EM ENGENHARIA DE SERVIÇOS E GESTÃO

Susana Coutinho

Gestão da Segurança da Informação – o caso do Grupo Lactogal

Orientador na FEUP: Professor António C. Brito

Orientador na Lactogal – Produtos Alimentares, S.A.: Engenheira Teresa Sampaio



Universidade do Porto

Faculdade de Engenharia

FEUP

Faculdade de Engenharia da Universidade do Porto

Junho 2012

*À minha Mãe, minha Amiga,
para sempre o maior Amor da minha vida!*

Resumo

A gestão da segurança da informação nas empresas tem vindo a ocupar o centro das preocupações nos últimos anos fruto da crescente evolução tecnológica e do aparecimento de novos modelos de negócio e novas formas de comunicar. A proteção da informação organizacional é por isso encarada como fundamental para garantir a competitividade das empresas e a ela está associada a preservação de três características fundamentais: a confidencialidade, a integridade e a disponibilidade da informação. Atualmente, as abordagens sobre a gestão da segurança da informação têm-se afastado das questões meramente tecnológicas e têm vindo a apostar noutras temáticas como o papel que os utilizadores finais desempenham e a necessidade de serem definidas políticas e procedimentos que suportem os processos a ela associados.

Deste modo, partindo da definição e mapeamento dos processos core, da avaliação do nível de criticidade das actividades associadas a esses processos e da análise dos incidentes que afetam os sistemas de informação, foi desenhado um plano de ação que considerou igualmente as principais dificuldades na utilização dos sistemas de informação e sugestões de melhoria da qualidade dos serviços da DSI (Direção de Sistemas de Informação), deixadas por uma amostra de colaboradores que operam diariamente estes sistemas.

As principais conclusões retiradas deste exercício destacam o papel que os utilizadores finais podem assumir na otimização dos sistemas de informação de uma organização, bem como a necessidade de existir uma política de segurança da informação acessível a todos os colaboradores da empresa, e de procedimentos escritos sobre os processos mais críticos num departamento de sistemas de informação.

Palavras Chave: Gestão da segurança da informação; políticas e procedimentos de segurança da informação; utilizadores finais; processo core; criticidade de processos/atividades de negócio; política de segurança da informação.

Abstract

Information security management has become the center of all concerns in organizations, in recent years has a result of increasing technological developments and the emergence of new business models and new ways to communicate. The protection of organizational information is therefore seen as crucial to assure the competitiveness of enterprises and it is associated with preservation of three fundamental characteristics: confidentiality, integrity and availability of information.

Currently, information security management approaches have been away from purely technical issues and have been focusing on other issues like the role played by end users and the need to define policies and procedures to support the processes associated with it.

Thus, based on the definition and processes modeling, the activities criticality evaluation and on the incident analysis affecting information systems, we designed an action plan which also considered the main difficulties in the use of information systems and suggestions for ISD (Information Systems Department) services quality improvement proposed by a sample of employees who daily operate those systems.

The main conclusions of this exercise highlight the role that end users can take on the optimization of information systems as well as the need for creating an information security policy, available to all employees and written procedures on the most critical processes in a information systems department.

Keywords: Information Security Management; Information Security Policies and Procedures; End-Users role; Core Process; criticality of processes / business activities.

Agradecimentos

A realização deste projeto só foi possível graças ao apoio e colaboração de um conjunto de pessoas a quem desejo expressar o meu sincero agradecimento.

À Dra. Maria Antónia Cadillon, Diretora de Recursos Humanos e Comunicação e ao Eng.º Emanuel Loureiro, Diretor dos Serviços de Informação, por terem permitido a realização deste projeto no Grupo Lactogal.

Ao Professor António Carvalho Brito por ter aceite o desafio de orientar este projeto, pelos seus ensinamentos, pela confiança em mim depositada e pela disponibilidade emprestada.

À Eng.ª Teresa Sampaio, minha orientadora na empresa, por todos os conhecimentos transmitidos, pela paciência, pelo empenho e pela elevada disponibilidade que apesar de limitada pelas numerosas deslocações ao serviço da empresa, nunca deixou de existir.

A todos os colegas do DSI, em particular aos que puderam acompanhar de forma mais próxima a evolução do meu projeto na empresa. Obrigada Sofia, Renato, Sara, Nuno, Franck, Susana, Filipe e Pedro por todo o apoio e, principalmente, pelo excelente ambiente de trabalho que proporcionaram e que em muito facilitou a minha integração na empresa.

Ao Departamento de Recursos Humanos do Grupo Lactogal, em especial à Dra. Clara Alegre pela sua simpatia e total disponibilidade no processo de construção e ministração de questionários aos utilizadores de sistemas de informação.

A todos os colaboradores do Grupo Lactogal manifesto a minha genuína gratidão pelo interesse e disponibilidade que tiveram em participar neste projeto.

A todos os meus professores do MESH por tudo o que com eles aprendi e por terem sido fonte de inspiração em tantos momentos ao longo do mestrado. Seguramente, continuarão a inspirar-me no futuro.

Aos meus colegas do MESH por todos os momentos que vivemos juntos, pelas “noites dentro” passadas na FEUP, pela partilha de ideias e de experiências, pelo apoio que demos uns aos outros, pelo respeito, pelo espírito de união e de entreajuda que nos distingue, pelos desabafos que fizemos, discussões que tivemos e por todas as gargalhadas, obrigada! Agradeço em particular a todos os elementos do meu grupo de trabalho, à Cecília, à Cristina, ao Nuno e ao Pedro, também eles responsáveis pelo sucesso do meu percurso académico.

O maior agradecimento vai para a minha família, as “peças” mais importantes da minha vida e sem as quais nada disto faria qualquer sentido. Obrigada por tudo, mãe, mana e Inês!

Finalmente, agradeço aos meus amigos e amigas pelas injeções de motivação ao longo destes quase dois anos. À Ana, à Daniela, à Sandra, ao Luís, ao Hugo, ao João, ao Miguel, à Joana e ao Migas, muito obrigada!

Abreviaturas

AMP – Armazém Matéria Prima

BIA – Business Impact Analysis

BPMN – *Business Process Modeling Notation*

COBIT – *Control Objectives for Information and Related Technology*

DM – Dados Mestre

DRHC – Direção de Recursos Humanos e Comunicação

DSI – Direção de Sistemas de Informação

EDI – *Electronic Data Interchange*

GR – Gestão de Risco

IAM – *Identity and Access Management*

ITIL – *Information Technology Infrastructure Library*

MP – Matéria Prima

OCTAVE – *Operationally Critical Threat, Asset, and Vulnerability Evaluation*

PA – Produto Acabado

PGI – Processos e Gestão da Informação

RPO – *Recovery Point Objective*

RTO – *Recovery Time Objective*

SLA – *Service Level Agreement*

TI – Tecnologias da Informação

Índice

Resumo	iii
Abstract	iv
Agradecimentos.....	v
Abreviaturas	vi
1 Introdução	1
1.1 A empresa	1
1.2 O Projeto de Dissertação	2
1.3 Metodologia	2
1.4 Estrutura do documento.....	4
2 Revisão Bibliográfica e Estado da Arte	5
2.1 Boas práticas na gestão da segurança da informação	6
2.2 Continuidade do negócio - <i>Business Continuity e Disaster Recovery</i>	9
2.3 O papel do utilizador na segurança dos sistemas de informação	12
3 A gestão da segurança da informação na Lactogal – identificação dos principais problemas	16
3.1 Definição e modelação dos processos core e sistemas de informação que os suportam	17
3.2 Identificação do grau de criticidade de cada processo de negócio.....	20
3.3 Levantamento dos principais incidentes que afetam os sistema de informação da Lactogal	22
3.4 Utilizadores finais - avaliação dos serviços da DSI e diagnóstico de necessidades formativas.	24
4 Plano de ação desenvolvido	30
4.1 Plano de ação orientado para problemas dos utilizadores.....	30
4.2 Plano de ação orientado para problemas relacionados com políticas e procedimentos	31
5 Protótipos desenvolvidos no âmbito do projeto	32
5.1 Proposta de projeto formativo de colaboradores internos a apresentar à DRHC	32
5.2 Política de Segurança da Informação	33
5.3 Procedimentos e matrizes de responsabilidade	33
6 Considerações finais	35
Referências	38
ANEXO A: Mapeamento dos processos core de negócio	41
ANEXO B: Grau de criticidade das atividades dos processos de negócio	42
ANEXO C: Levantamento de incidentes que afetam os SI	43
ANEXO D: Questionário	44
ANEXO E – Identificação de dificuldades dos colaboradores na utilização dos SI	46
ANEXO F – Política de Segurança da Informação do Grupo Lactogal	47
ANEXO G – Manual Procedimentos de Gestão de Identidades.....	48

Índice de Figuras

Figura 1 - Marcas comercializadas pelo Grupo Lactogal	1
Figura 2 - Estrutura funcional do grupo Lactogal	2
Figura 3 - Propriedades da segurança da informação - adaptado de Gibson (2010)	6
Figura 4 - Ciclo de vida da segurança dos sistemas de informação, adaptado de Johnson (2011)	8
Figura 5 - Ciclo de produção leite dia/UHT e derivados (iogurtes e queijo)	17
Figura 6 - Representação do macro processo "Tratar encomenda"	18
Figura 7 - Representação do macro processo "Tratar carga"	19
Figura 8 - Representação do macro processo "Produzir laticínios"	19
Figura 9 - Atividades com classificação de criticidade nível 1 e respectivos sistemas de informação	21
Figura 10 - Sistemas de informação/aplicações críticos	21
Figura 11 - Alvos dos incidentes	22
Figura 12 - Principais incidentes que afetam os sistemas de informação do Grupo Lactogal	23
Figura 13 - Distribuição de níveis de satisfação com serviços da DSI	25
Figura 14 - Categorização das principais sugestões de melhoria	26
Figura 15 - Distribuição de respostas segundo categorias de melhorias propostas	26
Figura 16 - Exemplo do questionário - dificuldades na utilização do módulo WM do SAP ECC	27
Figura 17 - Exemplo do tratamento de necessidades formativas do módulo FI do SAP ECC	28
Figura 18 - Distribuição de respostas da utilização do serviço de <i>helpdesk</i>	29
Figura 19 - Representação das principais áreas-problema na DSI	30
Figura 20 - Exemplo de matriz de responsabilidades criada	34

Índice de Tabelas

Tabela 1 - Fatores que influenciam a prática e cultura da segurança da informação (adaptado de Alnatheer and Nelson 2009)	5
Tabela 2 - Sistema de quatro níveis para classificar a confidencialidade, integridade e disponibilidade da informação do itil	7
Tabela 3 - Missão e responsabilidades da DSI	16
Tabela 4 - Distribuição dos respondentes por sexo e direção	24
Tabela 5 - Exemplo de dificuldades apontadas pelos utilizadores relativamente à utilização do SAP ECC FI	27

1 Introdução

O presente projeto foi desenvolvido em contexto empresarial entre fevereiro e julho de 2012 no Grupo Lactogal, na Direção de Sistemas de Informação (DSI), na área de Gestão de Risco (GR).

1.1 A empresa

A LACTOGAL, Produtos Alimentares S.A., é uma empresa agroalimentar portuguesa especializada em lacticínios e seus derivados. Fundada pela AGROS - União das Cooperativas de Produtores de Leite Entre Douro e o Minho e Trás-os-Montes, UCRL, a LACTICOOP - União das Cooperativas de Produtores de Leite entre Douro e Mondego, UCRL, e a PROLEITE/MIMOSA S.A., o propósito da Lactogal, Produtos Alimentares, S.A. é o de produzir e comercializar, nos mercados nacional e internacional, lacticínios e outros bens alimentares através das suas marcas.

Tem como missão “Fazer com que as pessoas se sintam bem ao longo da vida, com produtos pensados para uma alimentação equilibrada, onde o leite é determinante. Assumir um papel fundamental na valorização da produção de leite nacional”.

A Lactogal, Produtos Alimentares, S.A. produz e comercializa leite, manteiga, natas, queijo, leite condensado, iogurtes, chantili, águas, sumos e tisanas, representados pelas seguintes marcas:



Figura 1 - Marcas comercializadas pelo Grupo Lactogal

Funcionalmente, está estruturada da seguinte forma:

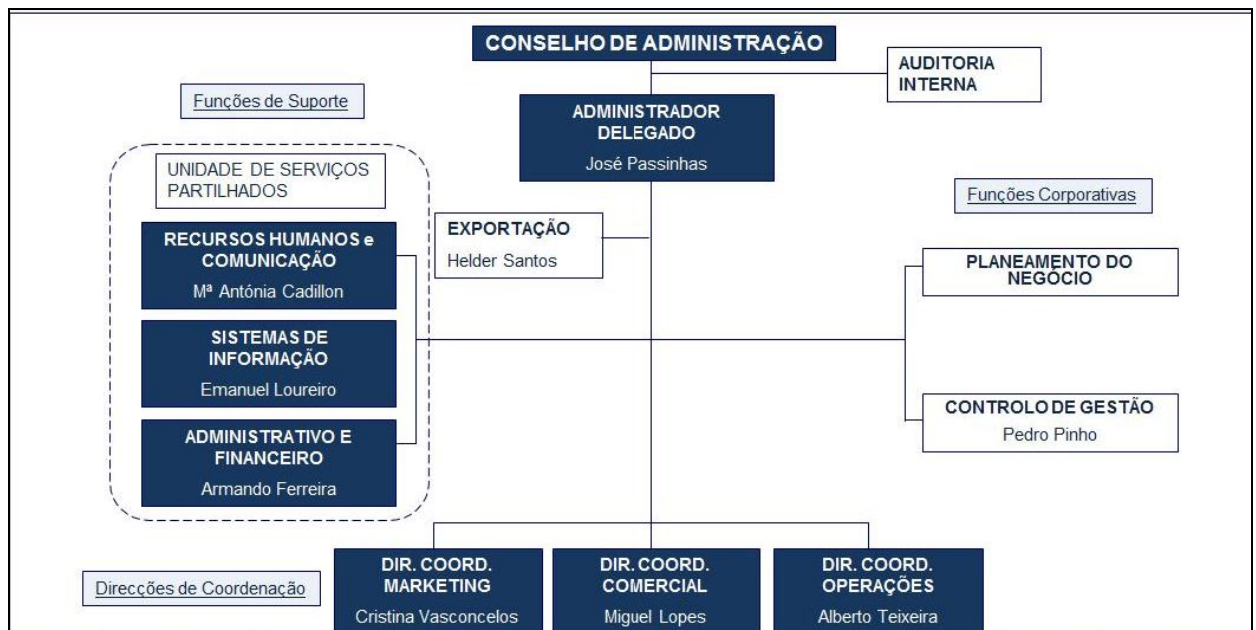


Figura 2 - Estrutura Funcional do Grupo Lactogal

1.2 O Projeto de Dissertação

O projeto teve como principal objetivo a identificação de problemas associados à segurança da informação e a elaboração de um plano de ação de melhoria. O impacto esperado da implementação das ações de melhoria deverá ser traduzido numa melhoria dos serviços prestados pela Direção de Sistemas de Informação do Grupo Lactogal. Deste modo, os objetivos específicos deste trabalho são:

- Compreender a importância que os sistemas de informação assumem para o negócio;
- Identificar as situações mais problemáticas que afetam os sistemas de informação;
- Avaliar o atual nível de satisfação dos utilizadores dos sistemas de informação do Grupo Lactogal para com os serviços prestados pela DSI;
- Definir um plano de ação com base na análise dos problemas identificados;
- Apresentar protótipos de documentos elaborados durante o projeto baseados no plano de ações definido.

1.3 Metodologia

Para suporte teórico do projeto efetuou-se uma pesquisa bibliográfica que procurou reunir as principais investigações conduzidas na área da gestão da segurança da informação. O estudo do estado da arte da segurança dos sistemas de informação foi focado nas boas práticas da segurança da informação, na temática da continuidade do negócio (*business continuity*) e nos

resultados apresentados em artigos científicos sobre o papel do utilizador na segurança dos sistemas de informação.

No âmbito do projeto de investigação realizado no Grupo Lactogal, foi feito um levantamento dos principais processos de negócio e de todos os sistemas de informação que os suportam. O objetivo deste primeiro passo prendeu-se com a definição clara de todos os processos core e dos sistemas de informação envolvidos. Os processos foram mapeados com recurso à técnica BPMN (*Business Process Modeling Notation*). O passo seguinte, foi compreender que atividades dentro dos processos core eram mais críticas para garantirem a continuidade do negócio e, neste sentido, foi efetuada uma avaliação de criticidade das atividades dos processos que considerou o tempo possível de paragem de cada processo e o tempo de recuperação do mesmo, medindo, deste modo o seu nível de criticidade. Para avaliação dos níveis de criticidade foram entrevistados os gestores funcionais de cada processo/área de negócio da DSI, responsáveis pelo suporte aos utilizadores. Participaram nesta fase cinco elementos.

Compreendidas estas dimensões, foi necessário perceber que incidentes afetavam os sistemas de informação e para tal, foram realizadas três sessões com grupos de trabalho correspondentes às áreas de suporte da DSI com o objetivo de listar que eventos resultaram no comprometimento da disponibilidade, integridade e confidencialidade da informação. Adicionalmente, procuramos perceber qual a frequência com que estes incidentes ocorriam e que medidas já tinham sido implementadas para reduzir ou eliminar estes eventos. As sessões contaram com a participação de 12 pessoas: 4 pertencentes à área de Tecnologias da Informação e 8 à área de Processos de Gestão da Informação. No início das sessões foi explicado ao grupo o objetivo do trabalho de investigação e os objetivos específicos daquelas sessões. À medida que as pessoas iam falando, eram anotadas as ideias principais e, no final da sessão, validadas por todos os elementos do grupo.

Finalmente, dada a importância que os utilizadores finais assumem na gestão da segurança da informação e atendendo aos resultados do levantamento de incidentes efetuado, o projeto no Grupo Lactogal incluiu a realização de um questionário, junto de uma amostra de utilizadores de sistemas de informação que procurou:

- Avaliar os níveis de satisfação dos utilizadores relativamente aos serviços prestados pela DSI;
- Diagnosticar as principais dificuldades que os colaboradores sentiam decorrentes da utilização dos sistemas de informação;
- Compreender de que forma o serviço de Helpdesk era utilizado, tendo em conta o motivo mais frequente do recurso a este serviço.

O questionário foi elaborado em parceria com a Direção de Recursos Humanos e Comunicação e foi validado pelas duas direções envolvidas. Este instrumento contou com a participação de 92 pessoas de diferentes departamentos e foi aplicado em duas unidades fabris (Modivas e Oliveira de Azeméis) e na sede (Porto), nos dias 21 e 22 de junho de 2012.

A apresentação do plano de ação e protótipos tiveram como base a análise dos resultados obtidos e consideraram as boas práticas na gestão da segurança de informação, nomeadamente as recomendações propostas pela norma ISO/IEC 27002.

1.4 Estrutura do documento

A primeira parte deste documento reúne a pesquisa bibliográfica efetuada que caracteriza o estado atual da investigação feita sobre a gestão da segurança da informação. Associada à gestão da segurança da informação, tiveram foco três subtemas: as boas práticas existentes, a continuidade do negócio e o papel do utilizador na gestão da segurança da informação.

A segunda parte procurou identificar os principais problemas encontrados no departamento de sistemas de informação do Grupo Lactogal. Para o efeito, estão descritos todos os passos que foram dados nesse sentido e os resultados encontrados.

Depois de identificados os problemas e com base na análise dos resultados, foi elaborado um plano de ação que procurou dar resposta às áreas-problema identificadas.

Um protótipo de cada uma das iniciativas propostas pode ser visto na quarta parte deste documento e a última parte apresenta as considerações finais sobre a elaboração deste projeto.

2 Revisão Bibliográfica e Estado da Arte

Os sistemas de informação representam a espinha dorsal da infraestrutura operacional de uma empresa. Hoje em dia, devido à depressão económica e ao aumento da intensidade de operações, as empresas reconhecem, cada vez mais, a importância das tecnologias de informação sobre a produtividade das mesmas (Teilans 2011).

A gestão da segurança da informação é, segundo Whitman e Mattord (2011) o conjunto de processos, procedimentos, recursos humanos e tecnologia encarregues de proteger os bens de informação de uma organização. Dito de outra forma, a gestão da segurança da informação, preocupa-se com as pessoas, processos e tecnologia. Os processos e as pessoas são influenciados pelo ambiente onde estão inseridos.

Neste sentido, Rob Jonhson (2011) define a segurança da informação como o ato de proteger a informação e os sistemas que a armazenam e processam. Acrescenta ainda que esta proteção é contra qualquer risco que possa conduzir ao acesso não autorizado, uso, divulgação, disrupção, modificação ou destruição da informação. O autor distingue o conceito de segurança dos sistemas de informação do conceito de segurança da informação defendendo que o primeiro concentra os esforços de proteção da informação independentemente da forma ou do processo e o segundo foca-se na proteção da segurança durante o processo e o seu uso.

Segundo Kim e Solomon (2012), a informação só poderá ser considerada segura se satisfizer três princípios: a disponibilidade, a confidencialidade e a integridade. A disponibilidade normalmente expressa a quantidade de tempo para os utilizadores fazerem uso dos sistemas, das aplicações ou dos dados. A integridade relaciona-se com a validade e precisão dos dados. A confidencialidade significa guardar a informação de toda a gente que não possua o direito ao seu acesso.

A literatura na área da segurança mostra que as pesquisas sobre segurança dos sistemas de informação ainda se encontram numa fase muito embrionária, embora já exista a preocupação em explorar novas conceptualizações e identificar subtemas importantes para as organizações (Alnatheer and Nelson 2009). Estes autores apresentam um conjunto de fatores que influenciam a prática e cultura da segurança da informação:

Tabela 1 - Fatores que influenciam a prática e cultura da segurança da informação (adaptado de Alnatheer and Nelson 2009)

Cidadania Corporativa	• Consciência da segurança da informação
	• Programas de Formação
Ambiente Legal	• Gestão da segurança da informação standardização e boas práticas
	• Política de segurança da Informação
Gestão Corporativa	• Participação da Gestão de Topo na Segurança da Informação
	• Análise de risco da segurança da informação
Fatores Culturais	• Cultura Nacional
	• Cultura Organizacional

Segundo os autores, a consciencialização sobre a segurança da informação e os programas de formação são aspetos muito importantes na segurança da informação, uma vez que podem contribuir para ajudar as organizações a minimizar alguns dos danos provocados pela má utilização dos sistemas de informação ou interpretação errada dos procedimentos a adotar. Por

sua vez, as normas e boas práticas internacionais aplicadas à segurança da informação servem o propósito de estabelecer e manter um ambiente seguro para a informação, ajudam os gestores seniores a monitorizar e controlar a segurança, minimizando o risco residual no negócio e assegurando o cumprimento dos requisitos de segurança da organização, dos clientes e requisitos legais. Os standards mais comuns para a gestão da segurança da informação são a ISO/IEC 27002, COBIT, OCTAVE e ITIL. O apoio da gestão de topo relativamente à gestão da segurança da informação é fundamental, sobretudo para implementar a política de segurança dos sistemas de informação. A análise de risco da segurança da informação desempenha um papel importante no sucesso de uma organização, uma vez que pode ajudar a medir nas perdas financeiras que acontecem devido a problemas na segurança dos sistemas de informação. Finalmente, os fatores culturais respeitam as características culturais do país onde a empresa se situa e a cultura organizacional e que são extremamente influenciadores no modo como a segurança dos sistemas de informação é gerida.

2.1 Boas práticas na gestão da segurança da informação

- ISO/IEC 27002

De acordo com a ISO/IEC 27002 que estabelece as diretrizes e princípios gerais para a criação, implementação, monitorização, revisão, manutenção e melhoria de um sistema de gestão da segurança da informação numa organização.

Este sistema é definido como uma parte de um sistema de gestão baseado no risco para o negócio para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação. Inclui a estrutura organizacional, políticas, planeamento de atividades, responsabilidades, práticas, procedimentos, processos e recursos. Um sistema de gestão da segurança da informação existe para preservar a confidencialidade, disponibilidade e integridade da informação de uma organização e bens de informação. Estas três propriedades são definidas da seguinte forma:

- **Confidencialidade** – é a propriedade da informação não estar disponível ou não ser divulgada a indivíduos, entidades ou processos não autorizados.
- **Disponibilidade** – é a propriedade de estar acessível e utilizável sempre que necessária por uma entidade autorizada que permite que a informação seja acessível por programas de *software* assim como por utilizadores humanos.
- **Integridade** – é a propriedade de salvaguardar a precisão e exatidão dos bens.

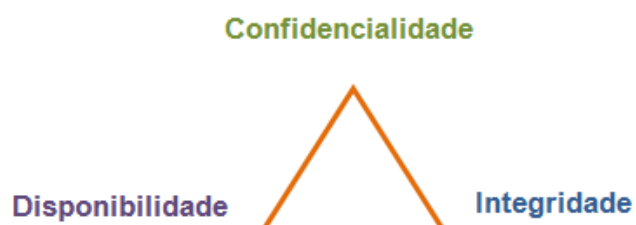


Figura 3 - Propriedades da segurança da Informação - Adaptado de Gibson (2010)

A norma é constituída por 11 capítulos que totalizam 39 categorias de segurança:

1. Política de segurança de informação;
2. Segurança Organizacional;
3. Gestão de bens (*assets*);
4. Segurança dos Recursos Humanos;
5. Segurança física e ambiental;
6. Gestão das comunicações e operações;
7. Controlo de acessos;
8. Aquisição, desenvolvimento e manutenção de sistemas de informação;
9. Gestão de incidentes de segurança da informação;
10. Gestão da continuidade do negócio;
11. Conformidade

- *ITIL – IT Infrastructure library*

As boas práticas definidas pelo ITIL explicam que as organizações colecionam dados de modo a produzirem bens ou serviços. De forma resumida, o ITIL defende que a integridade, a disponibilidade e a confidencialidade não podem ser problemas numa organização e que estas três condições devem ser sempre satisfeitas. O valor da informação tem que ser protegido e este valor é determinado pela confidencialidade, integridade e disponibilidade. A confidencialidade, integridade e disponibilidade podem ser classificadas segundo um sistema com quatro níveis:

Tabela 2 - Sistema de quatro níveis para classificar a confidencialidade, integridade e disponibilidade da informação do ITIL

Requisitos de segurança	Sem critério A segurança não é realmente necessária	Aconselhável Será apreciado um certo grau de segurança	Importante A segurança é absolutamente necessária considerando os interesses do negócio	Essencial A segurança é um critério essencial
Confidencialidade	Público A informação pode ser do domínio público	Protegido Os dados só podem ser vistos por um grupo particular	Crucial Os dados só podem ser acedidos por aqueles diretamente envolvidos	Obrigatório Os interesses do negócio poderiam ficar severamente comprometidos se existisse algum acesso não autorizado à informação
Integridade	Passivo Não é necessária proteção extra da integridade	Ativo O processo de negócio tolera alguns erros	Detetável Um pequeno número de erros é permitido	Essencial Os processos de negócio exigem informação sem erros
Disponibilidade	Desnecessário Não exige garantia	Necessário Downtime ocasional é permitido	Importante Difícilmente algum downtime	Essencial Só não está operacional em situações extremamente excecionais

- *Modelo COBIT – Control Objectives for Information and Related Technology*

A associação de controlo e auditoria aos sistemas de informação (ISACA – Information System Audit and Control Association) desenvolveu uma framework de boas práticas, internacionalmente aceites chamada COBIT – Control Objectives for Information and related Technology que introduz a ideia de ciclo de vida da segurança dos sistemas de informação. As boas práticas de COBIT são mais focadas em métodos de controlo do que na execução e

permitem ajudar a otimizar os investimentos em TI, assegurar a entrega dos serviços e fornecer métricas de avaliação dos mesmos.



Figura 4 - Ciclo de vida da segurança dos sistemas de informação, adaptado de Johnson (2011)

O domínio de Planear e Organizar do modelo COBIT inclui detalhes gerais dos requisitos e objetivos de uma organização. Este domínio procura responder às questões “o que é que se quer fazer?” e “Como conseguir fazer isso?”. Nesta fase, é revisto o modo como são geridos os investimentos em tecnologias da informação, os contratos, os SLA’s (*Service Level Agreements*) e novas políticas. O domínio Adquirir e Implementar, refere-se a prazos e entregas. Aqui constroem-se os controlos de segurança com base nos requisitos definidos no Planear e Organizar. No final desta fase, já existem equipamentos adquiridos e implementados, políticas, procedimentos e orientações escritas e equipas treinadas. A Entrega e o Suporte constituem outro domínio deste modelo. O pessoal responsável apetrecha o ambiente para minimizar as ameaças. Isto pode significar ajustar controlos, políticas, procedimentos, e SLA’s. Monitorizar e Avaliar. A supervisão deste domínio olha para o quadro geral. Os controlos, políticas e procedimentos acompanham todas as alterações tecnológicas e evoluções que acontecem na empresa? Esta fase olha para os requisitos específicos do negócio e para a orientação estratégica e verifica se o sistema continua a responder positivamente. Auditorias internas e externas acontecem nesta fase.

A orientação ao negócio deste modelo consiste em objetivos de negócio ligados a objetivos de TI, fornecendo métricas e modelos de maturidade para medir a sua eficácia e identificando as responsabilidades atribuídas aos donos dos processos de negócio e de TI.

De acordo com este modelo, são definidos sete critérios de informação:

1. **Eficácia** – a informação deve ser pertinente e relevante para os processos de negócio e deve ser entregue de forma atempada, correta, consistente e utilizável.
2. **Eficiência** – diz respeito ao fornecimento da informação através de uma utilização ótima dos recursos (os mais produtivos e os mais económicos).
3. **Confidencialidade** – relaciona-se com a proteção de informação sensível salvaguardando o seu uso indevido.
4. **Integridade** – tem relação com a precisão e exatidão da informação, bem como a sua validade, de acordo com os valores e expectativas do negócio

5. **Disponibilidade** – está relacionada com a informação estar disponível sempre que os processos de negócio assim o exigirem, hoje e no futuro. Também considera a salvaguarda dos recursos e capacidades necessários.
6. **Conformidade** – lida com a conformidade com as leis, regulamentos, acordos e contratos, afetos ao negócio e implicados nos diferentes processos de negócio.
7. **Confiabilidade** – relaciona-se com o fornecimento de informação apropriada para os executivos administrarem a organização e exercerem as suas responsabilidades fiduciárias e de gestão.

A bibliografia existente sobre a gestão da segurança dos sistemas de informação é extensa. Considerando os objetivos propostos pelo presente trabalho, foi dado maior foco aos subtemas da Continuidade do Negócio (*Business Continuity*), mais concretamente, ao *Disaster Recovery* e ao papel dos utilizadores na segurança dos sistemas de informação. Deste modo, importa resumir os principais conceitos e abordagens associados a estas temáticas específicas, resultantes da pesquisa bibliográfica efetuada.

2.2 Continuidade do negócio - *Business Continuity e Disaster Recovery*

Considerando que, hoje em dia, todas as organizações, independentemente do seu tamanho, são sustentadas por sistemas de informação (Karim 2011), estas devem possuir uma estratégia para recuperarem dados caso aconteça algum desastre que ponha em risco essa informação. O planeamento para recuperação depois de um desastre está rapidamente a tornar-se reconhecido como uma necessidade (Omar et al. 2011).

O *Disaster Recovery* e o *Business Continuity* surgem como processos que apoiam os negócios preparando-os para os eventos disruptivos que podem ser desastres naturais ou desastres com origem humana (Guy and Lownes-Jackson 2011).

Neste sentido, embora o *Disaster Recovery* possa ser entendido como uma reação a eventos raros nos quais se procura eliminar todo o caos subsequente de modo a que o negócio possa continuar formalmente, o *Business Continuity* deve ser um plano altamente proactivo com ações que garantam que independentemente do que possa acontecer, as operações do negócio continuam o mais estável que for possível (Karim, 2011).

O *Disaster Recovery* pode, deste modo, ser visto como uma parte do *Business Continuity* e relaciona-se com o impacto imediato de um evento. Cabem nesta categoria tudo o que possa estar relacionado com a recuperação dos sistemas após uma falha no servidor, uma falha de segurança ou a passagem de um furacão. O *Disaster Recovery* implica a paragem dos efeitos do desastre o mais rápido possível e o lidar com as consequências imediatas. Isto poderá incluir desligar sistemas que foram alvo de falha de segurança, avaliar que sistemas são afetados por uma inundação, terramoto ou qualquer outro evento e determinar a melhor forma de proceder. Em algum ponto do *Disaster Recovery*, as atividades do *Business Continuity* começam a sobrepor-se. Onde instalar os sistemas temporários, como obter sistemas substitutos ou partes deles, como instalar a segurança numa nova localidade – são questões relacionadas quer com *Disaster Recovery* como com *Business Continuity*. (Omar et al. 2011).

De acordo com o IDC Portugal (IDC 2011) as questões relacionadas com a continuidade do negócio e com as tecnologias de continuidade de negócio devem ser colocadas ao nível do negócio, ao nível aplicacional e ao nível da infraestrutura. Neste sentido, ao nível do negócio, o planeamento da continuidade do negócio deve iniciar com um mapeamento de sistemas e aplicações de informação e dos ativos da infraestrutura. Feito o mapeamento, deverá ser

conduzida uma análise do impacto no negócio. O nível aplicacional deve incluir a definição das políticas para as aplicações-chave que requerem operações contínuas no caso de falha. Finalmente, o nível da infraestrutura deve ocupar-se de assegurar a continuidade da rede de comunicações e dos serviços de telecomunicações, bem como as questões relacionadas com a energia e arrefecimento redundantes nos *data centers*. Atualmente, existe um conjunto de soluções tecnológicas que procura responder a necessidades de continuidade do negócio, mas é fundamental que os departamentos de TI inventariem os processos mais críticos de que a organização depende para manter as operações de negócio.

A análise do impacto no negócio (BIA – *Business Impact Analysis*) constitui um processo extremamente importante para determinar e listar todos os processos críticos que são vitais ao funcionamento do negócio. Segundo Sikdar (2011) existem três fases principais na análise do impacto no negócio:

1. Fase de recolha de dados – esta fase constitui a base para a identificação de processos críticos e processos sensíveis ao tempo assim como sobre os recursos que os suportam.

Esta fase pode fazer uso de diferentes fontes de informação:

- Documentos da empresa como políticas, procedimentos, organogramas, relatórios externos e internos, relatórios anuais, SLA, entre outros.
 - Entrevistas com os responsáveis de diferentes unidades de negócio e “donos” de processos para recolha de informação sobre atividades significativas que são executadas em cada unidade e respetivos processos. Podem ainda ser consultados outras entidades externas, parceiros, fornecedores, entre outros.
 - Podem ser usados questionários para recolha de informação pré-definida, evitando assim que os responsáveis ou gestores entrem em grandes discussões. O questionário também possui a vantagem de poder ser preparado com antecedência, permitindo aos responsáveis tempo suficiente para recolherem toda a informação necessária.
 - Os *Workshops* podem ser uma fonte de obtenção de resultados rápidos por exemplo na obtenção de informação sobre desastres que já ocorreram no passado como falhas de energia, incêndios, inundações, greves, entre outros. Permite a elaboração de listagem rapidamente e cumprem o objetivo de recolher dados com pouco detalhe informativo.
 - As *conference calls* podem ser usadas para ligar pessoas geograficamente dispersas e permitem o debate de ideias e a obtenção de consenso quando se discute informação importante que pode influenciar a análise do impacto de negócio.
2. Fase da análise dos dados – esta fase prevê um agrupamento da informação reunida num formato que tenha significado de modo a ser possível chegar-se aos dados necessários que resultam do impacto das interrupções nos processos de negócio. Uma vez feita listagem dos processos de negócio, procede-se à sua classificação. Numa situação de interrupção, a análise irá necessitar também da listagem das aplicações críticas. Será por isso necessário ligar as atividades críticas aos recursos que as suportam.
 3. Fase do relatório da análise do impacto no negócio – este relatório idealmente consiste num conjunto de subpontos, nomeadamente, o sumário executivo da análise efetuada;

a listagem dos processos críticos que devem continuar operacionais em caso de algum evento disruptivo; listagem com os tempos de recuperação (Recovery Time Objective e Recovery Point Objective) definidos para cada processo crítico; os critérios de classificação dos riscos que a organização enfrenta; O impacto no negócio considerando todos os impactos operacionais, legais e financeiros; estratégias alternativas de recuperação; a eficiência de custo em termos do custo de recuperação versus o benefício de estratégias de recuperação.

Um plano de continuidade do negócio prevê medidas que controlem o acesso à informação. Neste enquadramento, a IAM (Identity and Access Management) surge como uma temática relativamente recente que tem merecido a atenção de muitos investigadores (Young 2004; Small 2006; Olsen and Mahler 2007; Pulkkinen et al. 2007; Aldhizer III et al. 2008; Kho 2009; Mayne 2009; Ricart and Théoret 2011).

Dale Young (2004) define a Gestão de Identidades (Identity Management) como uma ampla área administrativa que lida com a identificação de indivíduos (identidade) e com o controlo do seu acesso aos recursos, serviços e sistemas e a Gestão de Acessos define o conjunto de regras necessárias para controlar e permitir o acesso individual aos sistemas internos e externos.

Na visão de Small (2006), a gestão de identidades e de acessos deve ser feita de um ponto de vista do negócio e não de uma perspectiva de tecnologias da informação. Outros autores reforçam esta ideia referindo que trata de algo mais do que instalar um software e que em primeiro lugar deve ser feito o levantamento dos dados sensíveis que devem ser protegidos e que estão associados aos processos mais críticos para o negócio (Aldhizer III et al. 2008).

A evolução tecnológica e o surgimento de novas necessidades na gestão de identidades e de acessos é também alvo de atenção e está patente em artigos nesta área onde referem que as soluções de IAM devem conseguir garantir a gestão de identidades e o controlo de acessos de todos os tipos de utilizadores e aplicações. As organizações devem ter a capacidade de disponibilizar informação a diferentes tipos de utilizadores incluindo colaboradores, clientes, fornecedores e parceiros e manter o controlo sobre quem tem permissão para aceder aos sistemas e a quais sistemas, sendo como tal, imprescindível a utilização de mecanismos de controlo de identidades e de acessos alinhados com as necessidades do negócio (Datinfor 2009).

Uma perspectiva mais recente, é a de Ricart e Théoret (2011) que apresentaram uma abordagem de gestão de acessos e de identidades baseada no risco. Todas as organizações, na opinião dos autores, devem considerar dois aspetos muito importantes antes de adotarem uma qualquer abordagem: em primeiro lugar, as organizações que escolhem uma abordagem geral de gestão de acessos que incluem todos os processos e aplicações, dedicam um grande esforço sem conseguirem obter grandes resultados; em segundo lugar, os processos de gestão de identidades e os sistemas implementados nas organizações tendem a falhar ao longo do tempo por falta de recursos, ferramentas eficazes ou consistência das aplicações. Assim, é necessária uma abordagem simples e sistemática que considere as constantes mudanças no ambiente interno e externo e que possua uma visão a longo-prazo. A proposta destes autores baseia-se nos seguintes pressupostos:

- A gestão de acessos e de identidades deve ser integrada nos processos de gestão de risco da empresa. Os objetivos da organização terão de estar em linha com as necessidades de segurança entre as quais, as relacionadas com a gestão de acessos. A

revisão do plano anual de identificação de riscos deve incluir o levantamento dos bens críticos da empresa que a gestão de risco identifica.

- Os processos de gestão de acessos devem ser sempre simples. Os gestores devem assumir a responsabilidade pela aplicação de políticas e procedimentos. Um maior entendimento e comunicação resultarão numa diminuição de ambiguidade.
- Aumentar o conhecimento entre os gestores de tecnologias da informação e os outros gestores de modo a que possam trabalhar juntos para definirem políticas, procedimentos, requisitos de controlo de acessos e para concordarem na melhor gestão de bens críticos comuns na organização.
- A implementação de um sistema de gestão de acessos deve ser faseada, feita por etapas e a primeira terá sempre que passar pela identificação dos bens críticos da organização, associados aos processos-chave do negócio.

Tendo em consideração os principais objetivos da gestão da segurança da informação, e respeitando a literatura existente sobre os dois subtemas aqui abordados, percebemos que a integridade e disponibilidade dos sistemas de informação são mais aprofundados em investigações relacionadas com o *Disaster Recovery* e *Business Continuity* e a confidencialidade é mais focada em temáticas relacionadas com a gestão de identidades e acessos. Não obstante, a preocupação em reduzir o número de incidentes que comprometem o desempenho dos sistemas de informação tem obrigado a um olhar mais atento sobre o comportamento dos utilizadores. Deste modo, o ponto que se segue procura reunir algumas das diferentes perspetivas assumidas pelos investigadores nesta área.

2.3 O papel do utilizador na segurança dos sistemas de informação

Até há bem pouco tempo atrás, o foco da segurança dos sistemas de informação estava totalmente direcionado para a tecnologia, contudo nos últimos anos tem vindo a ser dada atenção aos fatores humanos. Neste sentido, a segurança dos sistemas de informação deve respeitar não apenas os aspetos tecnológicos, mas também o comportamento das pessoas nas organizações e, mais concretamente, o respeito pelas políticas de segurança pré-definidas (Trcek et al. 2007). Neste contexto, alguns autores referem que as políticas, normas e procedimentos de segurança da informação constituem os mecanismos formais que definem os objetivos de uma organização em termos de segurança, bem como as medidas a serem tomadas para a concretização dos mesmos (Silva et al. 2003).

Sam Fleming (2007) chama a atenção para a necessidade das organizações criarem uma cultura coletiva de segurança, defendendo que esta poderá ser a base para sensibilizar os colaboradores para a necessidade de cumprirem com as políticas e procedimentos definidos.

Outros autores, referem que para enfrentarem ameaças internas e assegurarem a utilização eficaz das políticas e procedimentos de segurança, as empresas devem implementar medidas em diferentes níveis, com foco no controlo flexível mas rigoroso de informação sensível e na formação dos colaboradores sobre procedimentos e políticas de segurança da informação. O desenvolvimento de políticas de procedimentos é apenas a fase inicial do processo. A vulnerabilidade das empresas persistirá se os seus colaboradores não compreenderem como as suas decisões e comportamentos são determinantes para a segurança dos sistemas de informação (Tillery 2010).

Já anteriormente, Eirik Albrechtsen (2006) defendia que os utilizadores de uma empresa deveriam, ter um papel ativo no trabalho de segurança dos sistemas de informação através da prevenção de incidentes como por exemplo: proteção dos bens materiais e não materiais de uma organização, reação a incidentes e durante o dia a dia, através de ações como: bloquear o acesso ao seu computador, não escrever a *password* de acesso em nenhum local visível e acessível por terceiros, terem cuidados com a utilização de emails e da Internet, evitem o uso de software não licenciado e reportar todas as falhas de segurança ao departamento de sistemas de informação.

Os colaboradores pouco cuidadosos, que não cumprem com as políticas de segurança da informação constituem um sério risco para as organizações. Os resultados de pesquisas existentes sugerem que 91% das organizações empregam colaboradores que falham no cumprimento das políticas de segurança da informação (Siponen et al. 2009).

O Security Director's Report (2009) avança com a ideia de que a negligência ou ingenuidade do empregado é tão frequentemente a origem de falhas de segurança que os especialistas em segurança são quase unânimes em recomendar que as empresas gastem mais tempo a formar os seus trabalhadores de modo a garantir que estes possam conhecer os riscos, compreender a política de segurança dos sistemas de informação da empresa e fazer uso das ferramentas de proteção dos dados que eles controlam. De igual forma, o respeito e o cumprimento das políticas de segurança pelos colaboradores das empresas podem ser influenciados por um conjunto de razões como o grau de visibilidade das políticas de segurança da informação, o recurso a campanhas e formação sobre a segurança dos sistemas de informação, o exemplo dado pelos superiores hierárquicos e pelos pares é também determinante, a vulnerabilidade e o risco associado ao não cumprimento das políticas de segurança, percebido pelos colaboradores; o conhecimento, por parte dos utilizadores, das ameaças existentes ou possíveis a que os sistemas de informação estão sujeitos; a crença de que o cumprimento destas políticas pode de facto diminuir o risco, eliminando as ameaças a que as empresas estão sujeitas e conferindo deste modo, um papel determinante aos colaboradores constituem razões que podem contribuir para reforçar o cumprimento e respeito pelas políticas de segurança definidas pelas empresas (Siponen et al. 2009).

Siponen e Vance (2010), reforçam esta necessidade referindo que é estimado que cerca de metade das violações dos sistemas de segurança de informação são direta ou indiretamente causadas pelos colaboradores das empresas e habitualmente estão relacionadas com negligência ou ignorância das políticas de segurança existentes, mesmo em empresas com sistemas de segurança bem definidos e políticas implementadas. Os colaboradores de uma empresa constituem, por isso, a ameaça silenciosa, contudo mais perigosa, dado o grau de conhecimento que estes possuem sobre o negócio, sistemas de informação e acessos, muito mais significativo do que o conhecimento detido por elementos externos à organização (Hu et al. 2011).

Na perspetiva de Son (2011) os colaboradores podem ser envolvidos em abusos intencionais (roubo de informação, destruição de dados, entre outros) ou abusos não intencionais/acidentais (esquecimento de alteração de *password*, esquecimento de efetuar *log out*, entre outros). Dado que possuem acesso direto à rede da empresa, os colaboradores são muitas vezes o alvo preferencial de *hackers* que fazem de técnicas de engenharia social para acederem à informação da organização. Não obstante, as organizações parecem negligenciar a importância das pessoas na gestão da segurança da informação e continuam a apostar exclusivamente nas soluções tecnológicas para a segurança dos SI. Um exemplo claro reflete-

se no desenvolvimento de programas de segurança na empresa sem que estes considerem os aspetos humanos associados às falhas de segurança.

De acordo com Karjalainen e Siponen (2011), a literatura existente oferece várias abordagens sobre como garantir ou promover o cumprimento das normas e políticas de segurança pelos colaboradores de uma empresa, como é o recurso a sanções e dissuasões, campanhas de marketing e formação. De todas as abordagens, a formação de utilizadores é a mais comumente utilizada pelas organizações. Um artigo apresentado por Guo et al (2011) reflete algumas das violações mais comuns que os colaboradores das empresas podem cometer. Entre os exemplos referidos, estão o roubo de informação, a utilização de software não licenciado, o acesso a informação confidencial, a cópia ilegal de software, a cópia de informação sensível e confidencial, a utilização de *USB (Universal Serial Bus)* infetadas, a desativação de configurações de segurança, a não alteração de *passwords*, a não realização de *backups* ou de *updates de patches*.

O estudo conduzido por Albrechtsen e Hovden (2009) refere que a participação dos colaboradores, a reflexão de grupo, os processos de grupo, a criação de conhecimento ao nível organizacional, gera mudanças no conhecimento sobre a segurança da informação e nos próprios comportamentos adotados, a um nível individual. A participação dos colaboradores, o recurso ao diálogo e reflexões coletivas numa linguagem compreendida por todos os trabalhadores, a organização em pequenos grupos que partilharam experiências individuais, através de *workshops* de curta duração resulta, segundo os autores, em mudanças poderosas e estáveis relativamente ao aumento do compromisso dos colaboradores em cumprirem com os procedimentos e políticas de segurança dos sistemas de informação das empresas.

Assumindo uma abordagem totalmente distinta, orientada para as práticas impositivas ou estratégias de subordinação, Johnston e Warkentin (2010) realizaram um estudo que pretendeu analisar a influência dos apelos ao medo nos comportamentos, especificamente na conformidade dos utilizadores finais relativamente à segurança dos sistemas de informação. Deste modo, os investigadores procuraram perceber de que modo o recurso ao medo modifica as intenções comportamentais dos utilizadores finais associadas às ações de segurança recomendadas na utilização de computadores. O conceito de apelo ao medo pode ser definido como uma mensagem persuasiva para motivar indivíduos a cumprirem com recomendações de uma determinada ação através da estimulação do medo associada a uma ameaça. As principais conclusões do estudo evidenciaram que a corrente do tratamento de apelo ao medo é evidente não apenas no significado dos caminhos que ligam a resposta eficaz, autoeficácia e influência social com o comportamento intencional, mas também evidenciaram uma relação significativa entre a gravidade da ameaça e as duas dimensões da eficácia percebida (resposta eficaz e autoeficácia).

Seguindo uma linha de pensamento voltada para as distorções percetivas, alguns autores referem que a consciência da segurança da informação traduz-se no grau de vigilância das várias ameaças à segurança de informação e da vulnerabilidade percebida dessas ameaças. A compreensão das ameaças, por si só, não parece ser suficiente para motivar para a ação. As pessoas, na opinião dos autores, comprometem-se a tomarem ações preventivas quando têm a perceção de que o acidente pode acontecer com elas próprias. Acrescentam ainda que aquilo que as pessoas percebem não é, com frequência, a realidade mas uma visão distorcida da mesma, e isto acontece quer por não possuírem os conhecimentos apropriados para estimarem o risco real, quer por estarem motivados a sobrestimar o risco. A esta tendência para as pessoas sobrestimarem a probabilidade de passarem por experiências negativas é designada

por *viés otimista*. Na visão dos autores, o viés otimista relaciona-se com a percepção individual de invulnerabilidade e representa uma distorção defensiva que pode minar qualquer ação de prevenção, interferir no comportamento preventivo e agravar a tendência de procura de risco dos utilizadores (Rhee et al. 2012).

Por sua vez, Karjalainen e Siponen (2011) apresentam uma teoria que deve servir de base ao desenvolvimento de qualquer programa de formação de colaboradores em segurança dos sistemas de informação. Para os autores, a formação nesta área reveste-se de características muito próprias, devendo por isso ser diferente da formação que é dada noutras áreas. A teoria define quatro requisitos pedagógicos para desenhar e avaliar programas de formação em segurança dos sistemas de informação: o contexto psicológico, o conteúdo, o método de ensino e a avaliação da aprendizagem.

O interesse em perceber o papel que o utilizador final representa na segurança dos sistemas de informação ganha cada vez maior importância para os gestores das organizações e investigadores. A componente comportamental e percetiva tem vindo a assumir lugar de destaque nos artigos publicados, abrindo caminho ao aparecimento de novas abordagens e medidas preventivas associadas às falhas de segurança dos sistemas de informação com origem no incorreto uso dos mesmos por parte dos end-users.

3 A gestão da segurança da informação na Lactogal – identificação dos principais problemas

O departamento dos sistemas de informação do Grupo Lactogal está dividido em três grandes áreas: as tecnologias de informação (TI) que incluem uma equipa de sistemas e outra equipa de infraestruturas; a área de Processos e Gestão da Informação (PGI); e a área mais recente, a gestão de risco (GR). Cada área da DSI tem a seguinte missão e responsabilidades associadas:

Tabela 3 - Missão e Responsabilidades da DSI

	Missão	Responsabilidades
TI	Assegurar a satisfação das necessidades do negócio do grupo Lactogal no domínio das tecnologias de informação, garantindo os níveis de serviço previstos.	Planear, controlar e monitorizar os serviços e atividades da área de tecnologias de informação, nomeadamente ao nível dos fornecedores, serviços, sistemas, infraestruturas e redes, de acordo com as necessidades do negócio.
PGI	Assegurar a operacionalidade e eficiência dos processos de negócio e suporte à atividade do Grupo Lactogal, promovendo a adequação às necessidades identificadas e garantindo a satisfação das necessidades dos clientes internos.	Planear e controlar as atividades relacionadas com processos e sistemas de informação, controlo e conhecimento do negócio e operações de suporte avaliando a sua adequação; monitorizar a operacionalidade das plataformas, definir procedimentos, negociar com fornecedores para manutenção e desenvolvimento do portfólio aplicacional existente e avaliar os níveis de serviço prestados.
GR	Garantir a segurança, fiabilidade e disponibilidade da informação que dá suporte ao negócio do Grupo Lactogal bem como assegurar que os acessos estão de acordo com as definições, garantindo que os owners da informação têm os dados que monitorizam acessíveis.	Planear e monitorizar a implementação dos processos de Gestão e Controlo de Risco no âmbito de Sistemas de informação, nomeadamente através da definição de procedimentos de segurança, de acessos e de disponibilidade de sistemas, de acordo com as políticas em vigor.

Considerando o enquadramento deste projeto na área de gestão do risco, foi conduzido um trabalho de identificação dos principais problemas existentes no departamento de sistemas de informação de modo a ser possível sustentar um plano de melhoria dos serviços que o DSI oferece, em particular todos os relacionados com a segurança da informação. Esta fase inicial incluiu:

1. A definição e modelação dos principais processos de negócio e sistemas de informação que os suportam;
2. Identificação do grau de criticidade de cada processo de negócio e atividades associadas, considerando a indisponibilidade dos respetivos sistemas de informação e o tempo de recuperação associado;
3. Identificação dos principais incidentes que afetam os sistema de informação da lactogal com impacto para o negócio, assim como a frequência com que ocorrem.

Decorrente da avaliação dos resultados obtidos no levantamento dos principais incidentes que afetam ou afetaram no passado os sistemas de informação, foi necessário dar continuidade à análise dos principais problemas considerando a participação dos colaboradores do Grupo Lactogal. Neste sentido, procurou-se aferir junto dos utilizadores finais:

4. A avaliação global da qualidade dos serviços prestados pela DSI e sugestões de melhoria propostas;
5. A identificação, das principais dificuldades sentidas na utilização dos sistemas de informação durante a execução das suas tarefas diárias.
6. O modo como habitualmente utilizavam os serviços do Help Desk.

Esta análise foi feita com recurso à utilização de um questionário ministrado a uma amostra de colaboradores de diferentes departamentos e os principais resultados estão descritos no ponto 3.4 deste capítulo: Utilizadores finais - avaliação dos serviços da DSI e diagnóstico de necessidades formativas.

3.1 Definição e modelação dos processos core e sistemas de informação que os suportam

Com o objetivo de melhor compreender o que faz o Grupo Lactogal realizamos duas visitas a duas das unidades fabris (Modivas e Oliveira de Azeméis). O esquema que se segue procura representar todo o ciclo produtivo dos diferentes tipos de lacticínios que esta empresa produz, desde a receção de leite cru até ao carregamento dos camiões para transporte de produto acabado.

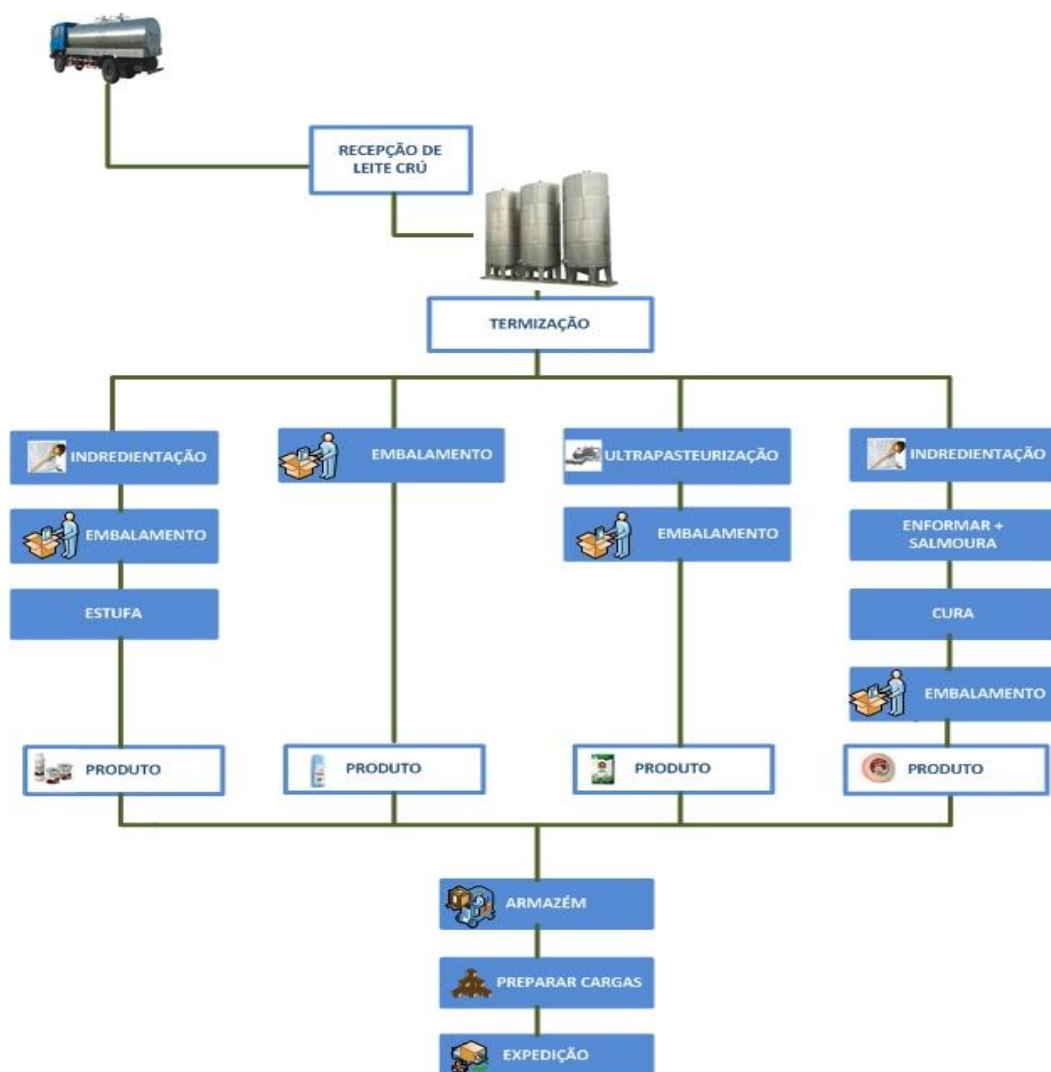


Figura 5 - Ciclo de produção Leite Dia/UHT e derivados (iogurtes e queijo)

Na identificação dos processos core, consideramos a definição de processo de negócio de Sharp e McDermott (2001) que o definem como “Um conjunto de tarefas de trabalho interrelacionadas, iniciadas como resposta a um evento que procura alcançar um resultado específico para o cliente e para todas as partes interessadas no processo”. Consideramos, igualmente, as orientações dos autores na definição e desenho de processos, nomeadamente:

- Todos os processos devem ter um nome com uma estrutura “verbo + nome” e devem ser denominados no singular;
- O nome deve indicar o resultado do processo e este resultado deverá ser distinto, contável e essencial, isto é, absolutamente fundamental ao funcionamento da empresa;
- Todos os processos devem ser definidos pela essência de “o quê” e não de “quem faz” ou “como faz”;
- Devem ser utilizados verbos com ações claras e não verbos sem consistência ou com significado pouco objetivo (ex: gerir, manter, administrar, monitorizar, entre outros);
- Todos os processos devem terminar com um resultado (output) e deve existir sempre um evento despoletador que dá origem ao processo (input).

A identificação dos processos core teve em conta os principais sistemas de informação que os suportam. Deste modo, assumimos a definição de processos *core* do Business Dictionary que refere tratar-se de uma atividade-chave ou de um conjunto de atividades-chave que devem ser executadas de forma exemplar para assegurar a continuidade da competitividade de uma empresa, uma vez que acrescenta valor a um output. O mapeamento dos processos foi elaborado com recurso à técnica BPMN e pode ser consultado no anexo A deste documento.

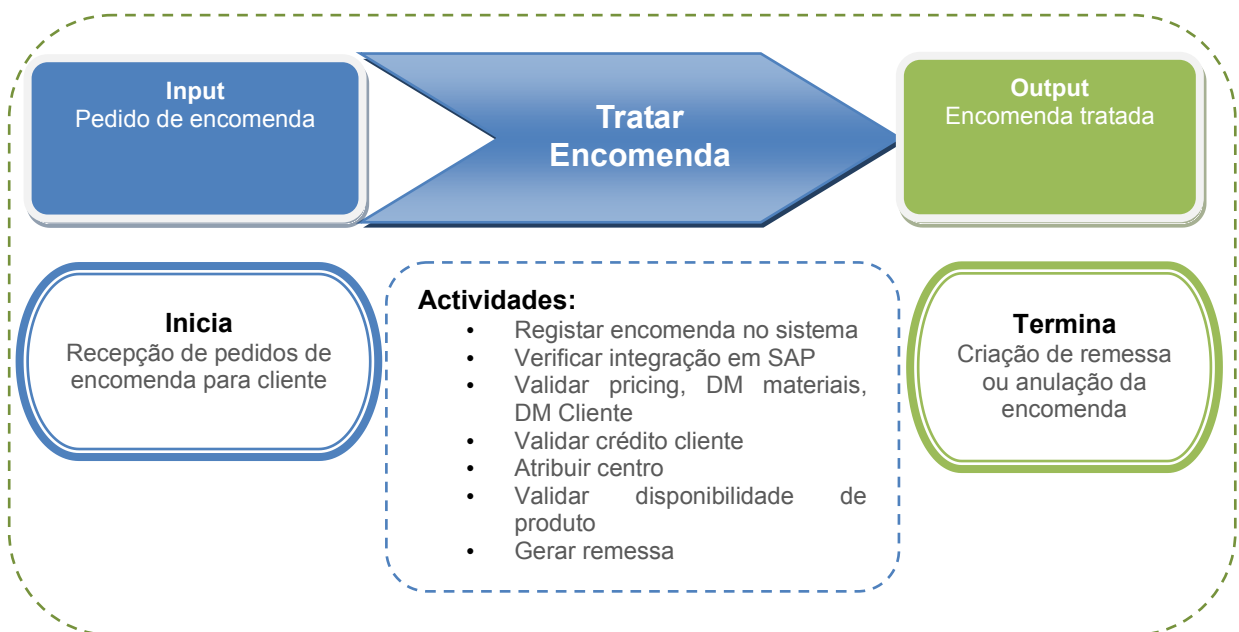


Figura 6 - Representação do macro processo “Tratar Encomenda”

Este processo inicia com a entrada do pedido de encomenda e termina com a criação da remessa. Os pedidos de encomenda chegam por diferentes vias (call center, EDI e vendedores) e são sempre integrados no sistema de informação (SAP). O tratamento de cada encomenda é contabilizado pelo tipo de *status* que assume neste sistema.

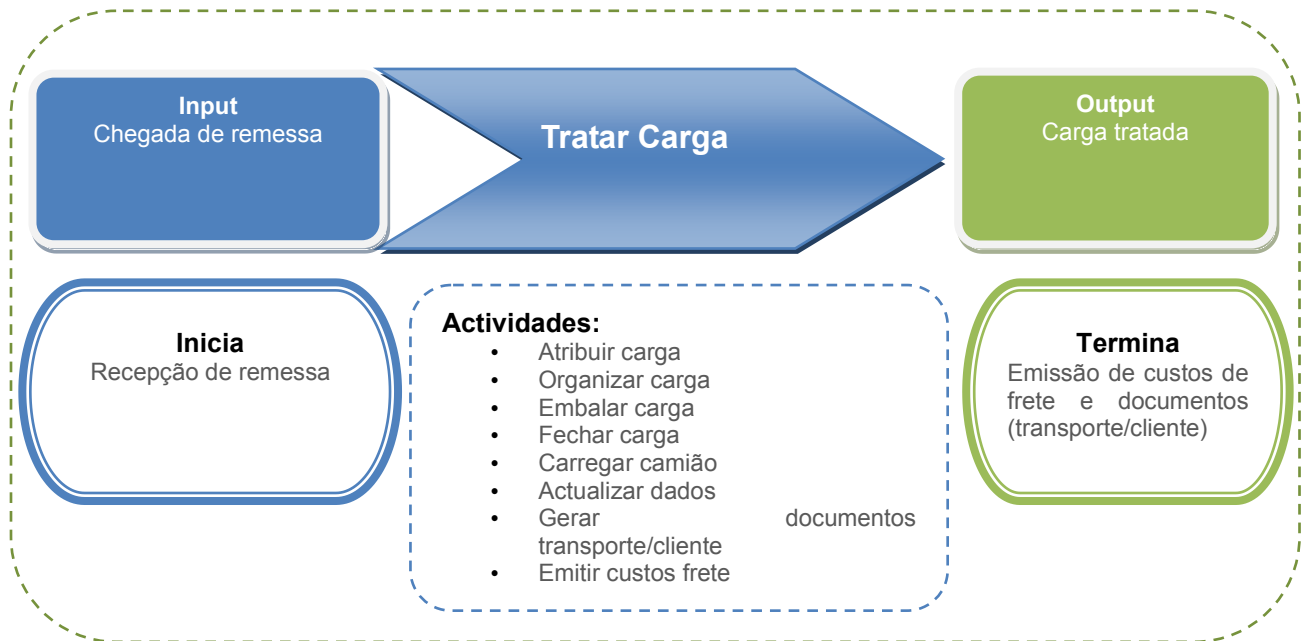


Figura 7 - Representação do macro processo "Tratar Carga"

A criação de uma remessa como resultado do processo anterior constitui o *input* para o tratamento da carga. Deste modo, é possível monitorizar o número de cargas tratadas através da informação dada pelos sistemas de informação (SAP) sobre o *status* de cada remessa/carga.

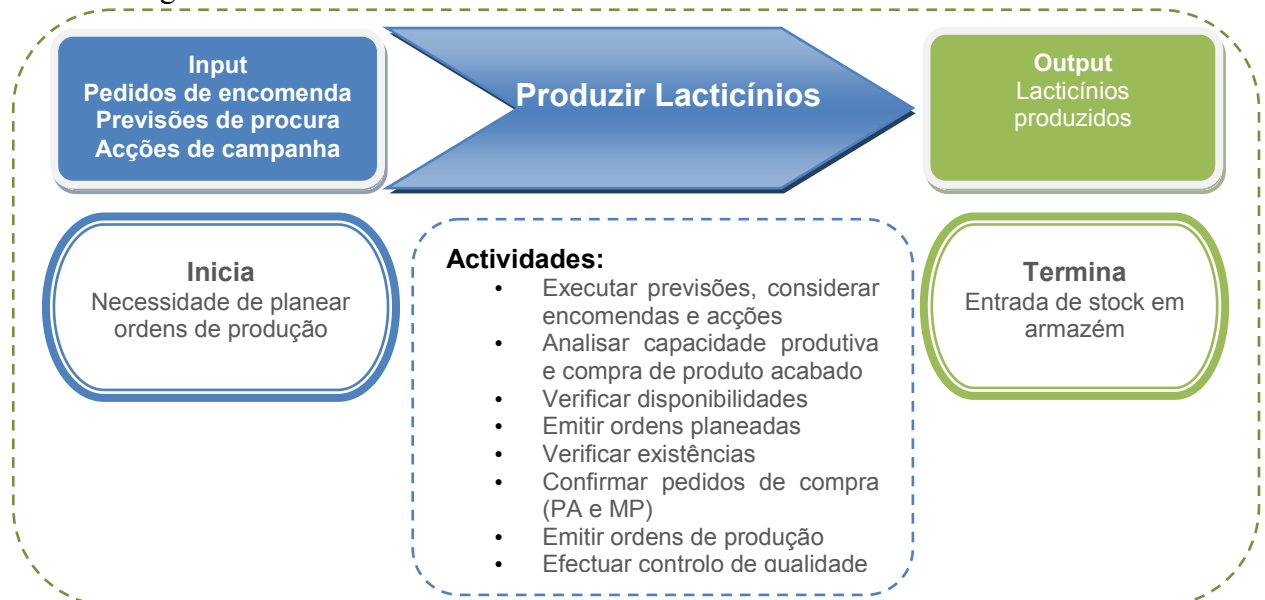


Figura 8 - Representação do macro processo "Produzir Lacticínios"

O processo de produção de leite e seus derivados é o que possui maior visibilidade por estar diretamente relacionado com os bens consumidos pelo cliente final e, por isso, ligado à produção de valor. As decisões associadas às quantidades e tipo de produtos a produzir são determinadas pelos pedidos de encomenda, pelas previsões de procura de cada produto e pelas campanhas em vigor como por exemplo do tipo "leve quatro e pague três".

3.2 Identificação do grau de criticidade de cada processo de negócio

Após a compreensão dos processos core do Grupo Lactogal, procedeu-se à identificação dos processos críticos e atividades associadas aos mesmos. Deste modo, a definição de processos críticos para o negócio continuamos a assumir a definição do *Business Dictionary* que refere tratem-se de processos de negócio que devem ser imediatamente restaurados, em caso de interrupção, garantindo, deste modo, a capacidade da empresa em proteger os seus ativos, satisfazer as suas necessidades mais críticas e cumprir com regulamentos e requisitos obrigatórios.

Tal como já foi anteriormente referido, esta fase incluiu a realização de entrevistas junto dos gestores funcionais do DSI por área (logística, vendas, armazém e produção). As entrevistas objetivaram a enumeração dos processos críticos e a aferição do nível de criticidade assumindo uma escala com quatro níveis, baseada no modelo de avaliação da criticidade defendido por Sikdar (2011). Esta escala procura atribuir níveis de acordo com duas grandes premissas:

- Quanto tempo pode o processo estar indisponível? Um a três dias? Uma semana? Mais de um mês?
- No caso do processo estar dependente de dados, que quantidade aceitável de dados se podem perder? Esta informação irá definir o grau de urgência na recuperação de dados. Isto é se o objetivo de tempo de recuperação (RTO – Recovery Time Objective), se será imediato, duas ou três horas depois, um ou três dias, ou mais de um mês.

Uma vez encontrada a resposta a estas questões, é possível definir quatro níveis de criticidade:

- Nível 1 – Os processos de negócio devem estar disponíveis durante todas as horas de trabalho (o objetivo de recuperação deverá ser inferior a duas horas);
- Nível 2 – Os processos de negócio podem ser executados sem algumas atividades normais por um período limitado de tempo (objetivo de recuperação entre 2 a 24 horas);
- Nível 3 – O negócio pode sobreviver por um período mais longo (até três dias) com perda de dados até um dia (objetivo de recuperação entre 24 a 72 horas);
- Nível 4 – O negócio pode sobreviver por um período mais alargado (objetivo de recuperação superior a 72 horas).

A análise efetuada considerou o conjunto de atividades que integram cada processo anteriormente identificado. A cada atividade foi atribuída um nível de criticidade de acordo com a escala pré-definida. O resultado final pode ser analisado com maior detalhe no anexo B deste documento. Do conjunto de atividades alvo da análise, quinze obtiveram a classificação de nível 1, doze de nível 2, sete de nível 3 e três com nível 4. A figura que se apresenta reúne o conjunto de atividades que foram classificadas como nível 1 e por isso, as mais críticas para o negócio, bem como os sistemas de informação que as apoiam:

PROCESSOS	ATIVIDADES CRÍTICAS	Sistemas informação
Tratar encomenda 	Fazer pedido encomendas automático	SAP ECC - SD
	Fazer pedido encomendas manual	SAP ECC - SD
	Determinar centro (armazém)	SAP ECC - SD
	Verificar disponibilidade produtos	SAP ECC - SD
Tratar carga 	Enviar cargas para WHM	SAP ECC-SD + WHM AS400
	Fechar cargas	SAP ECC-SD + WHM AS400
	Emitir Pré Facturação Vigor	SAP ECC-SD
	Enviar informação de Rotas	SAP ECC-SD + WHM AS400
	Movimentar stocks	SAP ECC-SD + SAP ECC- FI
	Movimentar produto	WHM AS400
Produzir lacticínios 	Recepcionar de leite cru	SAP ECC-MM + SFW Portarias AS400
	Preparar de lotes	SAP ECC-PP
	Encher produto acabado	SAP ECC-PP+WHM AS400
	Aprovar lote	SAP ECC-QM+ACCEPT ACCEPT
Actualizar dados mestre 	Fazer Abertura mês	SAP ECC MM + SAP ECC FI

Figura 9 - Atividades com classificação de criticidade nível 1 e respetivos sistemas de informação

No que diz respeito aos sistemas de informação que apoiam estas atividades críticas, percebemos que as aplicações SAP, ACCEPT e WHM são fundamentais para que sejam executadas. A figura que se segue representa os sistemas de informação e mais concretamente as aplicações informáticas críticas para o negócio, isto é que no caso de existir algum evento disruptivo, devem ser imediatamente restauradas e a recuperação da informação, por elas geradas, assegurada em menos de duas horas:



Figura 10 - Sistemas de informação/aplicações críticos

3.3 Levantamento dos principais incidentes que afetam os sistemas de informação da Lactogal

Após termos a visão dos principais processos de negócio e dos sistemas de informação que os suportam, assim como do grau de criticidade de cada atividade, avançamos para a identificação dos principais incidentes que afetam ou afetaram os sistemas de informação e qual o impacto que têm ou tiveram no negócio.

Para tal, realizamos três entrevistas coletivas com representantes das diferentes áreas do DSI. O objetivo principal foi o de recolher informação sobre quais as situações mais problemáticas ou incidentes que afetam ou afetaram a confidencialidade, integridade ou disponibilidade dos sistemas de informação. Adicionalmente, procuramos perceber que impacto tinham para o negócio, aferindo que entidades estariam afetadas sempre que o incidente ocorria, qual a frequência e que medidas já tinham sido tomadas ou que sugestões os colaboradores gostariam de deixar para tratar cada incidente. A tabela com o detalhe do levantamento de incidentes pode ser observada no anexo C deste documento.

Para cumprimento dos objetivos propostos e considerando as limitações de tempo que constroem o desenvolvimento mais aprofundado de outros subtemas, resumimos no quadro que se segue, os principais incidentes que afetam os sistemas de informação do DSI e sobre os quais nos vamos debruçar no capítulo seguinte, quando apresentarmos as nossas propostas de melhoria em resposta aos problemas encontrados.

Deste modo, associada à descrição de cada incidente, foram listados os principais alvos afetados pela ocorrência do mesmo. A sua definição foi baseada na matriz de risco e impacto do portfolio dos sistemas de informação apresentada por Larentiu e Adrian (2007). Neste sentido, consideramos que os incidentes que comprometem a confidencialidade, integridade ou disponibilidade dos sistemas de informação podem afetar:



Figura 11 - Alvos dos incidentes

Do conjunto de incidentes que afetam ou afetaram os sistemas de informação e que têm impacto no negócio do Grupo Lactogal destacamos todos os que ocorrem mais vezes durante o ano (mais de 3 vezes por ano) e que afetam sobretudo a informação crítica, as operações e as aplicações:



Figura 12 - Principais incidentes que afetam os sistemas de informação do Grupo Lactogal

3.4 Utilizadores finais - avaliação dos serviços da DSI e diagnóstico de necessidades formativas.

Com o objetivo de aprofundar as questões apresentadas na identificação de incidentes diretamente relacionados com os utilizadores finais, e de obter informação que sustente um plano de ações de melhoria também baseado na perspetiva dos colaboradores, foi desenvolvido um questionário que pode ser consultado no anexo D deste documento e que procurou:

- Avaliar a perceção dos utilizadores da qualidade dos serviços prestados pela DSI;
- Proceder à identificação das principais dificuldades na utilização dos sistemas de informação de suporte aos processos de negócio;
- Compreender a perceção da utilização que os colaboradores do Grupo Lactogal fazem, habitualmente, dos serviços de *Helpdesk*;

O inquérito foi elaborado em parceria com a DRHC e foi aplicado a uma amostra que procurou ser representativa da população de utilizadores dos sistemas de informação do Grupo Lactogal. A selecção dos participantes foi realizada pela DRHC e considerou o n.º total de colaboradores/utilizadores por área/direção, assim como a função desempenhada de modo a incluir diferentes níveis da estrutura funcional hierárquica (coordenadores, supervisores, técnicos e operacionais). A necessidade de seleccionar pessoas de diferentes direções e com responsabilidades diferentes, prendeu-se com a importância em garantir que a amostra incluísse utilizadores de todos os sistemas de informação que executassem diferentes tarefas nesses sistemas. Foram seleccionadas pessoas afetas à unidade fabril de Modivas (produção ambiente), à unidade fabril de Oliveiras de Azeméis (produção de frios) e à sede, no Porto. Os responsáveis de direção foram previamente consultados pela DRHC, no sentido de indicarem as pessoas que melhor correspondiam ao perfil definido.

Responderam, no total, 92 colaboradores distribuídos da seguinte forma:

Tabela 4 - Distribuição dos respondentes por sexo e direção

Direção	HOMENS	MULHERES	TOTAL
Administrativa-Financeira	6	13	19
Comercial	14	16	30
Compras	3	1	4
Industrial	5	9	14
Logística	10	4	14
Qualidade	1	1	2
Recursos Humanos	2	6	8
Funções Corporativas	0	1	1
	41	51	92

Para garantir o anonimato das respostas dadas, não foi exigida a indicação, no questionário, da função desempenhada, pelo que não é possível apresentar a distribuição da amostra por função.

Com relação ao nível de satisfação global com a qualidade dos serviços prestado pela DSI, os respondentes deveriam responder de acordo com uma escala com cinco níveis de apreciação:

- Má
- Baixa
- Satisfatória
- Boa
- Muito boa

Os resultados obtidos indicam que:

Nível geral de satisfação com os serviços da DSI

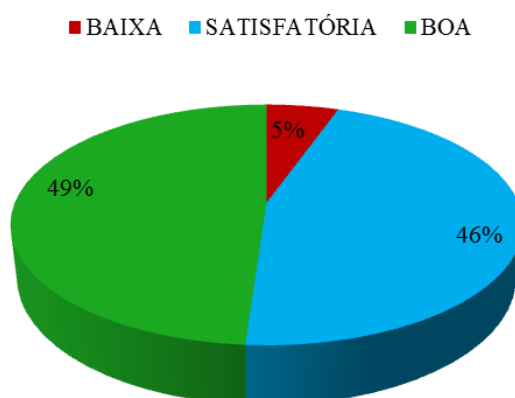


Figura 13 - Distribuição de níveis de satisfação com serviços da DSI

Do grupo de colaboradores que participaram nesta fase do estudo, 45 responderam que a qualidade dos serviços prestados pela DSI é “boa” e 42 “satisfatória”. Apenas 5 pessoas classificaram a qualidade dos serviços como “baixa”. Não foram obtidas respostas que situassem a qualidade dos serviços no nível mau ou muito bom. A apreciação global da qualidade dos serviços prestados, feita pela amostra de colaboradores, revelou ser positiva.

A segunda questão do inquérito pedia aos participantes que deixassem as sugestões de melhoria dos serviços da DSI. Optou-se por fazer uma pergunta aberta que permitisse o tratamento de informação qualitativa. A informação obtida, depois de analisada foi distribuída por um conjunto de categorias. A figura que se segue representa as categorias de melhorias definidas e exemplos de respostas dadas pelos colaboradores.

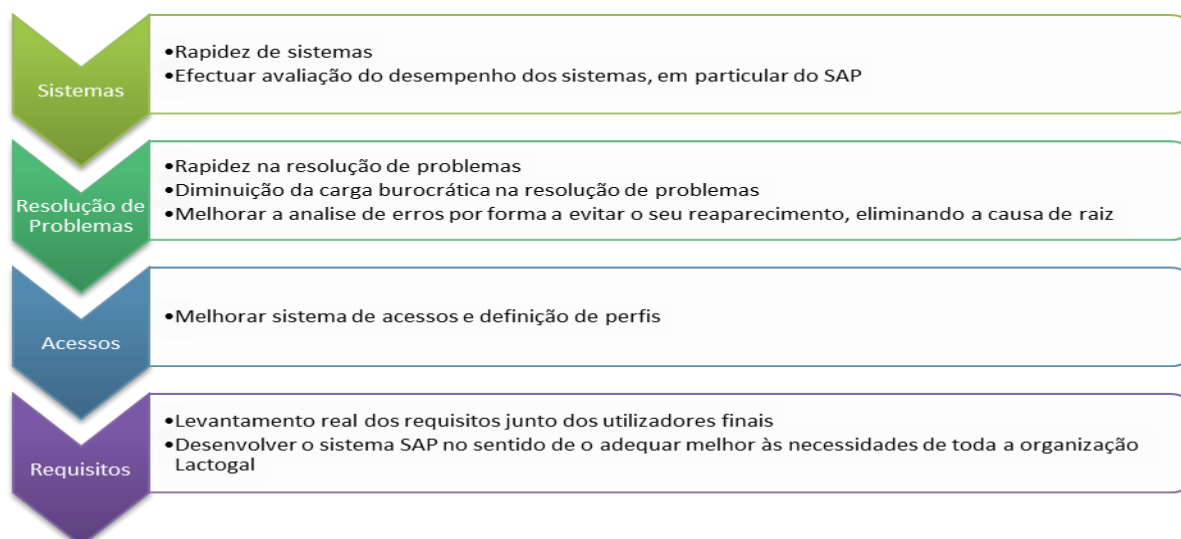


Figura 14 - Categorização das principais sugestões de melhoria

A melhoria mais sugerida pelos colaboradores foi categorizada como “Resolução de Problemas”. Neste âmbito, a análise das respostas indica que a maior parte dos colaboradores refere que gostaria que os problemas reportados fossem resolvidos mais rapidamente. No que diz respeito à categoria “Sistemas”, a maior parte das pessoas referiu a lentidão dos sistemas como um aspeto a ser melhorado. Todas as respostas relacionadas com a falta de acessos e erros de acessos foram incluídas na categoria “Acessos”. As sugestões diretamente relacionadas com a necessidade de otimizar os sistemas de informação através de uma análise das necessidades do negócio e dos utilizadores e a resposta atual e desejável dos sistemas, foram agrupadas na categoria “Requisitos”. O gráfico que se segue representa a distribuição de respostas dos colaboradores:

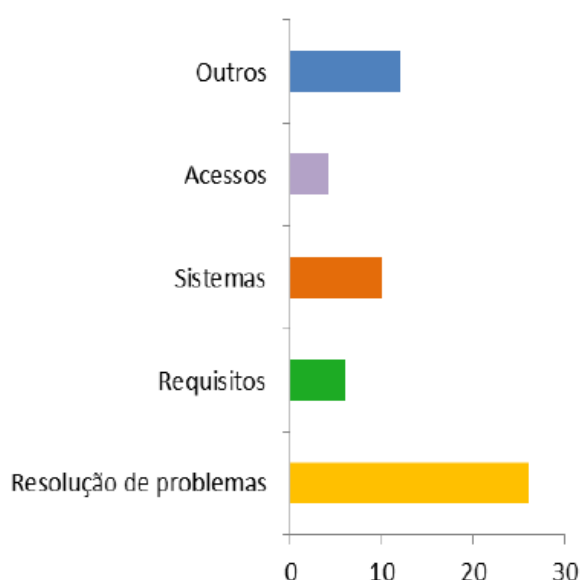


Figura 15 - Distribuição de respostas segundo categorias de melhorias propostas

A categoria “Outros” inclui comentários relacionados com pedidos de formação de colaboradores e alterações de atividades específicas e por isso difíceis de categorizar.

A segunda parte do questionário objetivou a enumeração das dificuldades na utilização dos sistemas de informação, identificadas por cada colaborador. Para o efeito, o questionário incluiu uma curta descrição funcional da aplicação e um exemplo de dificuldade para cada um dos sistemas de informação. Este trabalho de exemplificação de dificuldades foi feito para cada um dos módulos do ERP SAP, para a aplicação WHM do AS400, para a aplicação estatística de controlo de qualidade ACCEPT e para a Intranet. Foram ainda listadas todas as aplicações da Microsoft Office utilizadas no Grupo Lactogal (Word, Excel, Powerpoint e Outlook). As dificuldades exemplificativas foram sugeridas pelos gestores funcionais da DSI. As dificuldades foram descritas pelos colaboradores, numa caixa de texto associada a cada aplicação como se pode observar na figura que se segue:

SAP ECC WM - Gestão de Armazém MP	Apoia funções de gestão do armazém desde a entrada de mercadoria, gestão do inventário, picking e abastecimento à produção
(ex: tenho dificuldade em reimprimir etiquetas de palete)	

Figura 16 - Exemplo do questionário - dificuldades na utilização do módulo WM do SAP ECC

Os resultados obtidos estão detalhadamente descritos no anexo E deste documento. A análise das dificuldades será feita pelos gestores funcionais da DSI em colaboração com a DRHC para elaboração de um plano de formação feito à medida que dê resposta às necessidades formativas identificadas.

A tabela a seguir apresentada mostra um exemplo de dificuldade, apontada por um dos participantes, devidamente tratada:

Tabela 5 - Exemplo de dificuldades apontadas pelos utilizadores relativamente à utilização do SAP ECC FI

SISTEMA	MÓDULO	DIFICULDADES IDENTIFICADAS PELOS UTILIZADORES
SAP ECC	FI	“Parametrizações cash and liquidify” “Emissão de relatórios com a informação pretendida” “Query” “Não conhecer todas as potencialidades do módulo”

Os resultados obtidos na identificação de dificuldades deverá ser convertido num diagnóstico de necessidades formativas. O quadro que se segue exemplifica o trabalho ser desenvolvido entre os gestores funcionais da DSI e a DRHC, na conversão destas dificuldades num projecto formativo.

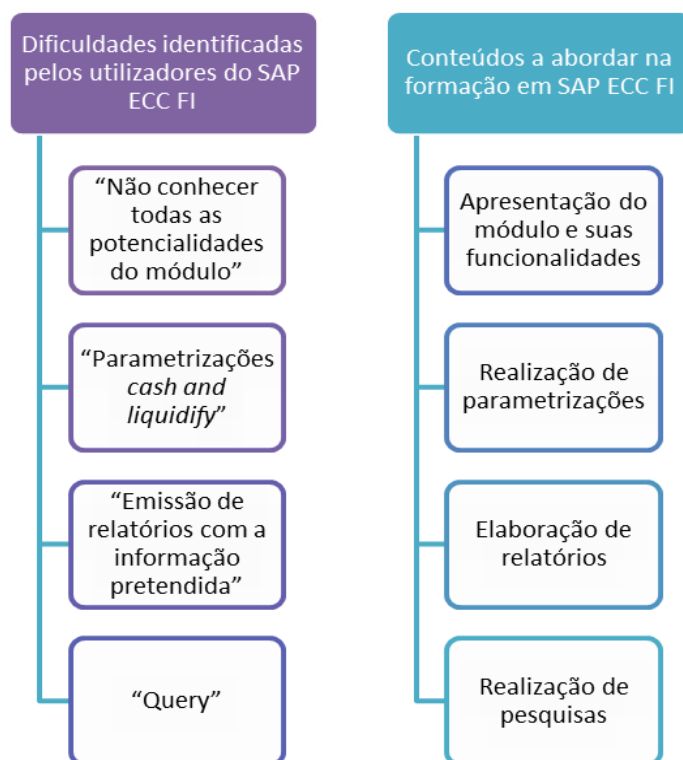


Figura 17 - Exemplo do tratamento de necessidades formativas do módulo FI do SAP ECC

O plano de ações elaborado incluiu a apresentação de dois protótipos de planos de formação para colaboradores e podem ser analisados no ponto 5 (5.1) deste documento.

A terceira parte do questionário procurou compreender de que modo os colaboradores usavam, com maior frequência, os serviços do *Helpdesk*. O objetivo desta questão prendeu-se sobretudo com a validação da perceção potencialmente errada que os utilizadores poderiam ter da utilização deste serviço, uma vez que um dos incidentes identificado referia precisamente que os colaboradores em vez de usarem o serviço para reportarem incidentes, utilizavam-no para pedirem esclarecimentos. A análise dos resultados indica que na perspetiva dos utilizadores, este serviço é usado para reportar incidentes e não para pedir esclarecimentos, contudo não se pode excluir a possibilidade dos colaboradores terem respondido de acordo com o princípio da desejabilidade social, isto é, a resposta politicamente correta e não de acordo com o que realmente fazem. A realidade dos factos deve por isso ser averiguada com o cruzamento de outras fontes de informação como a listagem de pedidos de esclarecimentos feitos ao *Helpdesk* e com outras técnicas de avaliação como entrevistas e observação em campo. A figura que se segue ilustra a distribuição das respostas dadas:

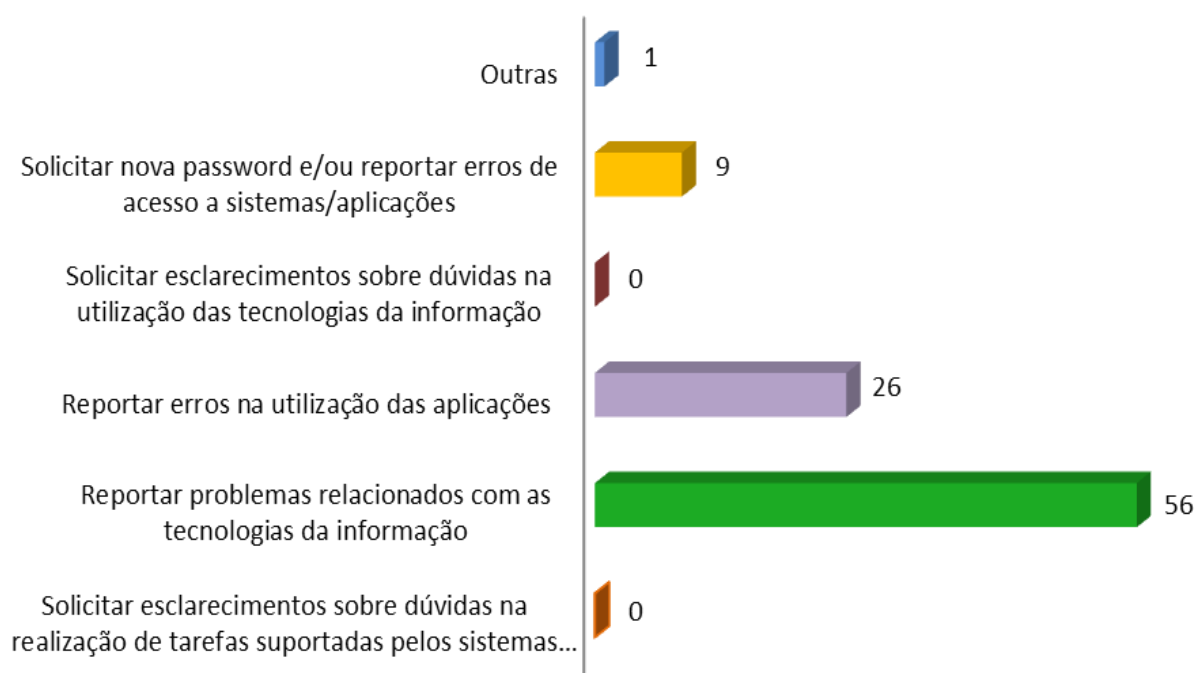


Figura 18 - Distribuição de respostas da utilização do serviço de Helpdesk

A leitura do gráfico permite identificar o reporte de problemas relacionados com a utilização das tecnologias de informação como sendo a utilização mais frequente deste serviço, seguido do relato de problemas relacionados com a utilização das aplicações informáticas. Menos expressiva foi a seleção do reporte de situações associadas à gestão de acessos com apenas 9 pessoas a identificarem esta utilização como a mais frequente.

Como é possível observar, as duas situações relacionadas com pedidos de esclarecimentos não obtiveram nenhuma resposta. Uma outra interpretação possível para estes resultados pode dever-se ao facto de apesar de o fazerem, na perspetiva dos utilizadores, estes pedidos não acontecerem com frequência, o que invalidou a possibilidade de escolha desta resposta.

Após análise de todos os dados obtidos, considerando os processos *core*, os processos e atividades críticas para o negócio, os incidentes mais frequentes na DSI e os resultados do questionário aplicado à amostra de utilizadores do Grupo Lactogal, identificamos duas áreas-problema principais e sobre as quais foi desenhado um plano de ação cujo o objetivo se prendeu com a diminuição ou eliminação do n.º de incidentes e com a otimização dos serviços de gestão da segurança da informação e gestão do risco nos sistemas de informação. O plano de ação está descrito no ponto 4 deste documento.

4 Plano de ação desenvolvido

Da análise dos problemas identificados no ponto anterior deste documento foi possível reconhecer duas grandes áreas-problema que afetam os serviços da DSI.

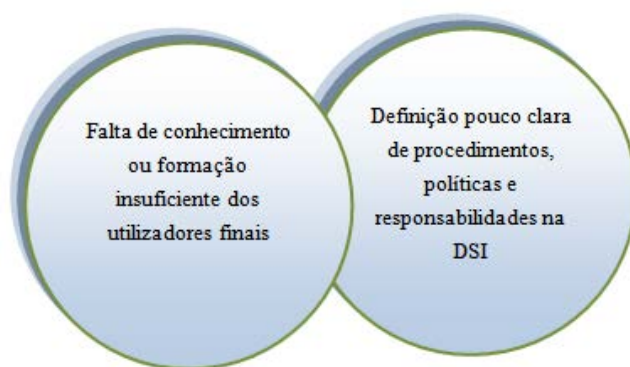


Figura 19 - Representação das principais áreas-problema na DSI

Neste sentido, a elaboração do plano de ação focou-se, principalmente, nestas duas áreas.

4.1 Plano de ação orientado para problemas dos utilizadores

A pesquisa bibliográfica que sustenta este projeto inclui uma parte relacionada com o papel que os utilizadores finais desempenham na gestão da segurança da informação. Muitos artigos referem que grande parte dos incidentes nos sistemas de informação das empresas têm origem na má utilização dos recursos de informação pelos seus colaboradores e várias são as propostas apresentadas para as empresas lidarem com esta realidade e diminuírem o n.º de incidentes que afetam os sistemas de informação das organizações. Deste modo, as questões relacionadas com a formação técnica inadequada ou a falta de conhecimento de políticas e procedimentos de segurança são, frequentemente, apontadas como as principais causas destes incidentes.

A análise dos resultados do levantamento de incidentes confirma esta realidade. Dos 11 incidentes que ocorrem com maior frequência, cinco estão diretamente relacionados com a má utilização, desconhecimento ou falta de formação técnica dos utilizadores:

- Sub utilização das capacidades dos sistemas de informação. Por desconhecimento, os utilizadores por vezes realizam operações complexas que exigem uma maior capacidade dos sistemas quando na verdade poderiam obter as mesmas informações de forma menos complexa e usando menos recursos (ex: relatórios de BW).
- Utilizadores criam tickets para o *helpdesk* para solicitar resolução de pequenos problemas que poderiam ser resolvidos imediatamente pelos próprios (ex: instalação de impressoras).
- Desconhecimento por parte dos utilizadores finais do impacto das suas ações. Por exemplo criam uma ordem no sistema e nunca mais dão seguimento ao que criaram, sem perceberem que isso vai gerar um conjunto de inconformidades noutros processos, por exemplo no crédito.

- O *helpdesk* é utilizado de forma errada pelos utilizadores que o usam, frequentemente, para tirarem dúvidas sobre a execução de tarefas e não para reportarem erros, contribuindo para a lentidão de outros serviços prestados pela DSI.
- Utilizador fica sem receber ou enviar emails por ter atingido a cota máxima.

O plano de ação desenhado para responder a estes problemas considerou:

- Desenho de um projeto formativo para todos os utilizadores de sistemas de informação baseado no diagnóstico de necessidades técnicas formativas resultante da análise das dificuldades apontadas pelos utilizadores no questionário;
- Desenho de plano formativo de cursos/*workshops* de sensibilização a todos os colaboradores do Grupo Lactogal sobre a gestão da segurança da informação: políticas e procedimentos.

4.2 Plano de ação orientado para problemas relacionados com políticas e procedimentos

A análise efetuada revelou igualmente que a falta de clareza de alguns procedimentos, políticas e responsabilidades estão na origem de parte dos incidentes que afetam a disponibilidade, confidencialidade e integridade da informação:

- Upgrade de sistemas não é comunicado às partes interessadas (ex SAP ECC). Este facto resulta em inconsistências de objetos em produtivo e em SAP corrompendo o próprio upgrade.
- Funcionalidade de programas ou aplicações comprometida pela baixa ou inexistente participação dos programadores internos no levantamento de requisitos e arquitetura dos sistemas (fases iniciais do desenvolvimento).
- Algumas não conformidades (erros) detetadas em aplicações são frequentemente assumidas como um problema de programação. Como resultado, existe dispêndio de tempo por parte dos gestores aplicacionais para perceberem a sua origem. Contudo, verifica-se que parte desses problemas poderiam ser identificados e resolvidos, desde logo pelo key user ou pelo gestor funcional, numa primeira análise.
- Conflitos de versões e passagem para produtivo de versões não testadas previamente.
- Alteração de acessos de utilizadores automáticos sem aviso.
- Técnico de sistemas procedeu a backup que interferiu no desempenho das máquinas de qualidade e desenvolvimento. Esta operação impediu colaboradores de Espanha de efetuarem um conjunto de procedimentos que estava previsto. O técnico de sistemas não tinha informação de que as máquinas iam ser utilizadas pelos colaboradores espanhóis.

Para responder a estes problemas, o plano de ação desenvolvido incluiu a elaboração de:

- Política de segurança da informação a ser disponibilizada a todos os colaboradores do Grupo Lactogal;
- Definição de procedimentos de alguns processos com inclusão de matrizes de responsabilidade e de conhecimento.

Os protótipos desenvolvidos encontram-se detalhados no ponto 5 (5.2 e 5.3) deste documento.

5 Protótipos desenvolvidos no âmbito do projeto

5.1 Proposta de projeto formativo de colaboradores internos a apresentar à DRHC

Workshop: Boas práticas, políticas e procedimentos de segurança da informação
Destinatários: todos os colaboradores do grupo Lactogal Objetivo: Dotar os formandos de noções essenciais de segurança da informação considerando as boas práticas existentes e as políticas e procedimentos definidos pela empresa. Duração da ação: 4 horas Calendário da ação: de janeiro a setembro de 2013 Local: Espaço para formação da Lactogal (sede, delegações e unidades fabris em Portugal Continental, Açores e Espanha) Conteúdos a abordar: A importância da segurança da informação • Mitos e preconceitos • Os incidentes mais comuns • Impacto das falhas de segurança para as organizações Boas práticas da segurança da informação – utilizadores finais Política de segurança da informação do Grupo Lactogal. Principais procedimentos de segurança da informação definidos (o que deve fazer)
Curso de Formação Técnica (SAP, ACCEPT, AS400, Microsoft Office e Intranet)
Destinatários: colaboradores que utilizem estas ferramentas para cumprimento das suas tarefas de trabalho. Objetivo: Definidos de acordo com as necessidades formativas identificadas no questionário Duração da ação: definida de acordo com o conteúdo programático e grau de dificuldade associado a cada curso de formação técnica e respetivo sistema de informação; Calendário da ação: de janeiro a dezembro de 2013 Local: Espaço para formação da Lactogal (sede, delegações e unidades fabris em Portugal Continental, Açores e Espanha) Conteúdos a abordar: Definidos por sistema de informação/módulo considerando o trabalho de diagnóstico de necessidades formativas elaborado.

5.2 Política de Segurança da Informação

A política de segurança da informação foi elaborada de acordo com as boas práticas existentes (ISO/IEC 27002) e deverá ser disponibilizada a todos os colaboradores. Pode de ser consultada no anexo F deste documento. Contém os seguintes conteúdos:

- Definição de segurança da informação;
- Objetivos e âmbito;
- Princípios de segurança;
- Políticas de Segurança:
 - Definição das políticas de Segurança da Informação
 - Controlo e classificação de activos
 - Responsabilidades do colaborador
 - Formação de colaboradores
 - Segurança física e ambiental
 - Gestão de computadores e redes
 - Controlo de acessos
- Glossário

5.3 Procedimentos e matrizes de responsabilidade

Foram reformulados documentos designados por “manuais de procedimentos” que procuraram definir regras aplicadas a processos específicos. O anexo G constitui um dos manuais revistos e atualizados e refere-se aos conjunto de procedimentos a considerar na gestão de identidades. O acesso a estes documentos será disponibilizado a todos os colaboradores da DSI.

O plano de acção contemplou a realização/reformulação de outros manuais de procedimentos mas por não se encontrarem concluídos e por tratarem de informação mais crítica, entendeu-se que não deveriam integrar este documento.

Para definição das responsabilidades e fluxo de informação, optou-se por inserir em cada manual uma matriz que designamos de Matriz de Responsabilidades onde é possível visualizar rapidamente que área é responsável por determinada actividade ou processo e que áreas devem ser informadas. Em alguns casos, existe ainda a representação, na matriz, da área que valida a informação. O objectivo destas matrizes é o de facilitar a compreensão das responsabilidades de cada área nos diferentes processos da DSI, uma das área-problema identificadas neste projecto.

Para além da introdução de matrizes de responsabilidade, neste manual está ainda definido:

- Objetivo do documento;
- Âmbito da aplicação;
- Definições – com explicação dos principais conceitos abordados no documento
- Modo de proceder



Figura 20 - Exemplo de matriz de responsabilidades criada

Alguns manuais incluem mapeamento de processos e glossários com as definições mais importantes para facilitar a compreensão do documento.

6 Considerações finais

A realização deste trabalho merece algumas considerações importantes sobre questões relacionadas com a gestão da segurança da informação nas organizações e sobre aspetos que devem ser atendidos durante a implementação de qualquer projeto na área dos sistemas de informação. Neste sentido, decorrente da experiência obtida na realização do projeto no Grupo Lactogal, importa apresentar as principais conclusões retiradas e assinalar outros trabalhos que poderiam ter sido feitos, caso não existisse um prazo de realização tão curto.

Uma das mais importantes conclusões retiradas do desenvolvimento deste projeto no Grupo Lactogal, prende-se com a importância que o conhecimento profundo dos processos de negócio, a experiência dos utilizadores finais e as políticas e procedimentos definidos possuem na garantia da confidencialidade, manutenção da disponibilidade e preservação da integridade da informação.

Deste modo, pudemos comprovar que a compreensão dos principais processos de negócio e actividades associadas é essencial para o desenvolvimento de qualquer projecto que vise a apresentação de melhorias, independentemente da área, processo ou departamento a que estejam associadas. Considero, por isso, que o fato de ter iniciado o meu trabalho focada nesse objetivo, o de procurar compreender, em primeiro lugar, o negócio do Grupo Lactogal, constituiu a base essencial para a construção deste projecto.

Adicionalmente, parece-nos importante sublinhar que apesar de não nos termos proposto a fazer o estudo profundo dos processos de negócio, a decisão de mapear os principais processos de negócio foi um exercício estimulante, uma vez que obrigou as pessoas envolvidas a pensarem no que fazem e a partilharem esse conhecimento com as restantes pessoas, o que resultou numa experiência enriquecedora para todos.

O envolvimento da direcção dos sistemas de informação e o acompanhamento regular do desenvolvimento do projecto por parte da orientadora da empresa foi fundamental para a concretização de todos os objectivos propostos, acima de tudo por ter contribuído para o interesse e participação das pessoas no mesmo.

Embora não tenha sido algo definido *à priori*, o fato do trabalho desenvolvido ter tido a preocupação de incluir a visão dos técnicos da DSI por um lado, e a visão dos utilizadores finais, por outro, permitiu estabelecer comparações importantes, com base nas diferentes experiências vividas pelas duas partes, com respeito à utilização dos sistemas de informação. Esta realidade vem reforçar a importância que os utilizadores ou clientes (internos) assumem no desenvolvimento de projectos com estas características e, sobretudo, quando directamente relacionados com a implementação de medidas que optimizem a qualidade de serviços oferecidos.

Com respeito ao tema principal abordado neste projecto, os resultados obtidos mostram a importância que a segurança da informação assume para as empresas, principalmente por terem implicações sérias na continuidade dos negócios e, como tal, a ausência de um sistema que faça a gestão eficaz e eficiente das questões da segurança da informação pode trazer implicações desastrosas para as organizações.

O desempenho lento dos sistemas de informação e o tempo de resposta na resolução dos problemas surgem como os principais tópicos, apontados pelos utilizadores finais, a merecerem melhorias. Na perspectiva da amostra de colaboradores que participaram neste

projecto, a disponibilidade da informação tem relação direta com o desempenho das suas funções.

Da identificação dos principais incidentes que afetam os sistema de informação na empresa e que contou com a participação de uma grande parte dos colaboradores da DSI, a disponibilidade da informação é a mais afetada quando existem incidentes, comparativamente com a confidencialidade e integridade da informação. Os incidentes que afetam a disponibilidade da informação são mais frequentes e, na opinião dos participantes uma parte deles resulta da utilização errada, dos sistemas e serviços, pelos utilizadores finais. Os resultados obtidos nesta fase reforçaram também a necessidade de existirem procedimentos claros que esclareçam sobre processos e responsabilidades associadas.

Se por um lado a realização deste projeto e a análise dos resultados obtidos permitiu retirar conclusões importantes, por outro lado, a limitação temporal relacionada com a duração do projeto também permitiu identificar outros trabalhos que podem dar continuidade a tudo o que foi desenvolvido neste âmbito, até à data. Neste sentido, as linhas que se seguem procuram enumerar as considerações feitas com relação a projetos futuros que, na nossa opinião mereciam atenção, nesta área.

Assim, e desde logo, o trabalho realizado não contemplou uma análise mais aprofundada das ações de melhoria sugeridas pelos colaboradores da empresa. Este seria um tópico muito importante para a melhoria dos serviços prestados pela direção dos sistemas de informação, nomeadamente no que respeita a análise de tempos de respostas dos sistemas de informação. Uma das recomendações mais frequentes nas respostas ao questionário ministrado prendeu-se com a melhoria de performance de algumas aplicações, mais concretamente de alguns módulos específicos do ERP SAP. Era por isso, importante, na nossa opinião, que fosse feito um estudo de campo que procurasse identificar os tempos de resposta dos sistemas que dão suporte aos processos de negócio, de forma a ser possível elaborar um plano de ação que procurasse otimizar o desempenho destes sistemas.

De igual forma, a celeridade na resposta à resolução de problemas constituiu a ação de melhoria mais citada pelos colaboradores. A visibilidade desta direção está altamente dependente da perceção que os utilizadores possuem sobre a rapidez e eficácia na resolução de problemas. Deste modo, seria igualmente importante que a DSI se debruçasse sobre uma estratégia que permitisse otimizar os serviços de apoio ao cliente que oferece e diminuísse os tempos de resposta a ele associados.

Durante o contacto com os colaboradores e após análise dos resultados dos questionários, ficou clara a necessidade de avaliar o sistema de gestão de acessos. Muitos foram os colaboradores que no contacto direto se mostraram insatisfeitos por não possuírem acessos que facilitassem a execução das suas tarefas diárias. Os diferentes relatos sugeriram que era necessário que fosse feito um trabalho de estudo em campo, junto de cada utilizador, de modo a que ficasse claro que sistemas cada pessoa diariamente acedia e que tipo de operações neles executava. Alguns exemplos remetiam para a falta de autonomia relacionada com o facto de apenas o supervisor poder executar determinados comandos/transações obrigando a tempos de espera, desnecessários, na opinião destas pessoas. Deste modo, seria importante para a organização efetuar um trabalho de análise profunda que resultasse no desenho de processos e atividades, sistemas de informação associados e operações efetuadas considerando a função de cada pessoa na organização.

De igual forma, seria importante cruzar algumas informações obtidas neste estudo, como por exemplo relacionar as respostas de satisfação com os serviços do DSI, com os diferentes

departamentos da empresa ou perceber as maiores dificuldades técnicas considerando os diferentes sistemas e departamento a que estão as pessoas afetadas.

Os resultados obtidos foram esclarecedores da importância que o trabalho em equipa assume em processos de suporte ao negócio com a criticidade que caracteriza um departamento de sistemas de informação. Alguns incidentes que afetam os sistemas de informação denotam falhas de comunicação entre as pessoas das diferentes áreas de suporte. Esta fragilidade é maior, se for acompanhada da ausência de procedimentos escritos que salvaguardem estas questões. Deste modo, acreditamos que todos os incidentes relacionados com estas questões devem ser alvo de uma avaliação no sentido de se perceber se já existem procedimentos escritos que regulamentem os fluxos de comunicação entre todas as partes. Adicionalmente, para reforço desta prática e interiorização das ações definidas, deveriam ser conduzidas sessões de sensibilização e esclarecimento dos procedimentos existentes para todos os colaboradores da DSI.

Finalmente e considerando o âmbito de conclusão do mestrado em engenharia de serviços e gestão, onde se insere este projeto, concluímos que a engenharia de serviços assume, na nossa opinião, uma importância fundamental na otimização de serviços nesta área, uma vez que independentemente da tecnologia, são as pessoas as maiores protagonistas em qualquer departamento de sistemas de informação de uma organização. O desenvolvimento de novos serviços ou o redesenho dos serviços existentes carece de particular atenção às diferentes entidades envolvidas, desde os colaboradores, aos processos de negócios, aos clientes, aos produtos, às máquinas, aos sistemas, entre outras. A participação de pessoas com conhecimentos nas mais variadas áreas organizacionais com a capacidade de elaborar uma análise que atente a todos estes fatores, parece assumir uma grande importância nestes contextos.

Para concluir gostaria apenas de referir que este trabalho resultou numa experiência muito positiva dada a enorme riqueza que consegui dela retirar e que em muito contribuiu para o meu crescimento pessoal e profissional.

Referências

- Albrechtsen, Eirik and Jan Hovden. 2010. Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. *Computer & Security*. 29:432-445 (Albrechtsen and Hovden 2010)
- Albrechtsen, Eirik. 2007. A Qualitative Study Of User's View On Information Security. *Computers & Security*. 26: 276-289 – (Albrechtsen 2007)
- Aldhizer III, G., Paul E. Juras and Dale R. Martin. 2008. Using Automated Identity and Access Management Controls. *The CPA Journal*. September: 66-71 (Aldhizer III et al. 2008)
- Alnatheer, Mohammed and Karen Nelson. 2009. *Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context*. Australian Information Security Management Conference – (Alnatheer and Nelson 2009)
- Datinfor. 2009. IAM solutions are undervalued in a changing business environment. *Feature Analysis*. February: 5-15 (Datinfor 2009)
- Denis, Treck, Roman Trobec, Nikola Pavesic and J. F. Tasic. 2007. Information Systems Security and Human Behavior. *Behaviour & Information Technology*. 16 (2):113-118. – (Denis et al. 2007)
- Fleming, Sam. 2007. Implicit Trust Can Lead To Data Loss. *Information Systems Security*. 16:109-113. – (Fleming 2007)
- Gibson, Darril. 2010. *Managing risk in Information Systems*. Sudbury: World Headquarters
- Guo, Ken H, Yufei Yuan, Norman P. Archer and Catherine E. Connelly. 2011. Understanding Nonmalicious Security Violations in the Workplace. *Journal of Management Information Systems*. 28(2): 203-236. (Guo et al. 2011)
- Guy, Retta and Millicent Lownes-Jackson. 2011. Business Continuity Strategies. Review of Management Innovation & Creativity. 4 (9): 55-69 (Guy and Lownes-Jackson 2011)
- Hu, Qing, Zhengchuan Xu, Tamara Dinev and Hong Ling. 2011. Does Deterrence Work in Reducing Information Security Policy Abuse By Employees. *Communications of the ACM*. 54(6): 54-60 (Hu et al. 2011)
- IDC (International Data Corporation). 2011. Tecnologias e Empresas em Continuidade de Negócio. *Caderno IDC*. 154 (Julho) – (IDC 2011)
- IOMA (Institute of Management & Administration). 2009. Security Director's Report IOMA. 9 (November) – (IOMA 2009)
- Johnston, Allen and Merrill Warkentin. 2010. Fear Appeals and Information Security Behaviors. *MIS Quarterly*. 34(3):549-566 (Johnston and Warkentin 2010)
- Jonhson, Rob. 2011. Security Policies and Implementation Issues. Sudbury: World Headquarters (Jonhson 2011)
- Karim , Akram Jahal . 2011. Business Disaster Preparedness. *International Journal of Business and Social Science*, 2 (18) – (Karim 2011)

- Karjalainen, Mari and Mikko Siponen. 2011, Toward a New Meta-Theory For Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems*. 12 (8): 518-555. – (Karjalainen and Siponen 2011)
- Kho, Nancy Davis. 2009. The Changing Face of Identity Management. *EContent*. April: 25-29
- Kim, David and Michael Solomon. 2012. *Fundamentals of Information Systems Security*. Sudbury: World Headquarters – (Kim and Solomon 2012)
- Laurentiu, Frasila and Tantau Adrian. 2007. Aspects of IT Risk Management for a Company. *Annals of the University of Oradea, Economic Science Series* – (Laurentiu and Adrian 2007)
- Mayne, Mark. 2009. The Big IAM – The Identity and Access Management (IAM) is at heart of corporate security, a difficult task with potential for great savings. *SC Magazine*. July: 32-36 (Mayne 2009)
- Olsen, Thomas and Tobias Mahler. 2007. Identity Management and Data Protection Law – Risk, responsibility and compliance in «circles of trust». *Law & Security Report*. 23(4). – (Thomas and Mahler 2007)
- Omar, Adnan, David Alijani and Roosevelt Mason. .2011. Information Technology Disaster Recovery Plan. *Academic of Strategic Management Journal*. 10 (2) (Omar et al. 2011)
- Pulkkinen, Mirja, Anton Naumenko and Kari Luostarinen. 2007. Managing Information Security in a Business Network of Machinery Maintenance Services Business – Enterprise Architecture as a Coordination Tool. *The Journal of Systems and Software*. 80: 1607-1620. (Pulkkinen et al. 2007)
- Rhee, Ayeun-Suk, Young U. Ruy and Cheong-Tag Kim. 2012. Unrealistic Optimism on Information Security Management. *Computers & Security*. 31:221-232. – (Rhee et al. 2012)
- Ricart, Philippe and Pascal Théoret. 2011. Safe Virtual Environments - a risk-based approach to access and identity management can lessen the impact of potentially detrimental situations. *CAMagazine*. August: 39:41 – (Ricart and Théoret 2011)
- Sharp, Alec and Patrick McDermott. 2001. *Workflow Modelling*. Boston: Artech House, Inc. (Sharp and McDermott 2001)
- Sikdar, Priti. 2011. Alternate Approaches to Business Impact Analysis”. *Information Security Journal: a global perspective*. 20:128-134 – Sikdar 2011)
- Silva, Pedro Tavares, Hugo Carvalho and Catarina Botelho Torres. 2003. *Segurança dos Sistemas de Informação*. Vila Nova de Famalicão: Centro Atlântico
- Siponen, Mikko and Anthony Vance. 2010. Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations. *MIS Quarterly*. 34 (3): 487-502. (Siponen and Vance 2010)
- Siponen, Mikko, Adam Mahmood and Seppo Pahlila. 2009. Are Employees Putting Your Company at Risk by Not Following Information Security Policies?, *Communications of the ACM*. 52 (12) – (Siponen et al. 2009)
- Small, Mike. 2006. Unify and Simplify. *Network Security*. (July):11-14
- Son, Jai-Yeol. 2011. Out of Fear or Desire? Toward a Better Understanding of Employees Motivation to Follow IS Security Policies. *Information & Management*, 48: 296-302. (Son 2011)

Teilans, Artis, Andrejs Romanovs, Yuri Merkuryev, Arnis Kleins, Pjotrs Dorogovs and Ojars Krasts. 2011. *Functional Modelling of IT Risk Assessment Support System*. Economics and Management. 16: 1061-1068 (Teilans 2011)

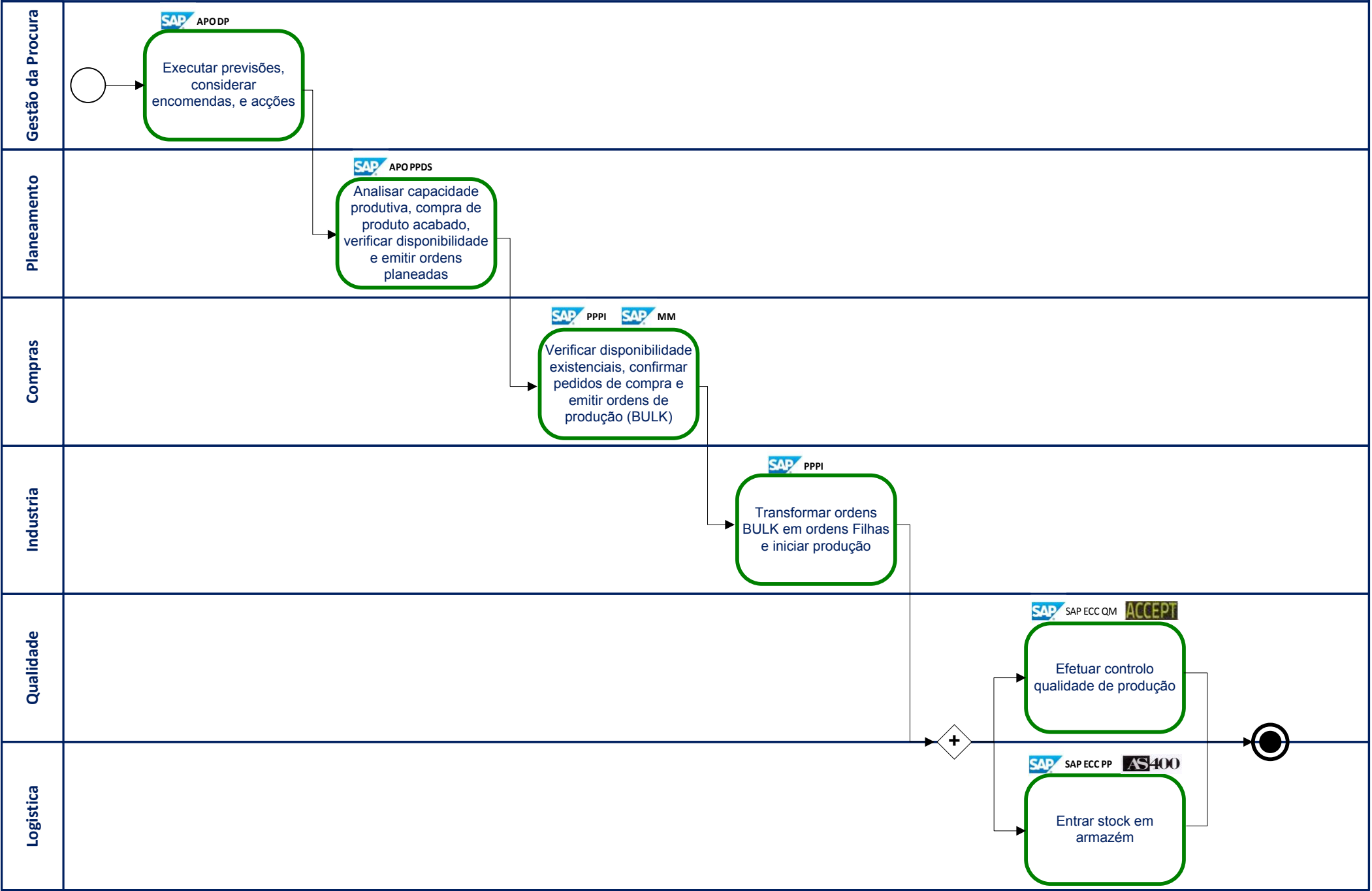
Tillery, Steve. 2010. How Safe Is The Cloud?. *Baseline Magazine*. September/October – (Tillery 2010)

Whitman, Michael and Herbert Mattord. 2011. *Principles of Information Security*. Hampshire: Cengage Learning. (Whitman and Mattord 2011)

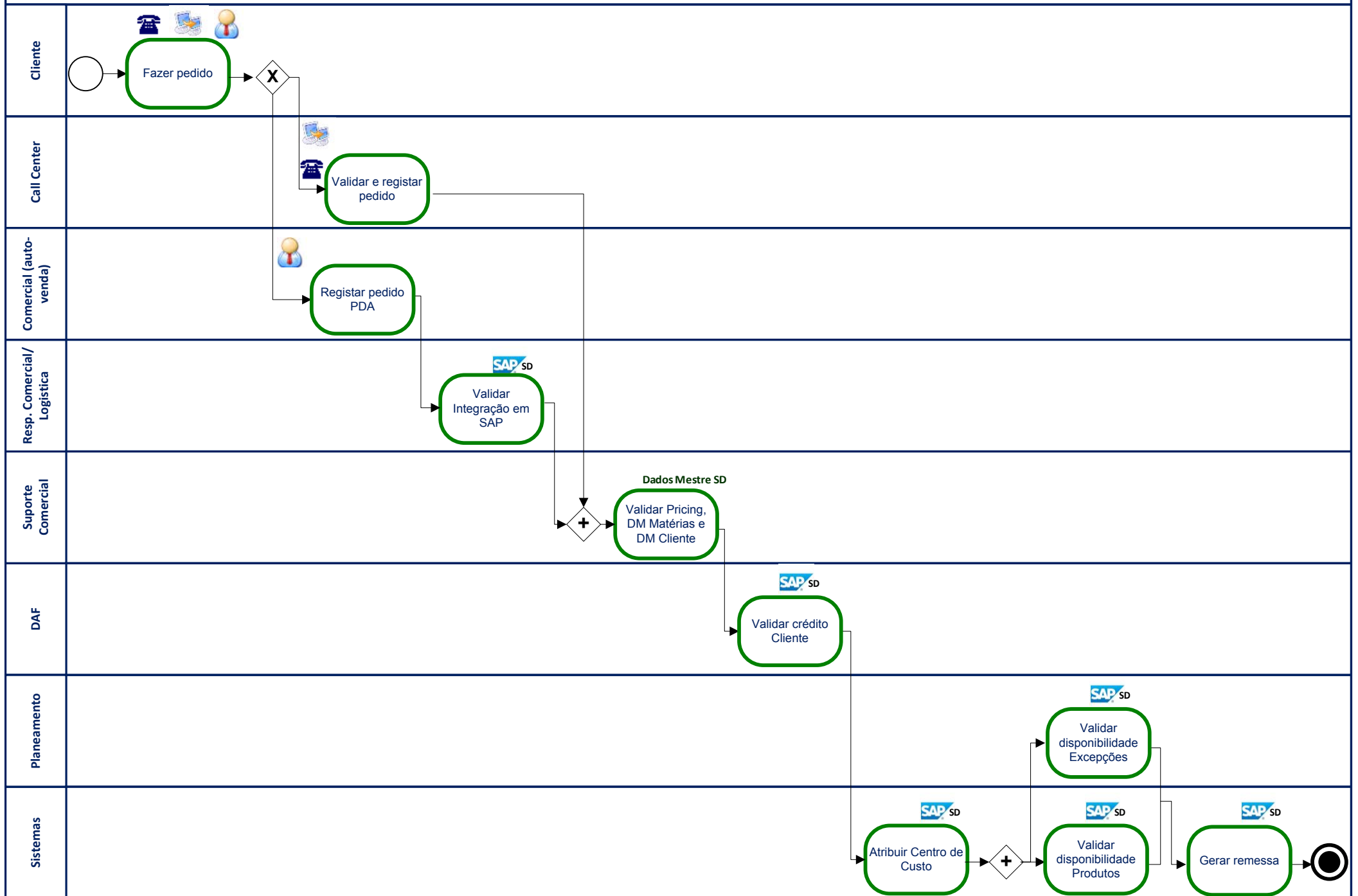
Young, Dale. 2004. Human Resources have a vital role to play within employee identity and access management. *Network Security*. November: 5-7 – (Young 2004)

ANEXO A: Mapeamento dos processos core de negócio

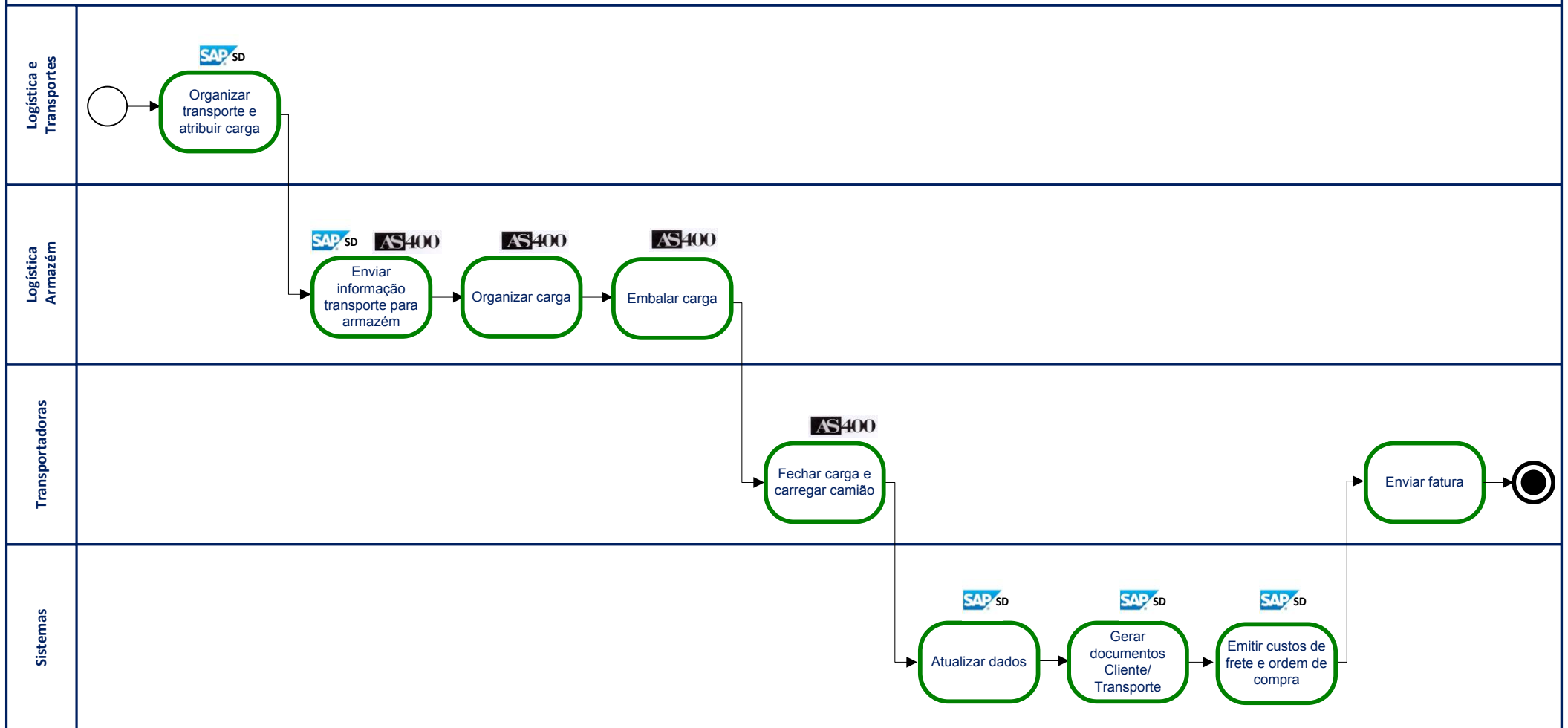
Produzir Lacticínios



Tratar Encomenda



Tratar Carga



ANEXO B: Grau de criticidade das atividades dos processos de negócio

Anexo B - Grau de criticidade das atividades dos processos de negócio

Nível 1	Os processos de negócio devem estar disponíveis durante todas as horas de trabalho/sempe (o objectivo de recuperação deverá ser inferior a duas horas);
Nível 2	Os processos de negócio podem ser executados sem algumas actividades normais por um período limitado de tempo (objectivo de recuperação entre 2 a 24 horas);
Nível 3	O negócio pode sobreviver por um periodo mais longo (até três dias) com perda de dados até um dia (objectivo de recuperação entre 24 a 72 horas)
Nível 4	O negócio pode sobreviver por um período mais alargado (objectivo de recuperação superior a 72 horas)

Macro Processo	Actividades	Sistemas Informação	Nível de Criticidade
Tratar encomenda	Fazer pedido encomendas automático	SAP ECC SD	Nível 1
	Fazer pedido encomendas manual	SAP ECC SD	Nível 1
	Determinar centro (armazém)	SAP ECC SD	Nível 1
	Controlar/Validar crédito	SAP ECC SD	Nível 2
	Fazer pedido de carga (Auto-venda – AV)	SAP ECC SD + servidores SRLEITE xx	Nível 2
	Verificar disponibilidade produtos	SAP ECC SD	Nível 1
	Fazer pedidos de carga (Pré-vendedores)	SAP ECC SD + servidores SRLEITE xx	Nível 2
Tratar carga	Enviar cargas para WHM	SAP ECC SD + AS400 (WHM)	Nível 1
	Fechar cargas	SAP ECC SD + AS400 (WHM)	Nível 1
	Emitir facturas electrónicas	SAP ECC SD	Nível 3
	Emitir Pré Facturação Vigor	SAP ECC SD	Nível 1
	Enviar informação de Rotas (Listas Visitas e Pricing)	SAP ECC SD + servidores SRLEITE xx	Nível 1
	Movimentar stocks	SAP ECC MM + SAP ECC FI	Nível 1
	Movimentar produto	PDT's terminais portáteis em AS400 (WHM)	Nível 1
	Fazer fecho de rotas (AV)	SAP ECC SD + servidores SRLEITE xx	Nível 2
Produzir lacticínios	Recepcionar de leite cru	SAP ECC MM + AS400	Nível 1
	Informar fornecedores leite	SAP ECC MM + AS400	Nível 4
	Prepararar de lotes	SAP ECC PP	Nível 1
	Encher produto acabado	SAP ECC PP + AS400 (WHM)	Nível 1
	Controlar estatisticamente produção	Accept + SAP ECC QM	Nível 3
	Aprovar lote	SAP ECC QM + ACCEPT	Nível 1
	Movimentar MP's	SAP WM + PDT's	Nível 3
	Alocacar MP'S	SAP WM + PDT's	Nível 3

Anexo B - Grau de criticidade das atividades dos processos de negócio

Macro Processo	Actividades	Sistemas Informação	Nível de Criticidade
Calcular rappel	Rappel	SAP ECC SD	Nível 2
Actualizar Dados-Mestre	Fazer Abertura cliente	SAP ECC (Dados Mestres)	Nível 3
	Fazer Abertura Produto	SAP ECC (Dados Mestres)	Nível 3
	Fazer Manutenção dados Produção	SAP ECC (Dados Mestres)	Nível 2
	Fazer Manutenção dados Qualidade	SAP ECC (Dados Mestres)	Nível 3
	Fazer Abertura mês	SAP ECC MM + SAP ECC FI	Nível 1
	Fazer Manutenção preço	SAP ECC SD	Nível 2
	Definir acordos promocionais	SAP ECC SD	Nível 2
	Gerir tabelas parametrização	SAP ECC (Parametrização)	Nível 2
Fechar tempos e remunerações	Processar salários	SAP ECC HCM + SAP ECC FI	Nível 2
	Processar tempos de trabalho	SAP ECC HCM	Nível 4
Tratar documentação fiscal	Submeter declarações fiscais	SAP ECC FI/CO	Nível 2
Tratar cobranças	Enviar cobranças	SAP ECC FI/CO	Nível 2
Pagar fornecedores	Pagar aos fornecedores	SAP ECC FI/CO	Nível 4

ANEXO C: Levantamento de incidentes que afetam os SI

Descrição do incidente	PROPRIEDADES DA INFORMAÇÃO AFECTADAS			Impacto/Alvos	Frequencia	Medidas/Sugestões
	Disponibilidade	Integridade	Confidencialidade			
Falha de energia				Afetou as operações de negócio; infraestruturas (switch) e as aplicações. Não existiu perda de informação existente, apenas indisponibilidade de acesso.	Pouco frequente (2 xs ano)	Backups, restore (P10).
Shutdown descontrolado				Inconsistencia de dados quando se voltam a ligar os sistemas	Pouco frequente (2 xs ano)	Sistemas que desligue controladamente os sistemas e os volte a ligar de forma ordenada
Quando ligaram cabos, as UPS deitaram sistemas abaixo				Afetou as operações de negócio e as aplicações. Não existiu perda de informação existente, apenas indisponibilidade de acesso.	Pouco frequente (1 x ano)	Backups
Paragem das comunicações por falha técnica do provider (PT)				Operações e informação (indisponibilidade de acesso)	Pouco frequente (1 x ano)	
IBM deu indicações erradas na resolução de um problema que resultou na paragem de sistemas				Afetou as operações de negócio e as aplicações. Não existiu perda de informação existente, apenas indisponibilidade de acesso.	Pouco frequente (1 x ano)	
Um grupo de colaboradores da Lactogal acedeu a informação confidencial (listagens de remunerações dos colaboradores da lactogal)				O acesso a informação sensível e restrita pode afetar os processos de negócio, sobretudo pela quebra de produtividade com origem na desmotivação de colaboradores, mau ambiente e conflitos interpessoais.	Pouco frequente (1 x ano)	Implementação de um sistema de gestão de identidades e de acessos, definição de matriz de responsabilidades e workflows na gestão de identidades e de acessos.

Descrição do incidente	PROPRIEDADES DA INFORMAÇÃO AFECTADAS			Impacto/Alvos	Frequencia	Medidas/Sugestões
	Disponibilidade	Integridade	Confidencialidade			
Conflitos de versões e passagem para produtivo de versões não testadas previamente				Aplicações, processos e informação.	Frequente (mais de 2xs ano)	Restringir as permissões de programação aos gestores aplicacionais. Definição clara das responsabilidades e papéis de cada colaborador do DSI.
Alteração de acessos de utilizadores automáticos sem aviso				Processos, aplicações e informação	Frequente (mais de 2xs ano)	Melhoria dos processos de comunicação e definição do fluxo de informação de todas as actividades que afectam os sistemas de informação para todas as partes interessadas.
Utilizador fica sem receber ou enviar emails por ter atingido a cota máxima				Operações e informação	Frequente (mais de 2xs ano)	Sensibilizar utilizadores para boas práticas de gestão da conta de email.
Upgrade de sistemas não é comunicado às partes interessadas (ex SAP ECC). Este facto resulta em inconsistências de objectos em produtivo e em SAP corrompendo o próprio upgrade				O sucesso do próprio upgrade (processos), informação e aplicações	Frequente (mais de 2xs ano)	Melhoria dos processos de comunicação e definição do fluxo de informação de todas as actividades que afectam os sistemas de informação para todas as partes interessadas.
Sub utilização das capacidades dos sistemas de informação. Por desconhecimento, os utilizadores por vezes realizam operações complexas que exigem uma maior capacidade dos sistemas quando na verdade poderiam obter as mesmas informações de forma menos complexa e usando menos recursos. Ex: relatórios de BW				Aplicações e processos	Frequente (mais de 2xs ano)	Deveria existir um plano de formação regular para os utilizadores finais de maneira a otimizar a utilização de todas as ferramentas disponíveis pelos sistemas de informação.

Descrição do incidente	PROPRIEDADES DA INFORMAÇÃO AFECTADAS			Impacto/Alvos	Frequencia	Medidas/Sugestões
	Disponibilidade	Integridade	Confidencialidade			
Funcionalidade de programas ou aplicações comprometida pela baixa ou inexistente participação dos programadores internos no levantamento de requisitos e arquitetura dos sistemas (fases iniciais do desenvolvimento). Não assegurando confidencialidade dos dados na concepção de novos desenvolvimentos				Aplicações	Frequente (mais de 2xs ano)	Os programadores (gestores aplicacionais) deviam participar nas diferentes fases de um projecto de desenvolvimento de nova aplicação ou em alterações às existentes.
Utilizadores criam tickets para o helpdesk para solicitar resolução de pequenos problemas que poderiam ser resolvidos imediatamente pelos próprios (ex: instalação de impressoras)				Processos	Frequente (mais de 2xs ano)	Existe já um projeto de formação para utilizadores que vai ser estendido a cerca de 90% dos users e tem como principal objetivo a diminuição destes tickets e o aumento da produtividade. O projeto vai ser assegurado pela área de Tecnologias da Informação e terá início no segundo semestre do ano.
Desconhecimento por parte dos utilizadores finais do impacto das suas acções. Por exemplo criam uma ordem no sistema e nunca mais dão seguimento ao que criaram, sem perceberem que isso vai gerar um conjunto de inconformidades noutros processos, por exemplo no crédito.				Processos e informação	Frequente (mais de 2xs ano)	Supervisão e sensibilização dos utilizadores finais.

Descrição do incidente	PROPRIEDADES DA INFORMAÇÃO AFECTADAS			Impacto/Alvos	Frequencia	Medidas/Sugestões
	Disponibilidade	Integridade	Confidencialidade			
Algumas não conformidades (erros) detectadas em aplicações são frequentemente assumidas como um problema de programação. Como resultado, existe dispendio de tempo por parte dos gestores aplicacionais para perceberem a sua origem. Contudo, verifica-se que parte desses problemas poderiam ser identificados e resolvidos, desde logo pelo key user ou pelo gestor funcional, numa primeira análise.				Processos	Frequente (mais de 2xs ano)	Definição clara de procedimentos e papéis de cada colaborador dos DSI
O help desk é utilizado de forma errada pelos utilizadores que o usam,frequentemente, para tirarem dúvidas sobre a execução de tarefas e não para reportarem erros, contribuindo para a lentidão de outros serviços prestados pelo DSI				Operações	Frequente (mais de 2xs ano)	Sensibilização aos utilizadores finais sobre o papel do help desk e a necessidade de tirarem duvidas com colegas ou key users e usarem o help desk apenas para reporte de erros
Falha na comunicação GPRS impossibilita a actualização dos PDA's na rua				Processos, aplicações e informação	Pouco frequente (1 x ano)	

Descrição do incidente	PROPRIEDADES DA INFORMAÇÃO AFECTADAS			Impacto/Alvos	Frequencia	Medidas/Sugestões
	Disponibilidade	Integridade	Confidencialidade			
Tecnico de sistemas procedeu a backup que interferiu no desempenho das maquinas de qualidade e desenvolvimento. Esta operação impediu colaboradores de Espanha de efetuarem um conjunto de procedimentos que estava previsto. O tecnico de sistemas não tinha informação de que as máquinas iam ser utilizadas pelos colaboradores espanhois				Operações e aplicações. Não existiu perda de informação existente, apenas indisponibilidade de acesso.	Pouco frequente (1 x ano)	Melhoria dos processos de comunicação e definição do fluxo de informação de todas as actividades que afectam os sistemas de informação para todas as partes interessadas.

ANEXO D: Questionário

“Utilização dos Serviços da Direção dos Sistemas de Informação - Diagnóstico de Necessidades Formativas dos Colaboradores do Grupo Lactogal”

QUESTIONÁRIO

UTILIZAÇÃO DOS SERVIÇOS DA DIRECÇÃO DOS SISTEMAS DE INFORMAÇÃO - DIAGNÓSTICO DE NECESSIDADES FORMATIVAS DOS COLABORADORES DO GRUPO LACTOGAL

Este questionário está inserido no âmbito do Mestrado em Engenharia de Serviços e Gestão da FEUP, da aluna Susana Coutinho, actualmente a desenvolver o projecto de dissertação na Direcção de Sistemas de Informação (DSI), do Grupo Lactogal.

Tem como objectivo principal sustentar um plano formativo para a optimização da utilização dos sistemas de informação, por parte dos utilizadores finais, considerando a sua percepção sobre as maiores dificuldades apresentadas na execução de tarefas.

Deste modo, o documento foi revisto e validado pela Direcção de Recursos Humanos e Comunicação (DRHC) e pela Direcção dos Sistemas de Informação. Todas as respostas são anónimas e confidenciais e os dados recolhidos serão utilizados apenas para os fins já mencionados.

DADOS SÓCIO-PROFISSIONAIS

Idade: ____ **Sexo:** Masculino ☐ Feminino ☐

Área:

Administrativo-financeiro ☐ Compras ☐

Comercial ☐ Eng.º Industrial ☐

Qualidade ☐ Recursos Humanos ☐

Funções corporativas ☐ Logística ☐

Industrial ☐ Marketing ☐

Função: _____

PARTE 1 – AVALIAÇÃO GERAL DOS SERVIÇOS DA DSI

1. Na sua opinião, globalmente, como avalia a qualidade dos serviços prestados pela DSI, actualmente?

Má ☐ Baixa ☐ Satisfatória ☐ Boa ☐ Muito Boa ☐

2. Que sugestões de melhoria dos serviços da DSI, gostaria de deixar?

PARTE 2 - NECESSIDADES FORMATIVAS

1. Na utilização de aplicações **SAP**, dê exemplos, por favor, das tarefas que lhe parecem ser mais difíceis de executar, considerando os módulos que **habitualmente usa**:

SAP ECC MM - Compras	Apoia funções de fornecimento e manutenção de stocks
(ex: tenho dificuldade em criar documentos de compras)	

SAP ECC WM - Gestão de Armazém MP	Apoia funções de gestão do armazém desde a entrada de mercadoria, gestão do inventário, picking e abastecimento à produção
(ex: tenho dificuldade em reimprimir etiquetas de palete)	

SAP ECC PP - Gestão de Produção	Apoia funções de planeamento e controlo da produção
(ex: tenho dificuldade em abrir ordens de produção ou enviá-las para processamento em armazém; tenho dificuldade em dar consumos/entradas de produção)	

SAP ECC PM - Gestão de Manutenção	Apoia funções de planeamento, processamento e execução de tarefas de manutenção
(ex: tenho dificuldade em criar planos de manutenção)	

SAP ECC RH - Gestão de Recursos Humanos	Apoia funções de planeamento, registo e avaliação de todos os dados relativos aos colaboradores da empresa
(ex: tenho dificuldade em fazer alterações de dados-mestre; tenho dificuldade em corrigir erros de processamento salarial no sistema)	

SAP ECC FI- Financeira	Apoia a gestão financeira e processa a contabilidade
(ex: tenho dificuldade em corrigir ligações com entidades externas; tenho dificuldade em registar dados contábeis)	

SAP ECC QM – Gestão da Qualidade	Apoia as funções de planeamento e controlo de qualidade
(ex: tenho dificuldade em aprovar um lote; os resultados das análises não integram em SAP)	

SAP ECC LETRA – Transportes	Apoia as funções de execução logística e transportes
(ex: tenho dificuldade em criar o custo de transporte; tenho dificuldade em analisar o status de “fecho de carga”)	

SAP ECC SD – Vendas	Apoia as funções resultantes das actividades dos processos de venda
(ex: tenho dificuldade em interpretar alguns campos de uma factura; tenho dificuldade em (re) imprimir documentos)	

SAP BW – Informação de Gestão	Fornece ferramentas analíticas e soluções de armazenamento de dados e relatórios para a organização
(ex: tenho dificuldade em utilizar todas as funcionalidades do Bex Analyzer)	

SAP CRM – Gestão da Relação com o Cliente	Apoia as funções de gestão da relação com o cliente tais como gestão das reclamações, gestão de campanhas de marketing, acções de trade e gestão do contacto com clientes
(ex: tenho dificuldade em criar uma campanha, tenho dificuldade em aceder às minhas actividades)	

SAP APO	Apoia as funções relacionadas com a optimização da gestão da cadeia de abastecimento
(ex: tenho dificuldade em verificar se o tipo de erros que ocorrem nos processos nocturnos, afectam o meu trabalho)	

2. Na utilização do **Microsoft Office**, considere os programas que habitualmente utiliza.

Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar considerando a utilização do Microsoft **Word** (Processamento de texto)

Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar considerando a utilização do Microsoft **Excel** (Folha de Cálculo)

Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar considerando a utilização do Microsoft **Powerpoint** (Apresentações Gráficas)

Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar considerando a utilização do Microsoft **Outlook** (Correio Electrónico)

3. Na utilização do **ACCEPT (Ferramenta de Controlo Estatísticos de dados da qualidade)**
Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar

(ex: tenho dificuldade em enviar resultados para SAP quando existem erros pendentes em SAP)

4. Na utilização do **WHM (AS400) (Sistema de processamento de movimentos de stock de produto acabado)**
Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar

(ex: tenho dificuldade em corrigir um erro quando existe alguma anomalia no processo)

5. Na utilização da **Intranet (LACNET)**
Exemplifique, por favor, que actividades associadas às suas tarefas são, na sua opinião, mais difíceis de executar

(ex: tenho dificuldade em efectuar pesquisas e em encontrar a informação que necessito)

Parte 3 – UTILIZAÇÃO DO SERVIÇO HELP DESK

1. Considerando a utilização que faz do HELP DESK refira como utiliza habitualmente este serviço (Assinale, por favor, a resposta correspondente ao **uso mais frequente**)

- ☐ Solicitar esclarecimentos sobre realização de tarefas suportadas pelos sistemas de informação (ex: como obtenho um relatório no SAP?)
- ☐ Reportar problemas relacionados com as tecnologias da informação (ex: problemas de arranque do pc, problemas de impressão, cabos avariados, entre outros)
- ☐ Reportar erros na utilização das aplicações (SAP, ACCEPT, OFFICE, AS400) sempre que estes impeçam a normal execução das tarefas diárias
- ☐ Solicitar esclarecimentos sobre a utilização das tecnologias da informação (ex: como faço para instalar uma impressora de rede?)
- ☐ Solicitar nova password e/ou reportar erros de acesso a sistemas/aplicações
- ☐ Outra: _____

MUITO OBRIGADA PELA SUA PARTICIPAÇÃO!

ANEXO E – Identificação de dificuldades dos colaboradores na utilização dos SI

Sistemas/Aplicações		Dificuldades Identificadas pelos Utilizadores	
ERP SAP	SAP ECC	MM	Tirar uma única listagem com referencia do fabricante; preços e n.º de fornecedor; Pedidos de compra quantidades, Preços e n.º de fornecedor; Tirar listagem directa para a rotação de stocks e uma outra para a consulta dos ajustes; Sintetizar informação, muitas vezes é necessário tirar do SAP várias listagens para posteriormente compilar a informação.
		WM	Dificuldade em obter informação detalhada dos movimentos diários Analisar informação na transacção MB51. imprimir etiquetas de caixa e paletes Dificuldade em obter informação detalhada por dia Conhecer todas as funcionalidades do módulo.
		PP	Gerir os parametros que permitam ter sugestões de produção de qualidade Elaboração de planos de produção Ajustes de stocks Devolução de material ao AMP (Armazém Matérias Primas) Registos no PDT Parametrizar as capacidades dos recursos da fábrica de modo a reflectir a realidade Abrir op's Dar consumos Análise de erros Gestão de sub-produtos Perceber funcionalidades do módulo: é possível abrir ordens tal como as encerramos? Quando me engano ao dar consumos ZT não consigo corrigir erros como no Zorigem
		PM	Criação de reservas ao armazem de peças e visualização das mesmas Na consulta de notas encerradas, por encerrar ou abertas, o relatório apresentado não é muito conclusivo e tenho alguma dificuldade em obter a informação
		RH	Necessidade de conhecer todas as funcionalidades de forma a aprofundar e sistematizar tarefas diárias falta de conhecimento de todas as funcionalidades do módulo, sobretudo no processamento de salários Conhecer todas as funcionalidades do SAP que nos permite obter melhor aproveitamento do programa Não conseguimos criar horários
		FI	Parametrizações cash and liquidify Emissão de relatórios com a informação pretendida Query Não conhecer todas as potencialidades do módulo
		QM	Não foram registadas dificuldades na utilização deste módulo pelos utilizadores.
		LETRA	Dificuldade de fecho de cargas por exemplo quando transporte é criado como exportação Processo de brindes Dificuldade na percepção das paletes reais vs sistema Análise de custos de cargas (critérios de criação de custos) Análise do histórico de cargas
		SD	Gerir o direccionamento de encomendas para os centros correctos Dificuldade em interpretar algumas ofertas e relação de bónus Perceber quem fez alterações nos documentos Interpretar notas de crédito (motivos) Tirar listagens para consulta Interpretação do fluxo de documentos (ordem-GR-factura-etc) Retirar informação/customizar relatorios Pesquisar dados sobre clientes Reemprimir documentos Interpretar a relação bónus/acções que um cliente tem Gerir tabela de exclusão de materiais Análise à estrutura comercial dos clientes Analisar débitos de rappel Dificuldades em algumas análises relativas a clientes
		SAP BW	Conhecer todas as funcionalidades do módulo. análises de suporte actualização de dados
		SAP CRM	analisar reclamações da qualidade Classificar tipo de reclamação Consultar e encontrar FAQ Actualização de dados Fazer a distinção entre as várias reclamações Definir reclamação de um cliente se é qualidade, comercial, logística Registo de pedidos de informação e reclamações de clientes Na gestao de reclamações, falta informação sobre problemas com cargas
		SAP APO	Definição das parametrizações Plano de produção Verificar impacto dos erros que ocorrem nos processos nocturnos no meu trabalho Perceber se os dados foram carregados e actualizados

Microsoft Office	WORD	Criar caixas de texto Indices impressão em série
	EXCEL	Interligação entre folhas de cálculo Formulários para preenchimento automático Tabelas dinâmicas Filtro de dados Divisão de células Gráficos Macros Fórmulas
	POWERPOINT	Vídeo e audio Dinamizar apresentações
	OUTLOOK	Organização e gestão eficaz do arquivo Procurar mensagens arquivadas Partilhar tarefas com colegas Agendar reuniões;

INTRANET	Consulta de dados Emissão de certificados e boletins Preencher boletins de análise Fazer pesquisa por conteúdo Imprimir Academia Lactogal Dificuldade em pesquisar informação Dificuldade em encontrar fichas/fotos actualizadas de produto
ACCEPT	Elaborar relatórios genéricos (não de processo a processo) Compreender os erros quando ocorrem
AS400 (WHM)	corrigir erros quando existem anomalias no processo Dificuldade em imprimir os lotes dos queijos. Por vezes não consigo sequer visualizar esta informação Dificuldade em obter listagens

ANEXO F – Política de Segurança da Informação do Grupo Lactogal

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 1/21
	Direcção de Sistemas de Informação	Versão Draft 02

Índice

1 - INTRODUÇÃO	2
O que é a segurança da informação?	2
Âmbito.....	2
Objectivos	2
2 - PRINCÍPIOS DE SEGURANÇA.....	4
3 - POLÍTICAS DE SEGURANÇA.....	5
3.1 - Definição das Políticas de Segurança de Informação	6
3.2 - Controlo e Classificação de Activos	7
3.3 - Responsabilidades do colaborador.....	9
3.4 - Formação de Colaboradores.....	10
3.5 - Segurança física e ambiental	11
3.6 - Gestão de computadores e redes.....	12
3.7 - Controlo de acessos	14
3.8 - Auditoria e Conformidade	16
4 - GLOSSÁRIO.....	17

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 2/21
	Direcção de Sistemas de Informação	Versão Draft 02

1 - INTRODUÇÃO

O que é a segurança da informação?

A informação é um ativo que possui grande valor para a Lactogal, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A segurança da informação é a protecção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Âmbito

A complexidade associada ao uso dos sistemas de informação e o cumprimento dos requisitos legais vigentes, aconselham a elaboração de diretrizes claras e concisas que definam as normas e procedimentos a seguir no tratamento e segurança da informação e que complementam o estilo, práticas e costumes da Lactogal. Por essa razão, a Administração da Lactogal considerou necessário melhorar o seu posicionamento estratégico em matéria de segurança de informação, através da aprovação de um Manual de Políticas de Segurança da Informação.

As políticas de segurança de informação aqui descritas foram baseadas nas recomendações propostas pela norma ISO/IEC 27002:2005, reconhecida mundialmente como um código de boas práticas para a gestão da segurança da informação, e estão de acordo com as leis vigentes no nosso país.

Objectivos

O objectivo principal destas políticas consiste no estabelecimento das bases da Segurança da Informação da Lactogal, de modo a assegurar:

- A acessibilidade controlada e a disponibilidade da informação, de acordo com a criticidade e o valor da mesma;

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 3/21
	Direcção de Sistemas de Informação	Versão Draft 02

- A confidencialidade, integridade e disponibilidade da informação em qualquer suporte;
- A continuidade das operações de negócio.

Estes requisitos devem estar presentes em todos os processos do ciclo de vida da informação (criação, utilização, actualização, conservação, distribuição e destruição) e do respectivo sistema de suporte (processamento, armazenamento e transmissão), quer este seja manual ou automatizado, e independentemente de se encontrar sob a tutela administrativa e operacional da Lactogal, ou de entidades externas.

Considera-se de importância estratégica a existência de uma “Cultura de Segurança”, que propicie a todos os colaboradores da Lactogal uma perspectiva clara das suas responsabilidades no âmbito da Segurança da Informação.

A eficiência das Políticas aqui definidas, passa pela respectiva divulgação, implementação e permanente actualização.

Para cumprimento destes objectivos, estão aqui descritas as políticas de segurança da informação que pretendem regulamentar a definição das diferentes políticas, o controlo e classificação de ativos, as responsabilidades de cada colaborador, a formação nesta temática, a segurança física e ambiental, a gestão de computadores e rede, o controlo de acessos e a auditoria e conformidade com o cumprimento das políticas estabelecidas.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 4/21
	Direcção de Sistemas de Informação	Versão Draft 02

2 - PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Estes são os Princípios que devem orientar a prática da Segurança da Informação na Lactogal e que traduzem a estratégia da empresa, no que diz respeito à protecção e manutenção da integridade, confidencialidade e disponibilidade da informação.

1. A estratégia da Administração em Segurança da Informação assume a figura de uma Política de Segurança, a qual deve ser do conhecimento de todos os colaboradores da Lactogal.
2. Toda a informação e património pertença da Lactogal deve ser classificado de acordo com o seu valor, sensibilidade e risco face a possíveis ameaças e requisitos legais vigentes.
3. Todos os sistemas de informação da Lactogal devem ser utilizados, única e exclusivamente, para a execução de processos de negócio.
4. Os colaboradores da Lactogal que manipulem informação, devem ser instruídos e doutrinados na temática da Segurança.
5. O acesso físico aos Sistemas de Informação da Lactogal, bem como as condições ambientais que as envolvem, devem ser controladas.
6. Cada colaborador da Lactogal só deve ter acesso à informação e aos recursos necessários ao desempenho das suas actividades.
7. Devem ser planeados e implementados requisitos de segurança em todas as fases do ciclo de vida das tecnologias de informação.
8. Os sistemas de informação devem ser regularmente auditados por forma a verificar o grau de cumprimento das Políticas, Normas e Procedimentos que se encontram definidos.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 5/21
	Direcção de Sistemas de Informação	Versão Draft 02

3 - POLÍTICAS DE SEGURANÇA

As políticas de segurança encontram-se estruturadas segundo a seguinte ordem:

1. Definição das políticas de Segurança da Informação
2. Controlo e classificação de activos
3. Responsabilidades do colaborador
4. Formação de colaboradores
5. Segurança física e ambiental
6. Gestão de computadores e redes
7. Controlo de acessos
8. Auditoria e conformidade

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 6/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.1 - Definição das Políticas de Segurança de Informação

1. O documento de Políticas de Segurança da Informação prevê os requisitos de Segurança da Lactogal e representa uma declaração dos princípios e dos objectivos da Administração da Lactogal no âmbito da Segurança dos Sistemas de Informação.
2. As Políticas de Segurança da Informação são aplicáveis a todos os departamentos, aos seus colaboradores internos efectivos e não efectivos (tais como os trabalhadores temporários, trabalhadores honorários, contratados, entre outros), a todos os colaboradores externos (fornecedores, consultores e auditores), e a toda a informação residente nos sistemas de informação da Lactogal. Ter-se-ão de vincular a estas Políticas todos os parceiros e empresas externas que necessitem de utilizar a Infra-estrutura Informática da responsabilidade da empresa.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 7/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.2 - Controlo e Classificação de Activos

1. Toda a informação deve ser classificada segundo as três vertentes de Segurança: Confidencialidade, Integridade e Disponibilidade. Deve conter informação acerca do seu período de validade e acerca da categoria para o qual transitará após esse período. Essa classificação deve estar suportada num processo que permita proceder a uma análise de risco associada à perda de segurança dessa informação.
2. A confidencialidade da informação deve ser classificada segundo três categorias para que possa ser definido o seu nível de importância e de segurança: CONFIDENCIAL, USO INTERNO e PÚBLICA. Este sistema standard deve ser utilizado em toda a Lactogal:
 - a. CONFIDENCIAL: Esta categoria é aplicável à informação que só deve ser utilizada dentro de um grupo restrito e identificado de pessoas pertencentes à Lactogal. A disseminação não autorizada desta informação poderá prejudicar seriamente a empresa, os seus accionistas, os seus sócios comerciais ou os seus clientes.
 - b. USO INTERNO: Esta categoria é aplicável à informação destinada apenas a uso interno dos colaboradores. A empresa poderá sofrer algum impacto adverso caso esta se torne do conhecimento geral.
 - c. PÚBLICA: Esta categoria é aplicável a toda a informação não classificada dentro das categorias anteriores. A empresa, os accionistas, os empregados e clientes, não sofrerão nenhum impacto adverso caso esta informação se torne do conhecimento geral.
3. Se por razões relacionadas com a actividade da Lactogal, for necessário manter informação (em formato electrónico ou físico) que já não reflecta a situação actual da empresa, dever-se-á indicar que tal informação está OBSOLETA.
4. Toda a informação armazenada em qualquer tipo de media (papel, tapes, cd's, dvd's, entre outros), deve estar etiquetada com a classificação correspondente. No caso dos

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 8/21
	Direcção de Sistemas de Informação	Versão Draft 02

ficheiros conterem informação de diferentes categorias, o ficheiro deve ser etiquetado com a classificação mais alta de qualquer elemento de informação nele contido.

5. Os colaboradores devem seguir as seguintes regras de manuseamento e modos de transmissão/ destruição para o caso da Informação confidencial:
 - a. A etiqueta deve ser colocada em local visível e de fácil leitura.
 - b. A classificação Confidencial pode ser seguida pela data, tal como: "Confidencial até: 11/12/2014". Após essa data o proprietário da informação deverá rever a classificação da informação.
 - c. Os faxes que acompanham informação confidencial devem também ser etiquetados como Confidencial.
 - d. A etiqueta de classificação pode ser removida ou alterada caso a classificação sofra alterações.
 - e. A informação confidencial só pode ser copiada e distribuída por uma pessoa com necessidade de conhecimento e entregue a outra pessoa com necessidade de conhecimento.
 - f. Quando já não for necessária, a informação confidencial deve ser destruída num destruidor de papel/cd's/dvd's.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 9/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.3 - Responsabilidades do colaborador

1. Os sistemas de informação da Lactogal são propriedade da mesma e são uma ferramenta de trabalho que a empresa coloca à disposição dos colaboradores para o desempenho das suas funções. Por princípio, os colaboradores não podem usar os sistemas de informação para levar a cabo interesses pessoais.
2. Todos os contratos de trabalho assinados pelos colaboradores internos, efectivos e não efectivos (tais como os trabalhadores temporários, trabalhadores honorários, contratados, entre outros) devem incluir uma cláusula de confidencialidade que os responsabilize perante situações de fuga de informação.
3. Todos os colaboradores internos, efectivos e não efectivos (tais como os trabalhadores temporários, trabalhadores honorários, contratados, entre outros) e todos os colaboradores externos (fornecedores, consultores e auditores) devem assinar um termo de responsabilidade em que se comprometem a desenvolver o seu trabalho conforme as políticas, normas e procedimentos de Segurança. Este termo de responsabilidade deverá ser ajustado às funções desempenhadas pelo colaborador para, e dentro, da Lactogal, devendo ser revisto periodicamente, em intervalos regulares de tempo.
4. A violação das políticas de segurança da Lactogal por parte de algum colaborador interno, pode acarretar em última instância, o levantamento de acções disciplinares ajustadas à natureza da violação que foi cometida.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 10/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.4 - Formação de Colaboradores

1. Todos os colaboradores da Lactogal deverão ter formação em Segurança da Informação.
2. O Departamento de Recursos Humanos da Lactogal é responsável por coordenar a formação em segurança que deve ser dada a todos os colaboradores, sempre de acordo com os perfis de utilizadores que forem identificados. Devem ser realizadas acções de formação em sala, que podem ser reforçadas pela distribuição de manuais de segurança, circulares internas de alerta para temas específicos de segurança, envio de mensagens de correio electrónico, entre outros.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 11/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.5 - Segurança física e ambiental

1. Todos os colaboradores da Lactogal a quem seja atribuído um computador portátil tem de zelar pela sua segurança física dentro e fora das instalações da empresa utilizando para tal um conjunto pré-definido de controlos de segurança:
 - a. quando em viagem deixar o computador dentro dos cofres existentes no hotel;
 - b. em caso de roubo, furto ou perda do computador o utilizador deve reportar imediatamente ao DSI a ocorrência;
 - c. em viagens de avião, não despachar o computador junto com a restante bagagem;
 - d. não deixar o computador dentro dos automóveis.
2. Toda a informação não pública ou software licenciado deve ser definitivamente apagada dos dispositivos de armazenamento reutilizáveis (Ex.: discos rígidos, cd's, dvd's, tapes, entre outros) antes de estes serem entregues a empresas externas para destruição, retoma e substituição.
3. Toda a informação confidencial da Lactogal, esteja em que formato estiver, deve ser guardada de uma forma segura, sempre que o colaborador que a estiver a tratar, necessite de abandonar o seu local de trabalho por um período de tempo considerado alargado.
4. Todas os postos de trabalho, todos os servidores e todas as consolas de acesso aos sistemas centrais, têm de conter mecanismos para bloquear o acesso ao seu conteúdo, sempre que não estão a ser utilizados. Os utilizadores devem activar manualmente esses mecanismos, sempre que necessitarem de se ausentar do local onde se encontra esse equipamento (ex: "bloquear este computador" no ambiente de trabalho).

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 12/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.6 - Gestão de computadores e redes

1. A Lactogal reserva-se o direito de monitorizar a utilização dos Sistemas de Informação e de agir em conformidade, sempre que suspeitar que essa utilização viola as suas Políticas de Segurança.
2. Toda e qualquer cópia de ficheiros com origem externa (Internet, cd's, dvd's, correio electrónico, entre outras), para um sistema interno da Lactogal, deve ser limitado ao estritamente necessário para o negócio da empresa e deve ser acompanhado por uma verificação da presença de vírus informáticos, através de um anti-vírus, antes da sua execução / abertura.
3. Todo o Software instalado em todas os postos de trabalho e servidores que sejam propriedade da Lactogal, tem de ser devidamente autorizado pela empresa. Esse Software deve ser desenvolvido internamente ou deve estar em conformidade com os compromissos das licenças, acordos de compra e as leis de protecção de cópias. Como tal é estritamente proibido o carregamento e instalação de qualquer produto proveniente das mais diversas origens (Internet, correio electrónico, cd's, dvd's, entre outras) nos ditos equipamentos.
4. Caso um determinado utilizador tenha uma licença pessoal de um software e pretenda instalá-lo na sua estação de trabalho, essa utilização deve:
 - a. ser devidamente justificada e aprovada pelo seu director,
 - b. avaliado o respectivo risco de introdução de vulnerabilidades pelo responsável de segurança e pelo DSI e,
 - c. caso seja autorizado a proceder a essa instalação, esta deve ficar documentada.
5. O correio electrónico (interno ou externo) deve ser utilizado única e exclusivamente para fins profissionais. Como tal, a sua utilização deve ser cuidadosa e obedecer a um conjunto de regras que evitem a introdução de factores de insegurança nos sistemas de

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 13/21
	Direcção de Sistemas de Informação	Versão Draft 02

informação da Lactogal. Sendo assim, os utilizadores devem respeitar as seguintes regras:

- a. Devem ler regularmente as suas mensagens e eliminar as mensagens desnecessárias;
 - b. Não devem ser distribuídas mensagens que alertem para existência de vírus ou programas maliciosos (excepto para o DSI), que promovam campanhas de solidariedade (maioritariamente falsas) ou recolha de endereços (chain-letters), boatos (hoaxes), entre outros, a outros colaboradores;
 - c. Não se devem abrir mensagens de origem desconhecida ou duvidosa, ou que contenham ficheiros anexos suspeitos;
 - d. Deve existir o maior cuidado na identificação do destinatário (evitar envio erróneo de mensagens importantes);
 - e. Não se podem tentar fazer passar por outra pessoa (spoofing);
 - f. Não podem utilizar o correio electrónico para fins lúdicos (ex. envio de anedotas);
 - g. Não podem encaminhar (automática ou manualmente) mensagens de correio electrónico da Lactogal com informação (não pública e não encriptada), para sistemas de correio electrónico não geridos pela Lactogal.
6. O Correio Electrónico e a Internet não devem ser utilizados para consultar ou disseminar conteúdos considerados ofensivos ou que incitem à intolerância, violência e actividades ilegais.
 7. É estritamente proibido o armazenamento e processamento de informação não pública da Lactogal em sistemas e redes não pertencentes à empresa.
 8. É proibida a ligação de equipamentos que permitam estender a infra-estrutura de rede (ex.: routers, hubs, bridges, antenas wireless, etc) sem a devida autorização do DSI e do responsável de segurança

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 14/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.7 - Controlo de acessos

1. Todos os colaboradores autorizados devem ter um Identificador (User-ID), pessoal e intransmissível, e uma Password confidencial, que os identificará de modo único e auditável dentro dos sistemas de informação da Lactogal, e o responsabilizará pela sua correcta utilização. Esta Política deve também ser aplicável a todos os operadores dos sistemas da Lactogal.
2. Na gestão de acessos, todos os utilizadores são associados a um perfil (prédefinido) de acordo com um conjunto de atributos, entre os quais a função é mandatária. A cada perfil está associado um grupo de acessos a sistemas e serviços de informação atribuídos por defeito.
3. Qualquer pedido de acessos excepcional, isto é, que não esteja pré-definido pelo perfil obriga ao preenchimento de formulário próprio, devidamente validado pelo responsável de área.
4. Os colaboradores da Lactogal devem ter o máximo cuidado na definição e no manuseamento das suas passwords de acesso aos sistemas da Lactogal. Existe um conjunto de regras que devem ser cumpridas, as quais poderão, sempre que possível, ser configuradas nas tecnologias de informação da Lactogal. Assim sendo, as passwords:
 - a. devem ser alfanuméricas;
 - b. devem ser alteradas periodicamente (período de expiração de 90 dias);
 - c. não devem conter o userid (nome do utilizador);
 - d. devem ser alteradas após a primeira utilização;
 - e. não devem ser muito óbvias nem muito complicadas;
 - f. devem ter no mínimo 8 caracteres
 - g. não devem conter caracteres iguais consecutivos (00000000);
 - h. não devem ser usadas passwords iguais às utilizadas em locais públicos.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 15/21
	Direcção de Sistemas de Informação	Versão Draft 02

5. É proibido disponibilizar acessos não identificados e não autenticados (anónimos) a discos dos postos de trabalho e dos servidores que contenham informação confidencial

EMITIDO EM: 27-06-2012	EDIÇÃO Nº 0.2	EMITIDO	APROVADO
---	------------------------------------	----------------	-----------------

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 16/21
	Direcção de Sistemas de Informação	Versão Draft 02

3.8 - Auditoria e Conformidade

1. Toda a informação em formato electrónico que tenha sido criada, armazenada em, ou comunicada através de postos de trabalho da Lactogal são propriedade da empresa. Como tal, a Lactogal, na figura da Administração, do Responsável de Segurança ou dos Administradores de Sistemas, reserva-se o direito de aceder aos documentos ou comunicações residentes nos seus sistemas sempre que o considerar necessário, ou seja, quando existir justificativas de foro legal, de negócio ou de segurança.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 17/21
	Direcção de Sistemas de Informação	Versão Draft 02

4 - GLOSSÁRIO

Activos Físicos

Hardware que suporta os sistemas e aplicações existentes e hardware que suporta as linhas de comunicação e redes.

Activos Lógicos

Dados, aplicações, software, toda a informação em formato digital.

Activos de Informação

Activos lógicos e activos físicos.

Aplicação

Software de suporte à realização da totalidade ou de parte das actividades de uma área funcional da empresa. De um modo geral, abrange procedimentos de recolha, processamento, armazenamento e extracção de informação relativa à área funcional a que respeita.

Auditoria

Revisão independente que consiste na análise de registos e de actividades por forma a verificar a eficácia dos sistemas de controlo bem como o grau de cumprimento das políticas, standards e normas de segurança.

Autenticação

Processo de verificação da identidade de um utilizador bem como os seus privilégios de acesso aos sistemas de informação.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 18/21
	Direcção de Sistemas de Informação	Versão Draft 02

Confidencialidade

É a necessidade inerente ao negócio de partilhar ou restringir o acesso à informação e que obriga à implementação de controlos de segurança para restringir o acesso.

Controlo de Acessos

Processo que visa limitar o acesso dos colaboradores da empresa aos recursos dos sistemas de informação a que estão autorizados para o exercício das suas funções.

Disponibilidade

É a necessidade inerente ao negócio de dispor da informação quando o próprio negócio assim o requer e que obriga à implementação das medidas de segurança necessárias para o conseguir.

DSI

Departamento de Sistemas de Informação da Lactogal

Hardware

Equipamento onde está instalado o software de base, o de suporte à aplicação e a aplicação informática; por esta designação entende-se também qualquer periférico ou acessório do sistema.

Identificação

Conjunto de atributos de uma dada entidade.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 19/21
	Direcção de Sistemas de Informação	Versão Draft 02

Incidente de Segurança

Evento que poderá causar a divulgação não autorizada, modificação ou destruição de informação. São também considerados como incidentes de segurança, a perda ou destruição de equipamento informático e elementos da infra-estrutura informática.

Infra-estrutura Informática

Infra-estrutura técnica composta por hardware e software de base que suporta a exploração da aplicação informática.

Integridade

É a necessidade inerente ao negócio de controlar as alterações de informação e que obriga à implementação de controlos de segurança para proteger a precisão e exactidão da informação

Normas

São as concretizações dos princípios nos diferentes ambientes operacionais. Como exemplo desta gradação de detalhe podemos ter:

- Princípio: Todos os utilizadores devem ser autenticados por uma password.
- Norma: A password deverá conter 6 caracteres e ser alterada mensalmente.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 20/21
	Direcção de Sistemas de Informação	Versão Draft 02

Objecto Entidade que contém ou recebe informação. O acesso a um objecto tem como consequência directa o acesso à informação que lhe está associada.

Password Conjunto de caracteres alfanuméricos privados, que são utilizados no processo de autenticação de um dado utilizador.

Perfil de Acesso Associação de um dado utilizador a uma lista de objectos protegidos sobre os quais pode executar várias operações.

Procedimentos Conjunto de regras a aplicar na execução das actividades de cada processo.

Processo Sequência de actividades caracterizada por ter acontecimentos de início e de fim bem identificados e gerarem produtos mensuráveis e com valor acrescentado.

Tecnologia de Informação Conjunto formado pelas infra-estruturas informáticas, software, aplicações e dados.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

 LACTOGAL Produtos Alimentares S.A.	MANUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Pág. 21/21
	Direcção de Sistemas de Informação	Versão Draft 02

Serviços críticos

Todas as aplicações, serviços de rede e comunicações, entre outros, que a Lactogal considere extremamente importantes para o seu negócio e sem os quais a empresa seria bastante afectada no seu normal funcionamento.

Tape

Dispositivo de memória auxiliar, em suporte magnético, que permite armazenar uma quantidade bastante considerável de informação.

Vírus

É um programa de computador que, de um modo geral, tem capacidade de se copiar a si próprio para outros programas com fins destrutivos e que contém :

- Uma parte destinada a auto-reprodução a qual é responsável pela sua propagação, dando origem a cópias de si próprio, que podem interromper, modificar e destruir outros programas aos quais se prendem ou fixam.
- Outra parte que efectua acções destrutivas quando uma certa condição se verifica.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-06-2012	Nº 0.2		

ANEXO G – Manual Procedimentos de Gestão de Identidades

	MANUAL DE PROCEDIMENTOS Direcção de Sistemas de Informação	Pág. 1/5
	Gestão de Identidades	PE 008/DSI

1. OBJECTIVO

Este documento define as regras para processos no âmbito da Gestão de Identidades.

2. ÂMBITO DE APLICAÇÃO

Este procedimento aplica-se a todos os colaboradores da DSI.

3. DEFINIÇÕES

São entendidos como processos no âmbito da Gestão de Identidades todos os fluxos a aplicar na criação, manutenção de dados, manutenção de acessos, e gestão de utilizadores dos sistemas geridos pela DSI. Ficam fora do âmbito de aplicação deste procedimento os utilizadores designados como “contas de sistema” e “administradores de sistemas”.

4. MODO DE PROCEDER

A Gestão de Identidades pretende definir a “vida” de todos os utilizadores dos sistemas geridos pela DSI. Os utilizadores são criados em SAP ECC no módulo de Gestão de Recursos Humanos pela DRHC.

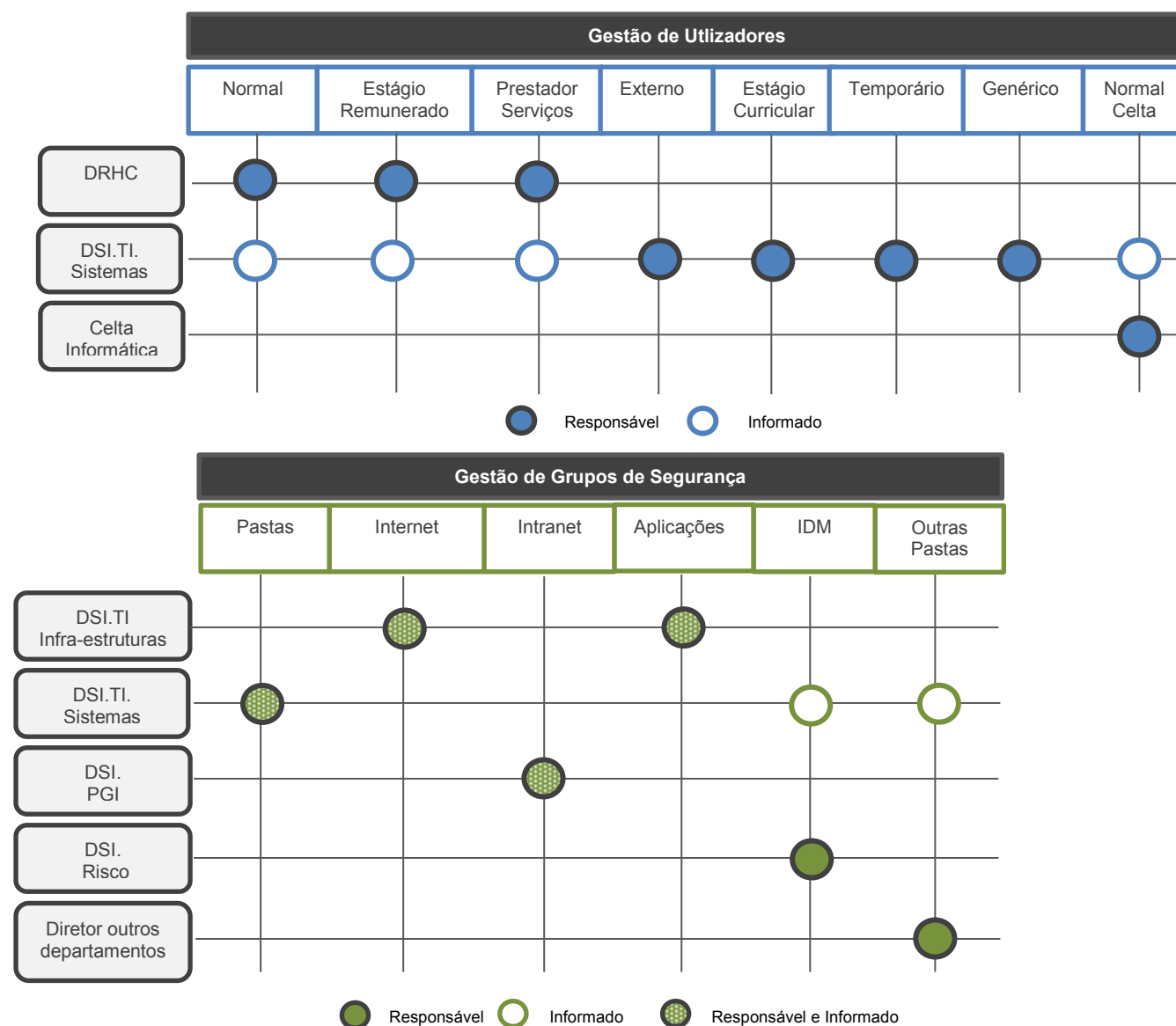
De acordo com os critérios definidos (utilizadores das empresas do grupo válidos na estrutura de RH), os utilizadores são incorporados no Portal FIM (Forefront Identity Management). Os utilizadores que não cumprem os requisitos anteriores, deverão ser criados directamente no Portal como Externos, Estagiários Curriculares, Temporários ou Genéricos.

A manutenção de dados de utilizadores directamente no Portal só poderá ser feita para os que foram criados no Portal e nunca para os que são migrados do SAP RH.

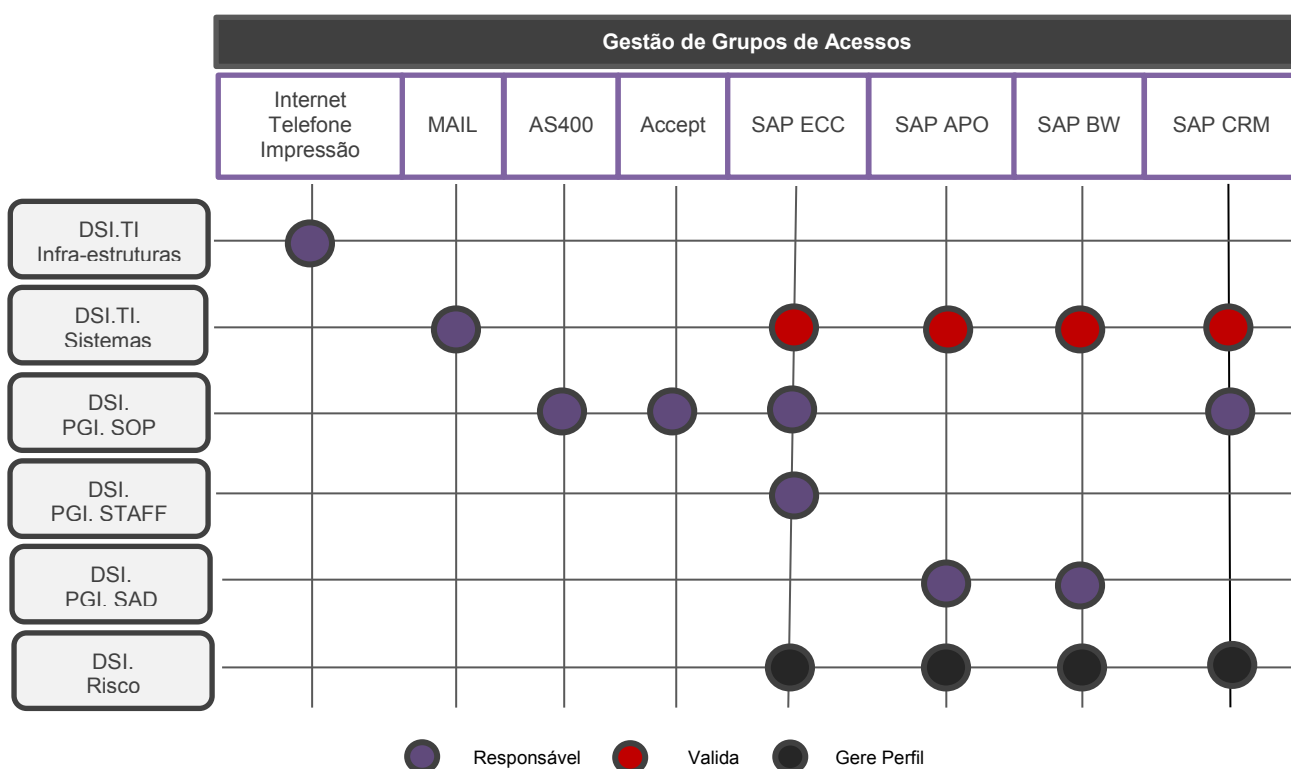
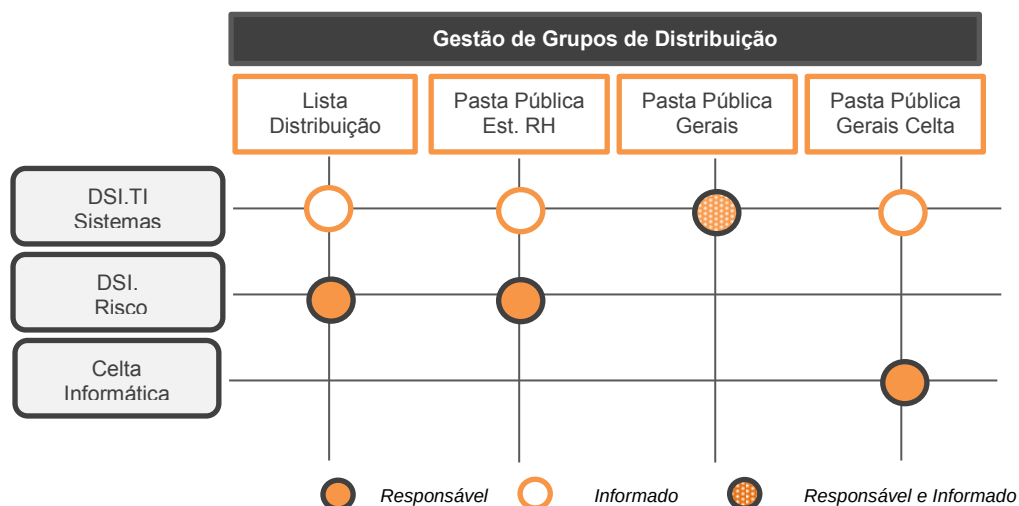
EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-01-2010	Nº 1.1		

A gestão de acessos deverá ser sempre feita pela utilização de Grupos de Segurança criados para o efeito no portal e migrados diariamente para a AD e posteriormente parametrizados na aplicação onde farão o respectivo controlo de acessos. A incorporação de utilizadores em Grupos de Segurança deverá ser feita sempre que possível com recurso à inclusão por critérios e, sempre que necessário, adicionado por gestão manual os utilizadores que correspondam a excepções.

5. RESPONSABILIDADES



EMITIDO EM: 27-01-2010	EDIÇÃO Nº 1.1	EMITIDO	APROVADO
---	--------------------------------	----------------	-----------------



É da absoluta responsabilidade de cada área de intervenção gerir apenas os objectos nos processos que lhe estão afectos respeitando as matrizes aqui apresentadas.

EMITIDO EM:	EDIÇÃO	EMITIDO	APROVADO
27-01-2010	Nº 1.1		

	MANUAL DE PROCEDIMENTOS Direcção de Sistemas de Informação	Pág. 4/5
	Gestão de Identidades	PE 008/DSI

A Gestão de Perfil definida no Sharepoint de suporte ao portal FIM será exclusivamente da responsabilidade da área de Gestão de Risco.

Será também da exclusiva responsabilidade da área da Gestão do Risco a gestão das restantes configurações existentes no Portal FIM, nomeadamente a gestão de workflows de suporte aos processos de gestão de identidades. Qualquer necessidade nesta área deverá ser validada pela chefia e, posteriormente, comunicada à área de Gestão do Risco.

O acompanhamento dos processos de sincronização automáticos será da responsabilidade da área de Sistemas.

EMITIDO EM: 27-01-2010	EDIÇÃO Nº 1.1	EMITIDO	APROVADO
---	------------------------------------	----------------	-----------------

Visão macro de responsabilidades

		DRHC	Celta Inf.	DSI Sist	DSI Infra-Es	DSI Risco	DSI PGI SOP	DSI PGI STAFF	DSI PGI SAD	Outras Direções
Gestão de utilizadores	Utilizador Standard	●								
	Utilizador Avulso			●						
	Utilizador Celta		●							
Gestão de Grupos de Segurança	Pastas			●						
	Internet				●					
	Intranet								●	
	Aplicações				●					
	IDM					●				
	Outras Pastas									●
Gestão de Grupos de Distribuição	Listas Distribuição					●				
	Pasta Publ Est. RH					●				
	Pasta Publ Gerais PT			●						
	Pasta Publ Gerais Celta		●							
Gestão de Acessos	Internet, Telf Impressão				●					
	Mail			●						
	AS400						●			
	Accept						●			
	SAP ECC						●	●		
	SAP BW								●	
	SAP APO								●	
	SAP CRM						●			

EMITIDO EM:

27-01-2010

EDIÇÃO

Nº 1.1

EMITIDO

APROVADO