IPS Instituto Politécnico de Setúbal
Escola Superior de Ciências Empresariais

Eliana Cristina Teixeira Nunes

GESTÃO DE ACESSOS AO SISTEMA DE INFORMAÇÃO.

Projeto de melhoria do processo numa empresa de telecomunicações

Dissertação/Trabalho de Projeto/Relatório de Estágio submetida como requisito parcial para obtenção do grau de **Mestre em Gestão de Sistemas de Informação**

Orientador
Dr., Pedro Anunciação, Instituto Politécnico de Setúbal

Janeiro 2018

Dedicatória

Dedico esta Dissertação de Mestrado aos meus pais e marido, sem os quais não teria sido possível a sua concretização.

Agradecimentos

A elaboração da Dissertação de Mestrado, no âmbito do mestrado de Gestão de Sistemas de Informação, apenas foi possível graças ao apoio de inúmeras pessoas que me acompanharam ao longo da realização desta dissertação.

Em primeiro lugar, quero deixar ao meu orientador, Professor Doutor Pedro Anunciação, o meu sincero agradecimento pela orientação, apoio incondicionais e paciência.

Agradeço pela amabilidade, amizade e boa disposição em todos os momentos. A sua sabedoria foi essencial para que chegasse ao fim deste projeto com um enorme sentimento de satisfação.

Agradeço a todos os colaboradores da empresa do caso de estudo, sem os quais não teria obtido todos os meios necessários para a realização desta dissertação.

Estou grata aos meus familiares pelo incentivo recebido ao longo destes anos, nomeadamente aos meus pais, Ana e António Nunes.

Por último, um agradecimento especial ao Mauro pelo apoio, compreensão na realização desta dissertação.

Para todos a minha gratidão.

Índice

Índice figuras

Índice Quadros

Lista de siglas e abreviaturas

BAU – Business as Usual

FCS – Fatores críticos de sucesso

GDPR - General Data Protection Regulation

ISO – International Standards Organization

PDCA – Plan-Do-Ckeck-Act

RH – Recursos Humanos

SI – Sistema de Informação

SGSI - Sistema de Gestão de Segurança da Informação

SLA - service-level agreement

SPOC – Single point of Contact

SOD – Auditoria de acessos e segregação de função

UAM – User Access Management

TIC - Tecnologias de Informação e Comunicação

TSO – Technology Security Officer

Resumo

O âmbito do presente trabalho de projeto integra a caracterização da importância e da criticidade da segurança da informação e dos sistemas de informação através da análise da gestão de acessos dos utilizadores numa empresa de telecomunicações.

Cada vez mais a segurança da informação e dos sistemas de informação é um tema muito importante para as organizações, na medida em que condiciona o normal desenvolvimento das atividades bem como pode mesmo comprometer a sua sustentabilidade.

O estudo basear-se-á na análise de uma empresa de grandes dimensões no sector das telecomunicações, nomeadamente através da identificação do modelo adotado para a gestão de acessos e respetivo enquadramento face aos riscos existentes. A escolha desta organização deveu-se à especificidade da sua atividade, na medida em que se trata de uma empresa que contém diferentes tipos de utilizadores (internos, externos, genéricos, etc). Nesta diversidade de utilizadores, embora colocando-se diferentes desafios na gestão de acessos aos diferentes tipos de utilizadores, circunscreveremos a nossa análise apenas aos utilizadores internos e externos.

O seu principal objetivo consistiu, através do recurso a metodologias diferenciadas de acordo com as fases adotadas no estudo, na apresentação, a partir de uma análise prévia à situação existente, de uma proposta de novo modelo/metodologia para a gestão dos diferentes tipos de utilizadores, através de uma valorização crítica e reflexiva sobre a situação vivida atualmente. Para tal, adotar-se-ão diversas metodologias (*focus group*, com o envolvimento de diversos profissionais especialistas e com responsabilidade na área, entrevistas semiestruturadas e abertas, e inquéritos), de acordo com a especificidade de cada uma das fases desenvolvidas.

O projeto, aqui apresentado, estará dividido em 7 capítulos que serão explicados com maior detalhe na introdução do projeto.

Palavras chave: Segurança da Informação, Gestão de Utilizadores, Perfilagem

Abstract

The scope of this project work integrates the characterization of the importance and criticality of information security and information systems through the analysis of the access management of users in a telecommunications company.

Increasingly, information and information security is a very important issue for organizations, as it conditions the normal development of activities and may even jeopardize their sustainability.

The study will be based on the analysis of a large company in the telecommunications sector, namely through the identification of the model adopted for access management and the respective framework against the existing risks. The choice of this organization was due to the specificity of its activity, since it is a company that contains different types of users (internal, external, generic, etc.). In this diversity of users, although there are different challenges in managing access to different types of users, we will circumscribe our analysis only to internal and external users.

Its main objective consisted in the use of different methodologies according to the phases adopted in the study, based on a previous analysis of the existing situation, a proposal for a new model / methodology for the management of different types of users, through a critical and reflexive appreciation of the current situation. To this end, a number of methodologies (focus group, with the involvement of several specialist professionals with responsibility in the field, semi-structured and open interviews, and surveys) will be adopted, according to the specificity of each of the phases developed.

The project, presented here, will be divided in 7 chapters that will be explained in more detail in the introduction of the project.

Keywords: Information Security, User Management, Profiling

1. Introdução

A evolução das novas tecnologias, bem como a importância da segurança da informação, leva as organizações a aperfeiçoar continuamente os seus processos, serviços e sistemas. A adoção de uma abordagem sistémica e integrada na prevenção dos riscos, que assegure a segurança de toda a informação das organizações, num quadro de gestão que vá muito para além da simples aplicação de normas, regulamentos e procedimentos legais, pode ser a resposta adequada.

Sendo a informação um dos recursos mais importantes para as organizações, torna-se cada vez mais importante a implementação de um SGSI. Um SGSI consiste nas políticas, procedimentos, diretrizes, recursos e atividades associados, geridos coletivamente por uma organização, na procura da proteção dos seus recursos de informação. Um SGSI é uma abordagem sistemática para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação de uma organização para atingir os objetivos de negócios. Baseia-se numa avaliação de risco e na aceitação do risco da organização (ISO27000,2016).

Segundo a norma ISO27000 (2016), os princípios fundamentais que contribuem para uma implementação com sucesso de um SGSI são:

- Consciência da necessidade da segurança da informação,
- Atribuição da responsabilidade pela segurança da informação,
- Incorporação da gestão do compromisso e interesse dos *stakeholders*,
- Aumento dos valores sociais,
- Avaliações de risco de forma a determinar os controlos apropriados para alcançar níveis aceitáveis de risco,
- Segurança incorporada como um elemento essencial das redes e sistemas de informação;
- Prevenção e deteção ativa dos incidentes de segurança da informação,
- Garantir uma abordagem abrangente da gestão de sistemas de informação,
- Reavaliação continua da segurança da informação e realização de modificações conforme apropriado.

Ainda segundo a norma ISO27000(2016), todas as organizações partilham um conjunto de características comuns, nomeadamente:

- Recolhem, processam e transmitem informação;
- Reconhecem que essa informação, os processos, sistemas, redes e as pessoas são recursos importantes para atingir os seus objetivos;

- Enfrentam uma série de riscos que podem afetar o correto funcionamento dos seus recursos;
- Abordam a sua perceção de exposição ao risco através de implementação de controlos de segurança da informação.

Desta forma conseguimos verificar a importância que a informação tem dentro das organizações e consequentemente a importância em protegê-la.

Neste âmbito, na sequência destas características e dos princípios fundamentais para a segurança da informação dos SI, definiram-se os seguintes objetivos para este projeto:

- Analisar, caracterizar a situação atual no que se refere à gestão dos acessos numa grande organização do sector das telecomunicações,
- Elaborar uma proposta de modelo que minimize os problemas identificados, e
- Validar a proposta de solução através da análise dos potenciais benefícios que o modelo pode proporcionar.

A solução a propor visa a melhoria do desempenho dos utilizadores e da segurança no dia a dia da organização. Serão utilizadas as metodologias de *focus group*, com o envolvimento de diversos profissionais especialistas e com responsabilidade na área, entrevistas semiestruturadas e abertas, e inquéritos conforme descrito no capitulo 3.

O projeto encontra-se organizado em torno de duas partes, a primeira constitui a componente conceptual da dissertação e a segunda a sua componente empírica, apresentadas em 7 capítulos.

Os três primeiros capítulos que compõem a primeira parte do projeto têm carácter introdutório, da caracterização do estudo e da metodologia.

O primeiro capítulo – Introdução – apresenta os principais aspetos que motivaram a presente dissertação, a questão de investigação e a metodologia seguida.

No segundo capítulo – Enquadramento teórico – é caracterizado o enquadramento teórico pertinente para a compreensão do desenvolvimento desta dissertação.

O terceiro capítulo – Objetivo e Metodologia – descreve o método e as técnicas de abordagem do estudo de caso. É apresentada a metodologia escolhida e as fases da mesma assim como os instrumentos e procedimentos para a recolha e tratamento dos dados. São também apresentadas algumas conclusões parciais.

No quarto capitulo inicia-se a segunda parte, dedicada ao estudo empírico – Avaliação da situação atual – neste capitulo é apresentada a realidade ao dia de hoje da empresa em estudo.

No quinto capítulo – Elaboração e validação do modelo proposto – é apresentada, face aos resultados obtidos, uma proposta de solução para a empresa do caso de estudo.

No sexto capitulo – Conclusões finais – são apresentadas as conclusões finais do estudo de caso.

No sétimo capitulo – Limitações e trabalho futuro – são apresentadas as limitações encontradas e propostas de trabalho futuro.

2. Enquadramento

2.1. Conceitos Nucleares

Cada vez mais as organizações dependem da informação como elemento essencial para a gestão, para a geração do conhecimento, para a tomada de decisões, desenvolvimento de novos produtos, vantagem tecnológica o que representa efetivamente valor para o negócio.

As empresas enfrentam incertezas constantes e a imprevisibilidade sobre o futuro, procurando novas informações sobre o seu meio ambiente, para adotar decisões, o que lhes permite crescer e ser competitivo. O gestor precisa constantemente de adotar estratégias e tomar decisões com base em informações confiáveis e úteis sobre o ambiente organizacional, o que reduz o risco, inevitavelmente, associado a qualquer decisão, e é isso lhe permite responder rápida e eficazmente aos desafios que surgem, garantindo a adequação dos níveis de competitividade e sobrevivência da organização (Garcia, 2015).

Para conseguir gerir de forma correta a informação, os gestores devem preocupar-se acima de tudo com a gestão do conhecimento. Segundo Knapp (1998), a gestão do conhecimento é a arte de transformar a informação e os ativos intelectuais em valores, apoiando os clientes e colaboradores de uma organização. O valor agregado de uma organização vem da partilha de conhecimento entre os seus colaboradores. A gestão do conhecimento permite a criação de fluxos de informação entre os vários níveis organizacionais, a fim de aumentar, desenvolver e divulgar o conhecimento dentro da organização (Serrano, 2005).

O conhecimento e as habilidades presentes no capital humano, a eficiência e eficácia das estruturas e dinâmicas organizacionais, bem como o valor extraído das sinergias estabelecidas na economia relacional são dimensões que necessariamente devem estar relacionadas. Nesta área, os fatores que melhoram o desempenho organizacional, influenciando a competitividade são: alianças estratégicas, capital humano, confiabilidade, conhecimento, custo, fatores culturais, flexibilidade, inovação, qualidade, velocidade, relacionamento com clientes, responsabilidade social, sistemas de controlo e TIC (Vala, 2013)

A informação é um conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenómeno ou evento. A informação permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional é a base do conhecimento.

Beal (2004), define a informação como um resultado da transformação ocorrida quando os registos ou factos que caracterizam os dados são organizados ou combinados de forma lógica e

significativa. Para Padoveze (2000), informação é um dado que foi processado e armazenado de forma compreensível para o seu recetor e que apresenta valor real para as suas decisões correntes ou prospetivas.

Ralph (2002) conceitua SI como um conjunto de elementos ou componentes inter-relacionados, que coletam (entrada), manipulam (processamento) e disseminam (saída) os dados e a informação e fornecem um mecanismo de feedback para atender a um objetivo.

Um SI bem estruturado é indispensável para a utilização da informação com oportunidade, isto é, para a tomada de decisões que ofereça competitividade. Essa competitividade é alcançada pela inteligência competitiva, processo pelo qual as informações de múltiplas fontes são coletadas, interpretadas e comunicadas a quem precisa delas para decidir (Cardoso,2005). Observe-se que um é meio para a outra, pois, para se obter a inteligência competitiva, faz-se necessário possuir um excelente SI.

Mesmo reconhecendo essas diferenças, para a segurança da informação, todas essas segregações serão incluídas num único contexto: o da informação. Dados, informação, conhecimento ou inteligência, para a segurança da informação, tudo deve ser visto como informação.

Podemos concluir que a informação é um conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenómeno ou evento. A informação permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional é a base do conhecimento, desta forma, as empresas devem preocupar-se cada vez mais com a sua segurança

2.2. Segurança da Informação

A Segurança da Informação refere-se à proteção existente sobre a totalidade da informação de uma determinada organização ou pessoa. A segurança de determinada informação pode ser afetada por fatores comportamentais pelo uso de quem a utiliza, pelo ambiente ou infraestrutura que a suporta, ou ainda por indivíduos mal-intencionados, que têm o objetivo de destruir ou modificar essa informação.

A segurança da informação é um tema importante para qualquer organização (Sêmola,2003), uma vez que vivemos num era cada vez mais tecnológica em que a informação é um dos dados mais importantes para o dia a dia de qualquer organização.

Desta forma as organizações tiveram de desenvolver mecanismos de segurança, para conseguir proteger as informações das organizações concorrentes e de forma a preservar os dados dos seus clientes.

Para Tavares, et al (2003), face à grande dispersão do acesso aos dados, sistemas e código, aliada à elevada conectividade que o futuro parece ter reservada para nós, teremos de aceitar a visão e controlo limitados que temos sobre a parte da "imagem global" sob a nossa alçada. A este fator juntam-se as necessidades de proteção da informação dos SI, não só das tecnologias de suporte aos objetivos da organização, num contexto hostil em que é cada vez mais difícil isolar perímetros ou áreas em que se possa confiar.

Este autor, para satisfação das necessidades supracitadas, surgiu um novo modelo, designado "Modelo de Sobrevivência da Informação", que integra o conceito da sobrevivência com o da gestão do risco pelo negócio, obrigando à utilização de estratégias de gestão do risco baseadas num conhecimento íntimo da missão a proteger.
Este modelo tem como princípios, o envolvimento, a exposição, a emergência, a diversidade e o contexto.

O primeiro destes princípios, o envolvimento, torna a segurança num problema de toda a organização, pelo que a viabilização de algumas soluções só pode ser avaliada no contexto do negócio, permitindo transcender soluções puramente técnicas (por exemplo,
recorrendo a advogados para introduzir cláusulas de [des]responsabilização nos contratos).

A exposição nega a qualquer componente imunidade a ataques, acidentes ou falhas, ou seja, segundo este princípio não existem santuários.

O terceiro princípio afirma que as propriedades globais de sobrevivência surgem (emergem) da combinação de componentes que isoladamente não são sobreviventes.

A diversidade, de há longa data a melhor amiga da segurança, introduz o bom senso de "não colocar os ovos todos no mesmo cesto".

Por fim, o contexto refere que as soluções técnicas deverão ser baseadas no verdadeiro ambiente em que os sistemas operam e não nas funcionalidades disponíveis no sistema, ou na forma correta de os usar. É um assentar dos pés na terra para os informáticos.

A implementação deste modelo assenta na análise da capacidade de sobrevivência dos sistemas e na posterior identificação de estratégias de mitigação de riscos, através da promoção

das capacidades de resistência, reconhecimento e recuperação de falhas, aumentando a segurança dos sistemas de informação.

Identificado o modelo considerado adequado para a segurança da Empresa, será agora necessário analisar um outro modelo, o de maturidade, que permite identificar o caminho a percorrer (Tavares, et al 2003).

O Programa de Segurança de uma empresa passa por vários estádios de desenvolvimento, cuja ultrapassagem representa amadurecimento, o chamado modelo de maturidade. Esses graus de maturidade correspondem à:

1) definição de políticas e normas de segurança;
2) definição da arquitetura e dos processos da segurança;
3) implementação dos processos de suporte à inspeção, proteção, deteção e reação;
4) realização de ações de sensibilização e de formação em segurança;
5) realização periódica de auditorias e testes à segurança;
6) implementação de processos de resposta reflexa;
7) validação do modelo de proteção e da sua implementação.

Para que a maturidade de segurança esteja num determinado grau, segundo este modelo, é necessário que a Empresa complete o grau em causa e todos os graus anteriores a esse. Por exemplo, para atingir o grau 3 (implementação dos processos de suporte à inspeção, proteção, deteção e reação) no modelo de maturidade, será necessário primeiro cumprir razoavelmente os requisitos dos graus 1 (definição de políticas e normas de segurança) e 2 (definição da arquitetura e dos processos da segurança). Apesar da subjetividade associada à implementação de cada grau, este modelo será a medida mais realista disponível para determinar a maturidade do Programa de Segurança. (Tavares, et al 2003). Como podemos proteger a informação?

- Atribuição de Passwords, pois desta forma será mais fácil controlar os acessos a determinada informação.
- Encriptação dos dados, por exemplo mascarando alguns dos dados de forma a manter a sua confidencialidade.
- Implementação de leis e procedimentos, por exemplo com a aplicação de normas e regulamentos (por exemplo; ISO 27001, GDPR, entre outros).
- Formação, na medida em que através de formação adequada aos utilizadores estes vão conseguir utilizar a informação disponibilizada de forma mais adequada.

Para reforçar esta importância da Segurança da informação foram criadas algumas normas internacionais como podemos verificar na figura 1, que devem ser seguidas pelas organizações. Segundo a norma ISO/IEC 27001 (2013), de forma a protegerem a sua informação, as organizações devem planear, implementar e controlar os processos necessários para dar resposta aos requisitos

da segurança da informação e implementar as ações necessárias. A organização deve também implementar planos de forma a atingir os objetivos da segurança da informação.

Figura 1 - Normas fundamentais para a implementação de um SGSI (Caldwell,2014)

Para o âmbito deste projeto vamos focar-nos na norma ISO 27001. A norma 27001 foi criada pela ISO (*Internacional Organization for Standardization*). Esta Norma Internacional especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI no contexto da organização. Esta Norma Internacional também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação adaptados às necessidades da organização. Os requisitos estabelecidos neste padrão internacional são genéricos e destinam-se a ser aplicáveis a todas as organizações, independentemente de tipo, tamanho ou natureza. Excluir qualquer dos requisitos especificados nas Cláusulas 4[1] a 10 não é aceitável quando uma organização reivindica conformidade com este padrão internacional.

[1] Contexto da organização, Liderança, Planeamento, Suporte, Operação, Avaliação de desempenho e Melhorias.

O SGSI preserva a confidencialidade, integridade e disponibilidade de informações, aplicando um processo de gestão de riscos e dando confiança às partes interessadas que os riscos são adequadamente geridos. (ISO/IEC FDIS 27001:2013(E)).

A adoção desta norma serve para que as organizações optem por um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um sistema de gestão de segurança da informação (Integrity,SD).

Na figura dois podemos verificar que a estrutura da norma 27001 apresenta 2 tipos de clausulas e um anexo. A azul, constam as clausulas com os requisitos correspondentes ao ciclo de melhoria. A verde, constam as cláusulas com os requisitos gerais do SGSI e a castanho, o anexo com os objetivos de controlo & controlos.

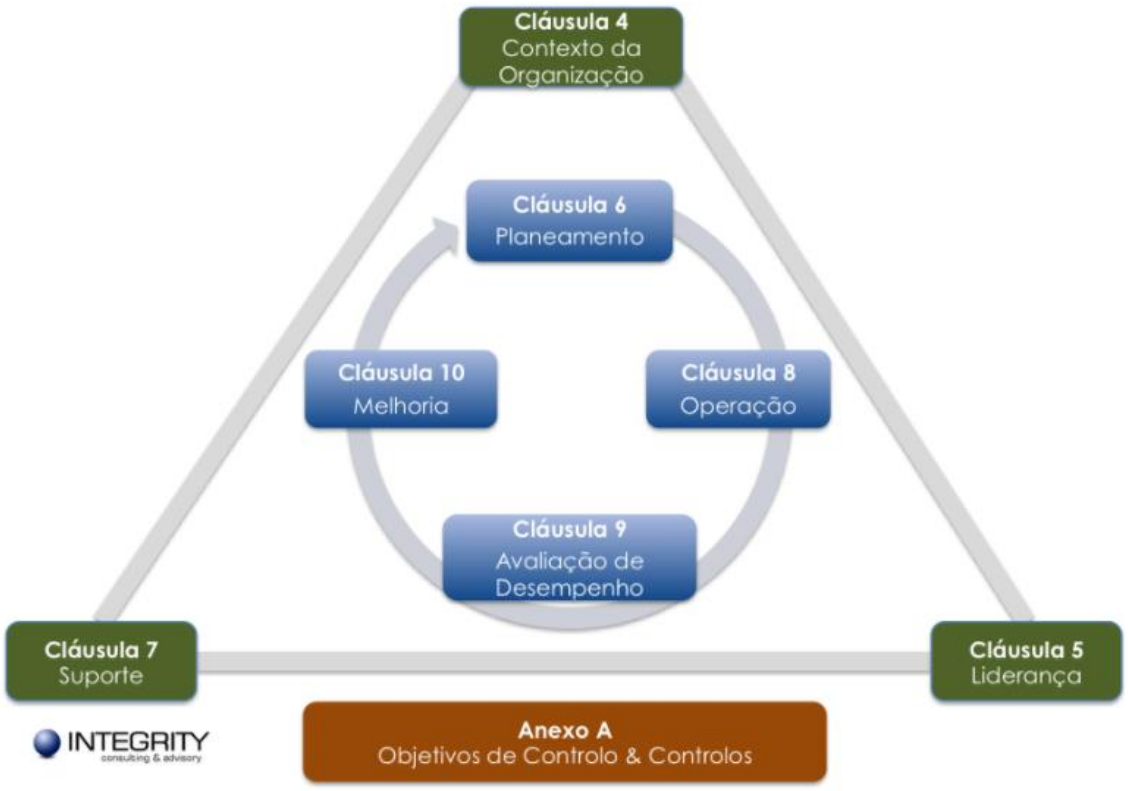


Figura 2 - Estrutura global da norma 27001(Integrity,SD).

A estrutura da norma 27001:2013 apresenta um suporte base constituído pela cláusula 4 (contexto da organização), cláusula 5 (Liderança) e a cláusula 7 (suporte), servindo estas de enquadramento a um ciclo controlado pelas clausulas 6 (planeamento), 8 (operação), 9

(avaliação de desempenho) e 10 (melhoria), na figura 3 podemos verificar o resumo das clausulas desta norma.

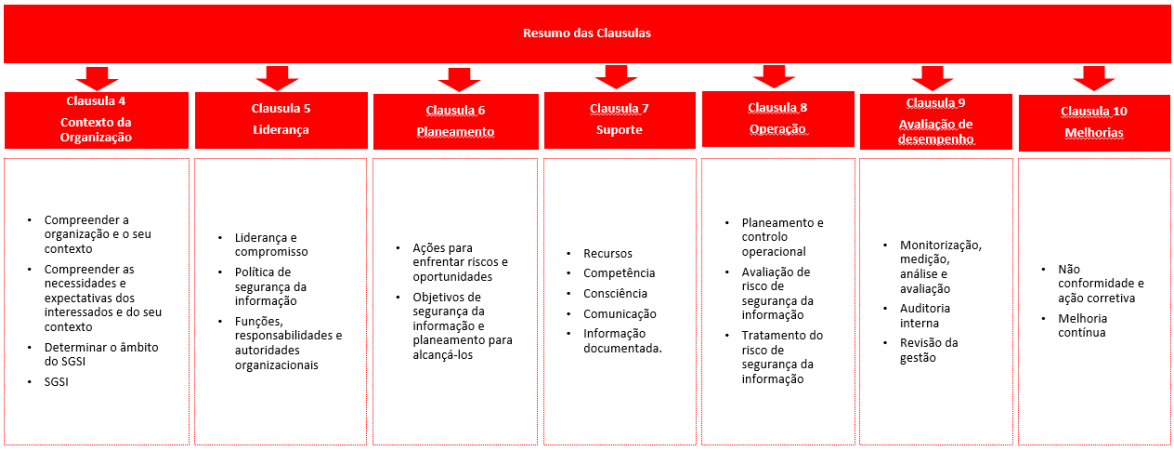


Figura 3 - Resumo das clausulas ISO 27001:2013 (Elaboração própria)

Segundo a norma 27000 (2016) a segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação. Além destas três propriedades, existem mais propriedades a ter em conta em relação á segurança da informação:

- Confidencialidade - a informação que não é disponibilizada ou divulgada a pessoas, entidades ou processos (exemplo: envio de documentação confidencial a pessoas não autorizadas, passagem de informações confidenciais de forma verbal em sítios públicos entre outros);
- Integridade - propriedade de exatidão e plenitude (exemplo: falsificação de documentos, alteração de dados da base de dados, entre outros);
- Disponibilidade – informação estar acessível e utilizável mediante requisição por uma entidade autorizada (exemplo: perdas de documentos, perda de acesso à informação, entre outros);
- Autenticidade - uma entidade é o que afirma ser;
- Responsabilização pela informação;
- Não repúdio - capacidade de provar a ocorrência de um evento reivindicado ou ação e as suas entidades de origem;
- Confiabilidade - propriedade de comportamento e resultados esperados consistentes.

Neste sentido, a segurança da informação não se trata apenas de confidencialidade, mas também de preservar a integridade e a disponibilidade dos dados, como podemos verificar na figura 4.

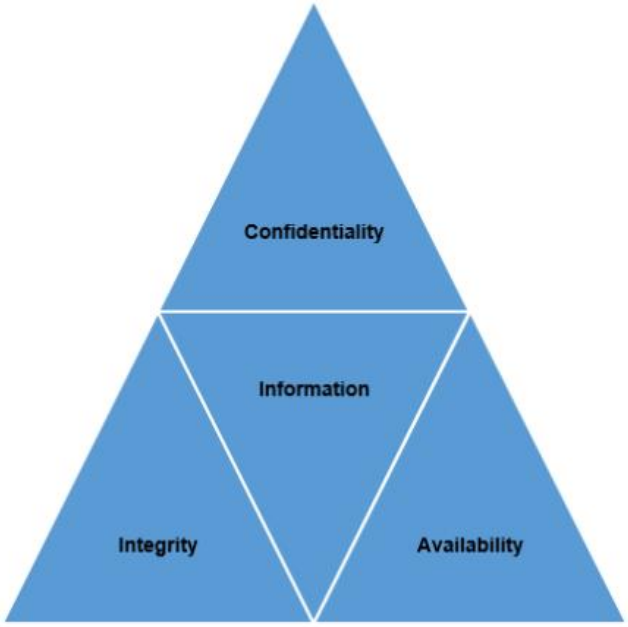


Figura 4 - Tríade dos princípios da segurança da informação (Silva, 2017)

Mas falar de segurança da informação segundo a norma 27000 (2016), pressupõe considerar outros conceitos associados à informação, nomeadamente:

- **Vulnerabilidades –** é a fraqueza de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças (podemos encontrar alguns exemplos na figura 5);

- **Ameaças –** é a causa potencial de um incidente indesejado, o que pode resultar em danos num sistema ou organização. São de origem natural ou humana e podem ser acidentais ou intencionais. Convém que tanto as fontes das ameaças acidentais como as intencionais, sejam identificadas.

- **Impacto –** resultado da concretização de uma ameaça contra a vulnerabilidade de um ativo. Pode ter um efeito imediato direto ou indireto (operacional) ou uma consequência futura.

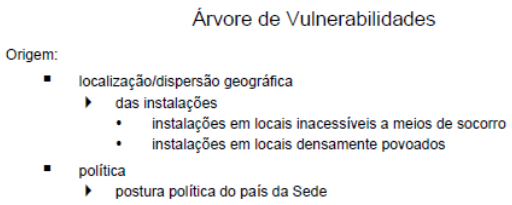


Figura 5 - Árvore de Vulnerabilidades (Silva,et al.,2003)

A junção de uma vulnerabilidade com uma ameaça vai resultar num incidente.

Um incidente de segurança da informação é uma ocorrência de um evento que possa interromper os processos do negócio de um ou mais dos três princípios básicos da segurança da informação (confidencialidade, integridade e disponibilidade)

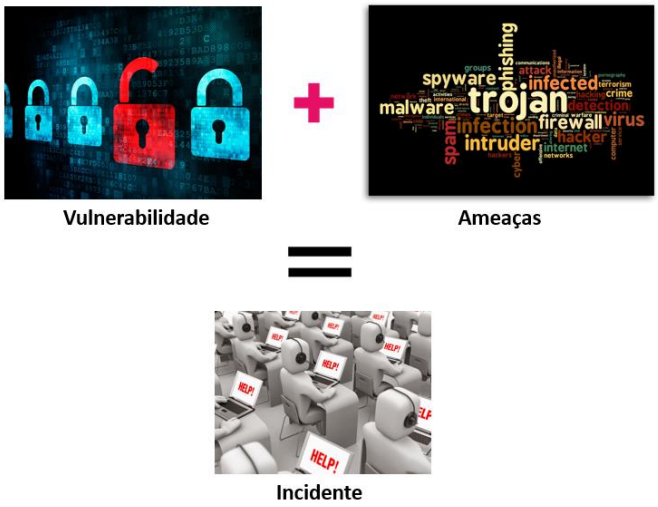


Figura 6 - Incidente (Elaboração Própria)

Portanto a segurança da informação de uma empresa não pode estar apenas ligada a produtos para a segurança como a *firewall*, *software* de encriptação de dados, entre outros:

- *Firewall*, segundo a CISCO (SD), uma *firewall* é um dispositivo de segurança de rede que monitoriza o trafego da rede que entra e a de saída e decide se permite ou bloqueia o tráfego com base num conjunto de regras de segurança previamente definidas.
- *Software* de encriptação de dados, podemos entender por encriptação como sendo um meio utilizado para garantir a segurança das comunicações de modo a que, mesmo que intercetadas, o conteúdo da mensagem não seja conhecido por terceiros (Piropo,2014).

As organizações, podem apostar em produtos de segurança, mas a sua abrangência deverá ir muito além disso, deverá abranger diversas áreas como a Análise de Riscos, Gestão de riscos, Politicas de segurança, Mecanismos de segurança, Auditorias de Sistemas e Controlo de acessos físicos e lógicos, onde será baseado o nosso estudo.

Em suma, podemos verificar que com o reconhecimento da informação como um ativo de uma organização, existe cada vez mais a necessidade de assegurar a sua segurança.

2.3. Gestão de riscos

Num cenário de incertezas, as ameaças e oportunidades têm o potencial de produzir perdas ou aumentar os ganhos. Os resultados positivos são alcançados com uma boa gestão das incertezas e dos seus riscos, gerando valor ao otimizar as suas oportunidades, e ao estabelecerem estratégias para os objetivos de crescimento, na busca da maximização dos seus resultados. Os resultados negativos são oriundos da ausência e/ou da fragilidade dessa gestão, em que os seus resultados podem produzir danos e perdas de grandes proporções (Dantas, 2011).

Segundo Dantas (2011), o risco é compreendido como algo que crie oportunidades ou produz perdas. Em relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de dados e perdas. É medido pela possibilidade de um evento via a acontecer e produzir perdas.

Segundo a 27005 (2011), o risco é um efeito da incerteza sobre os objetivos. Um efeito é um desvio do esperado - positivo e / ou negativo.

Os objetivos podem ter aspetos diferentes (como financeiro, saúde e segurança, segurança da informação e metas ambientais) e podem aplicar a diferentes níveis (como estratégia, organização, projeto, produto e processo).

O risco é frequentemente caracterizado por referência a eventos potenciais e consequências, ou a uma combinação destes.

O risco de segurança da informação é frequentemente expresso em termos de uma combinação das consequências de uma informação, um evento de segurança e a probabilidade associada de ocorrência.

A incerteza é o estado, mesmo parcial, da deficiência de informação relacionada, compreensão ou conhecimento de um evento, consequência ou probabilidade.

O risco de segurança da informação está associado à probabilidade de que as ameaças podem explorar as vulnerabilidades de uma informação ou grupo de ativos de informações e, desta forma causar danos a uma organização.

Podemos entender o risco de TIC como o potencial risco de exposição à perda para a organização de uma falha em qualquer aspeto do ambiente de TIC, podendo dar origem a interrupção de negócios, relacionamentos, tecnologia e governança (Edmiston, 2007). Quando consideramos a partilha de informações entre os parceiros da cadeia de valor e a informação como um ativo económico para vencer a concorrência no mercado, qualquer quebra ou violação de segurança no sistema de informação seria fundamental para toda a rede (Faisal, Banwet & Shankar, 2007). Assim, a governança da informação deve corresponder a um compromisso estratégico entre a área de TIC e todas as organizações, no sentido de promover uma melhor gestão e controlo de informações e TIC.

Cada uma das áreas de risco acima contém vários domínios de risco de TIC relacionados, que podem estar relacionados a alguns ou a todos os outros (Rasmussen, 2006):

- Interrupção do negócio - Os riscos de interrupção de negócios ocorrem como resultado de eventos externos, incidentes de segurança, problemas de informação e riscos on-line. Os domínios de risco de TIC englobam:
    - Continuidade do negócio - A continuidade do negócio refere-se à capacidade de uma empresa sobreviver a uma variedade de eventos e continuar a operação lucrativa. Tais eventos variam entre perdas financeiras causadas por uma variedade de razões até desastres naturais e os eventos causados pelo homem;
    - Segurança das TIC - A segurança das TIC refere-se à capacidade da organização de se proteger contra-ataques maliciosos, tanto de fontes externas como internas. Os ataques incluem vírus e a negação de incidentes de serviço, por exemplo;
    - Online - Os riscos online provêm do fato de que muitas organizações têm uma presença na Internet. Na verdade, para algumas organizações, elas não existiriam, exceto pela presença na Internet. Os riscos decorrem da necessidade de expor determinados sistemas da organização, ao mesmo tempo que protegem os outros sistemas do acesso não autorizado;
    - Informação - Os riscos de informação surgem quando há acesso não autorizado a informações mantidas em qualquer um dos sistemas de uma organização.
- Relacional - Os riscos relacionais ocorrem entre a função das TIC e fornecedores, terceiros e outras partes da organização e englobam:
    - Gestão de fornecedores - Existem vários riscos de gestão de fornecedores, incluindo seleção, requisitos e estabilidade;
    - Relacionamento de terceiros - relacionamentos de terceiros referem-se ao fato de que tantas empresas praticam *outsourcing* para funções anteriormente fornecidas internamente, bem como relacionamentos com parceiros e fornecedores;
    - Satisfação do cliente das TIC - Quando uma função de TIC não atende aos requisitos do cliente, a sua reputação sofre; este é um exemplo desse risco particular. Os requisitos do cliente incluem SLAs, solicitações de suporte e sistemas para suportar o negócio.
- Tecnologia - Os riscos tecnológicos referem-se a temas como agilidade de TIC, arquitetura de TIC, mudança de execução e desenvolvimento de projetos e consideram:
    - Agilidade das TIC - As TIC devem ser sensíveis às necessidades da organização;

    - Arquitetura das TIC - As TIC devem ser padrões para a organização ter uma arquitetura flexível;
    - Alteração da execução - Os processos de gestão de mudanças devem ser aplicados;
    - Desenvolvimento do projeto - A organização deverá estar envolvida no ciclo de vida do desenvolvimento do projeto.
- Governança das TIC – os riscos de governança das TIC estão nas áreas de estratégia das TIC, recursos das TIC, conformidade e questões legais. A governança das TIC é importante, pois é usada para mitigar muitos dos riscos mencionados anteriormente.
    - Risco estratégico das TIC - o principal risco estratégico das TIC resulta da falta de alinhamento entre as TIC e a organização. Os riscos adicionais decorrem de uma conformidade inconsistente com padrões de governança e perda de controlo.
    - Risco de recursos das TIC - para entregar sistemas com sucesso à organização, as TIC precisam das pessoas certas, com as habilidades corretas e no momento certo. Uma falha em qualquer destes requisitos põe em perigo a entrega dos sistemas.
    - Conformidade / risco legal - Qualquer organização deve cumprir uma variedade de obrigações legais e regulamentares. O não cumprimento dessas obrigações expõe a organização a uma série de riscos.

Esta suposição de todas estas dimensões de risco requer uma abordagem de gestão de melhoria contínua para aumentar a capacidade de resposta no ambiente das TIC, nomeadamente nos seguintes aspetos:

- Compreensão e responsabilidade da gestão das TIC (identificação de custos de TIC, especificação de processos de TIC, design de portfólio de projetos de TIC e serviços de TIC, suporte de TIC na tomada de decisões, etc.);
- Avaliação do retorno do investimento (cálculo de investimento de TIC, avaliação de risco de TIC, retorno de investimento de TIC, etc.);
- Suposição do valor das TIC e posicionamento de parcerias (área das TIC como parceiro de negócios, *joint ventures* com outras organizações, relações com os principais parceiros tecnológicos, participação na estratégia de negócios, promoção da flexibilidade organizacional para gestão de mudanças, etc.);
- Melhorar o desempenho das TIC (identificação de projetos críticos ou serviços de TIC para negócios, avaliação de desempenho associado, foco na melhoria contínua, estimulação de práticas de *benchmark*, etc.);
- Conformidade externa (facilitação de requisitos legais e regulamentares).

Assim, para a governança, os gestores das TIC devem considerar:

- Uma implementação de um modelo - um modelo que integre, encoraje e forneça uma metodologia para o alinhamento de negócios e TIC; que facilite o controlo de toda a organização; que evidencie orientações / políticas; e consolide uma visão de TIC partilhada por toda a organização.
- Um compromisso de gestão - essencialmente no nível da administração, que facilite uma definição clara de responsabilidades e deveres de negócios e garantia de TIC.
- Um consenso global - essencialmente entre as funções de Governança de TIC e controlo, que facilite a integração da Governança de TIC com outras práticas de gestão que fortaleça a consciencialização, motivação e métodos de comunicação para a adoção do modelo e *frameworks*; que assegure o equilíbrio entre políticas e práticas e minimize a burocracia.
- Uma sensação de confiança sobre a função de TIC - que vise a consolidação das relações de confiança estabelecidas entre todas as áreas organizacionais.
- Uma monotorização de metas – que incremente a definição de *scorecards* de TIC e métricas.
- Foco nos custos - através da identificação de oportunidades para reduzir custos.

Os gestores devem entender a gestão de riscos como um processo organizacional realizado pelo conselho de administração, diretores e todos os colaboradores (Committee Draft for Vote, 2008).

De forma a fornecer diretrizes para uma correta gestão dos riscos de segurança da informação foram criadas as normas internacionais ISO 27005 e a ISO 31000. Este Padrão Internacional suporta os conceitos gerais especificados na ISO / IEC 27001 e foi criado para ajudar a implementação satisfatória de segurança da informação com base numa abordagem de gestão de riscos.

Este Padrão Internacional é aplicável a todos os tipos de organizações (por exemplo, empresas comerciais, organizações sem fins lucrativos, entre outras) que pretendem gerir riscos que possam comprometer a segurança da informação da organização (ISO/IEC 27005:2011).

Esta norma contem a descrição do processo de gestão dos riscos da segurança da informação e as suas atividades, na figura 7 podemos verificar um resumo da estrutura desta norma.

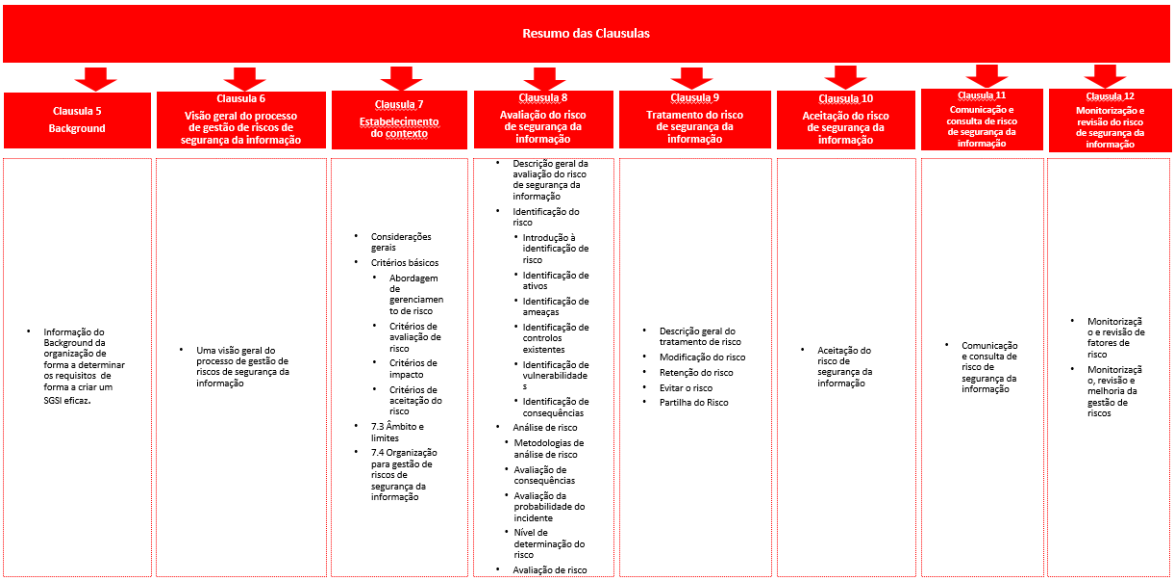


Figura 7 - Resumo das Clausulas ISO 27005 (Elaboração própria)

Segundo Dantas (2011) existem três tipos de riscos:

- Riscos naturais - Para os riscos naturais, dependendo do potencial do evento, pode parecer difícil existir uma proteção eficaz, mas, sabendo-se que tais eventos são comuns em determinada região, torna-se mais fácil adotar ações planeadas para prevenir os impactos, minimizar os danos quando aconteçam e poder retornar à normalidade das atividades.
- Riscos involuntários - Para os riscos involuntários, a identificação da sua origem tem relação direta com as vulnerabilidades humanas, físicas, de *hardware*, de *software*, com os meios de armazenamento e as comunicações, e que geralmente ocorrem por falha na condução do sistema de gestão da segurança da informação.
- Riscos intencionais - Ocorrem pela exploração intencional de um agente (interno ou externo) ao perceber alguma falha no sistema de proteção da organização, ou ao executar ataques diretos ou aleatórios, com o objetivo de detetar alguma vulnerabilidade nesse sistema.

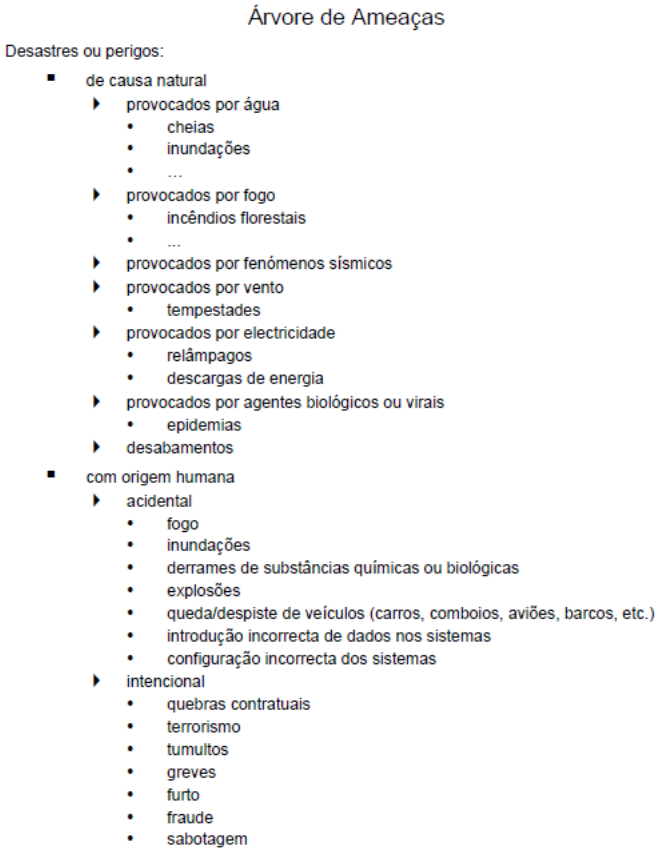


Figura 8 - Árvore de ameaças (Silva, et al (2003))

Segundo a norma 27005 (2011) as etapas do processo de gestão do risco são:

- É efetuado o estabelecimento do contexto;
- Executa-se o processo de avaliação de riscos de forma cíclica, sempre revendo o contexto, até que ele forneça informações suficientes para reduzir os riscos a um nível aceitável;
- Inicia-se o tratamento de riscos até um nível de risco residual que seja aceitável pelos gestores da organização;
- Efetua-se a comunicação ás áreas operacionais e aos gestores dos riscos que foram tratados e;
- Por último, de forma contínua, é efetuado a monitorização e análise crítica de riscos para verificar a eficácia do tratamento dos riscos ou se há necessidade de uma nova iteração do processo de gestão de risco da segurança da informação de acordo com novas circunstâncias do negócio.

Convém que os resultados detalhados de cada atividade do processo de gestão de risco da segurança da informação, assim como as decisões sobre o processo de avaliação de riscos e sobre o tratamento do risco, sejam documentados e é importante salientar que a aplicação da gestão de risco da segurança da informação deva satisfazer os requisitos do SGSI, caso existir.

Na figura 9 podemos consultar o processo da gestão de risco segundo a norma 27005 (2011).

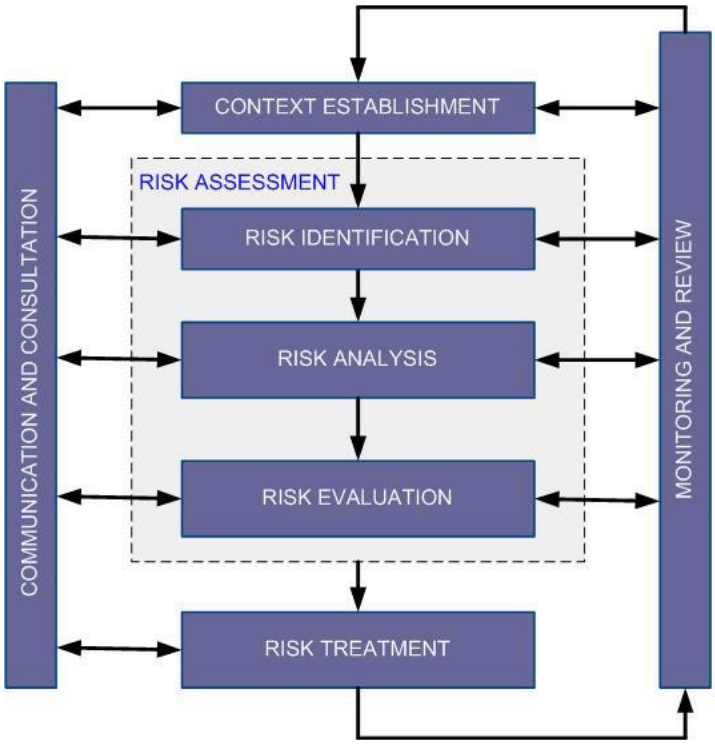


Figura 9 - Processo de Gestão de Risco 27005 (2011)

A figura 10 mostra como a 27005 (2011) aplica o processo de gestão de risco.

O processo de gestão de risco de segurança da informação consiste no estabelecimento do contexto (Cláusula 7), Avaliação do risco de segurança da informação (Cláusula 8), Tratamento do risco de segurança da informação (Cláusula 9), Aceitação do risco de segurança da informação (Cláusula 10), Comunicação e consulta de risco de segurança da informação (Cláusula 11) e Monitorização e revisão do risco de segurança da informação (Cláusula 12).

Como mostra a figura 10, o processo de gestão de risco de segurança da informação pode ser iterativo para avaliação de risco e / ou atividades de tratamento de risco. Uma abordagem iterativa para a avaliação do risco pode aumentar a profundidade e detalhe da avaliação em cada iteração. A abordagem iterativa proporciona um bom equilíbrio entre minimizar o tempo e esforço gasto na identificação de controlos, garantindo ainda que os riscos elevados sejam apropriadamente avaliados.

O contexto é estabelecido primeiro. Em seguida, é efetuada uma avaliação de risco. Se isso fornecer informações suficientes para efetivamente determinar as ações necessárias para modificar os riscos para um nível aceitável, então a tarefa está completa e o tratamento de risco segue. Se a informação for insuficiente, outra iteração do risco, com o contexto revisto (por exemplo, critérios de avaliação de risco, critérios de aceitação de risco ou critérios de impacto) será efetuada,

possivelmente em partes limitadas do âmbito total (ver figura 10, Ponto de Decisão de Risco 1). A eficácia do tratamento de risco depende dos resultados da avaliação de risco.

O tratamento de risco envolve um processo cíclico de:

- Avaliar um tratamento de risco;
- Decidir se os níveis de risco residual são aceitáveis;
- Gerar um novo tratamento de risco se os níveis de risco não forem aceitáveis; e
- Avaliar a eficácia desse tratamento

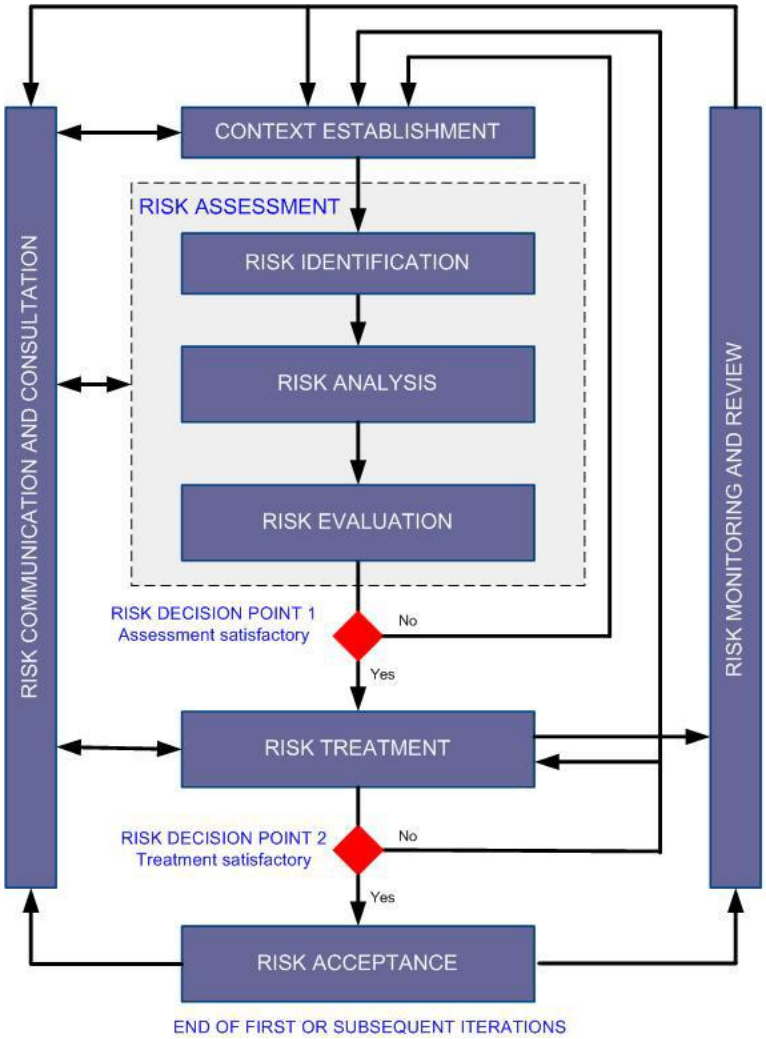


Figura 10 - Aplicação da gestão de riscos , 27005 (2011)

A Figura 11 ilustra a atividade de tratamento de risco dentro do processo de gestão de risco de segurança da informação como apresentado na Figura 10.

As opções de tratamento de risco devem ser selecionadas com base no resultado da avaliação de risco, o custo esperado para implementar essas opções e os benefícios esperados dessas opções.

Quando grandes reduções nos riscos podem ser obtidas com despesas relativamente baixas, tais opções devem ser implementadas. Outras opções de melhorias podem não ser econômicas e devem ser avaliadas em relação ao custo-benefício.

As quatro opções de tratamento de risco não são mutuamente exclusivas. Às vezes, a organização pode beneficiar substancialmente de uma combinação de opções, como reduzir a probabilidade de riscos, reduzindo as suas consequências e partilha ou retenção de riscos residuais.

Identificação do risco – processo de pesquisa, reconhecimento e descrição dos riscos. A identificação do risco envolve a identificação de fontes de risco, eventos, as suas causas e as suas potenciais consequências. A identificação de risco pode envolver dados históricos, análises teóricas, opiniões informadas e especialistas, e necessidades das partes interessadas.

Análise do risco – processo para compreender a natureza do risco e determinar o nível de risco. A análise de risco fornece a base para avaliação de risco e decisões sobre o tratamento de risco. A análise de risco inclui a estimativa do risco.

Avaliação do risco - processo de comparação dos resultados da análise de risco com os critérios de risco para determinar se o risco e / ou sua magnitude é aceitável ou tolerável. A avaliação do risco auxilia na decisão sobre o tratamento de risco.

Tratamento do risco - processo para modificar o risco. O tratamento de risco pode envolver:

– evitar o risco, decidindo não iniciar ou continuar com a atividade que dá origem ao risco;

– assumir ou aumentar o risco para prosseguir uma oportunidade;

– remoção da fonte de risco;

– mudar a probabilidade;

– mudar as consequências;

– partilhar o risco com outra parte ou partes (incluindo contratos e financiamento de risco); e

– manter o risco por escolha informada.

Os tratamentos de risco que lidam com consequências negativas às vezes são chamados de "mitigação de risco", "eliminação de risco "," prevenção de riscos "e" redução de risco ".

O tratamento de risco pode criar novos riscos ou modificar os riscos existentes.

Alguns tratamentos de risco podem efetivamente abordar mais do que um risco (por exemplo, formação em segurança da informação e consciência). Deve ser definido um plano de tratamento de riscos que identifique claramente a ordem de prioridade em que os tratamentos de risco

individuais devem ser implementados e os seus prazos. As prioridades podem ser estabelecidas utilizando várias técnicas, incluindo a classificação do risco e análise custo-benefício. É da responsabilidade dos gestores decidir o equilíbrio entre os custos de implementação dos controlos e a atribuição do orçamento.

A identificação dos controlos existentes pode determinar que estes excedem as necessidades atuais, em termos de comparações de custos, incluindo manutenção. Se a remoção dos controlos redundantes ou desnecessários for considerada (especialmente se os controlos tiverem altos custos de manutenção), segurança da informação e fatores de custo devem ser tomados em conta.

As opções de tratamento de risco devem ser consideradas tendo em consideração:

- Como risco é entendido pelas partes afetadas
- A maneira mais adequada de se comunicar com essas partes

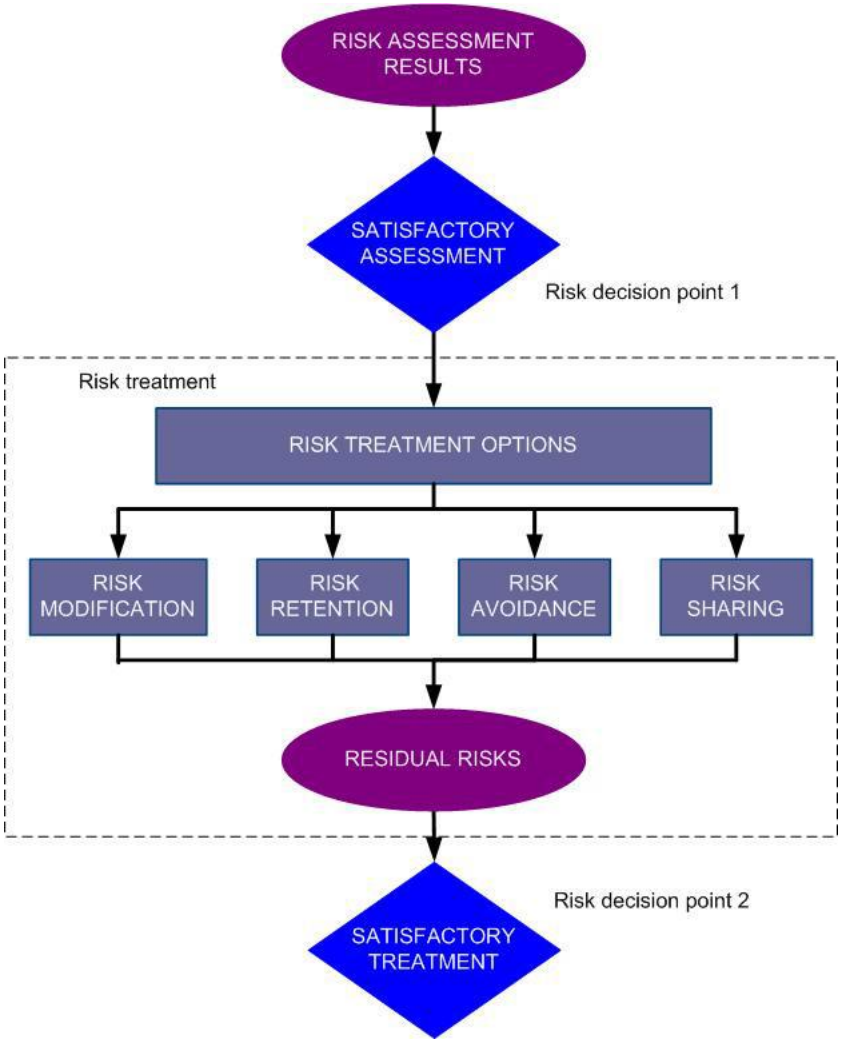


Figura 11 - Tratamento de um risco 27005(2011)

No âmbito do nosso projeto, fizemos um levantamento dos riscos junto da equipa de Compliance que apresentaremos no capitulo 3.

Cada vez é mais importante as organizações estarem cientes dos riscos que têm no seu dia a dia para que os possam tentar mitigar através da implementação de processos de melhoria.

2.4. Auditoria de acessos e segregação de funções (SOD)

2.4.1. Tipos de Auditoria

As auditorias são muito importantes para todas as organizações de forma a poderem desta forma avaliar as suas atividades e operações. Podemos entender por auditoria como sendo um processo sistemático que consiste no exame ou verificação objetiva das atividades e operações de uma organização. O objetivo desse exame é analisar a conformidade dessas atividades e operações em relação a determinadas regras e normas e aos objetivos definidos para essa organização. Deve ser realizada por uma pessoa idónea e tecnicamente preparada. A sua realização obedece a um conjunto de princípios, métodos e técnicas geralmente aceites, as quais permitem ao auditor formar uma opinião fundamentada e emitir um parecer acerca da matéria analisada. A auditoria permite identificar quaisquer tipos de desvios que possam vir a requerer uma ação corretiva e as suas conclusões e recomendações devem ser comunicadas a todos os detentores de interesse. (Gaai/Ipad,2009)

Existem vários tipos de auditorias, como por exemplo:

- Auditoria administrativa - Auditoria cujo objeto de análise são, para além do plano da organização, os procedimentos e os documentos de suporte dos processos de tomada de decisão, que conduzem à autorização das operações por parte da Direção.
- Auditoria articulada - Forma de implementação coordenada das auditorias internas e/ou externas, nas situações em que as responsabilidades estejam sobrepostas. Essa coordenação é feita por intermédio da comunicação recíproca da calendarização e dos resultados, assim como da utilização comum de meios, com o objetivo de utilizar eficientemente os recursos que estejam à disposição da auditoria.
- Auditoria da informação histórica - Este tipo de auditoria tem como objeto o conjunto de informação histórica, cuja análise é realizada, sempre, *a posteriori*.
- Auditoria das tecnologias de informação - Este tipo de auditoria incide na análise dos sistemas e ambiente informáticos de uma organização, da segurança das suas informações e das políticas e dos controlos organizacionais inerentes à área das Tecnologias de Informação da organização.

- Auditoria de sistemas - Auditoria que analisa os sistemas, especialmente o sistema de controlo interno da organização auditada e que procura identificar os eventuais pontos fortes e/ou deficiências desse controlo interno. Permite, desta forma, definir o local, a natureza e o âmbito dos trabalhos de auditoria considerados necessários para formular o seu parecer.
- Entre outras.

No entanto, no âmbito deste projeto a auditoria das TIC e a auditoria dos sistemas seriam as mais adequadas. Podemos entender por auditoria das tecnologias de informação como sendo um tipo de auditoria que incide na análise dos sistemas e ambiente informáticos de uma organização, da segurança das suas informações e das políticas e dos controlos organizacionais inerentes à área das TIC da organização (Gaai/Ipad,2009).

Podemos entender por auditoria de sistemas como sendo um tipo de auditoria que que analisa os sistemas, especialmente o sistema de controlo interno da organização auditada e que procura identificar os eventuais pontos fortes e/ou deficiências desse controlo interno. Permite, desta forma, definir o local, a natureza e o âmbito dos trabalhos de auditoria considerados necessários para formular o seu parecer(Gaai/Ipad,2009).

Após uma fase de auditoria é sempre importante a sua avaliação e as conclusões que resultaram da auditoria, pois desta forma as organizações podem identificar as suas lacunas, identificar riscos através das não conformidades identificadas e desta forma implementar novos processos, ou reformular processos existentes de forma a mitigar as lacunas e riscos identificados.

Quando existem não conformidades, segundo a norma ISO/IEC 27007(2013) a organização deverá:

- Reagir à não conformidade e se aplicável:
    - Agir de forma a controlar e corrigir a não conformidade, e
    - Lidar com as consequências.
- Avaliar a necessidade de ação para eliminar as causas da não conformidade, de forma a que não se repita ou ocorra noutro lado, nomeadamente através da:
    - Revisão da não conformidade;
    - Determinação das causas da não conformidade, e
    - Determinação da existência de não conformidades semelhantes ou que possam ocorrer;
- Implementar qualquer ação necessária;
- Avaliar a eficácia das ações corretivas; e
- Efetuar alterações ao SGSI, se necessário.

As ações corretivas, devem ser apropriadas aos efeitos das não conformidades encontradas. A organização deverá guardar documentação como evidências:

- da natureza das não conformidades e quaisquer ações subsequentes tomadas, e
- dos resultados de qualquer ação corretiva.

Desta forma, podemos assumir que as auditorias são muito importantes para as organizações pois através da identificação das não conformidades, as empresas conseguem identificar e mitigar os seus riscos.

2.4.2. Segregação de funções

A segregação de funções é um método para redução do risco de uso indevido acidental ou deliberado dos sistemas. Convém que sejam tomados certos cuidados para impedir que uma única pessoa possa aceder, modificar ou usar ativos sem a devida autorização ou deteção (ISO17991,2005).

Segundo Leal (2016), segregação de funções refere-se a práticas onde o conhecimento e/ou privilégios necessários para se completar um processo são partidos e divididos entre múltiplos utilizadores de forma a que apenas um seja capaz de executá-lo ou controlá-lo sozinho.

A ISO 27001 (2013) considera a segregação de funções como um dos potenciais controlos a serem implementados para controlar a implementação e operação da segurança da informação dentro da organização (controlo A.6.1.2 do Anexo A). (verificar anexo 1)

O controlo da norma requer que atividades e áreas de responsabilidades conflituantes sejam segregadas de forma a reduzir o risco de um acesso não autorizado a um ativo ou uma modificação ou mau uso não intencional. (Leal,2016)

3. Objetivo e Metodologia

3.1. Objetivo

O objetivo principal do presente trabalho corresponde à análise, caracterização, avaliação e eventual proposta de metodologia, relativamente à prática da gestão de acessos dos utilizadores, no que respeita à segurança da informação, numa grande empresa de grande dimensão no sector das telecomunicações.

Para além deste objetivo, procurou-se no decurso deste projeto, sensibilizar os diversos intervenientes para a relevância e criticidade da segurança da informação e dos SI.

3.2. Metodologia

Para o estudo, foram adotadas diferentes metodologias de acordo com os objetivos e especificidades das diferentes etapas das diversas fases desenvolvidas, que se apresentam na figura 12.

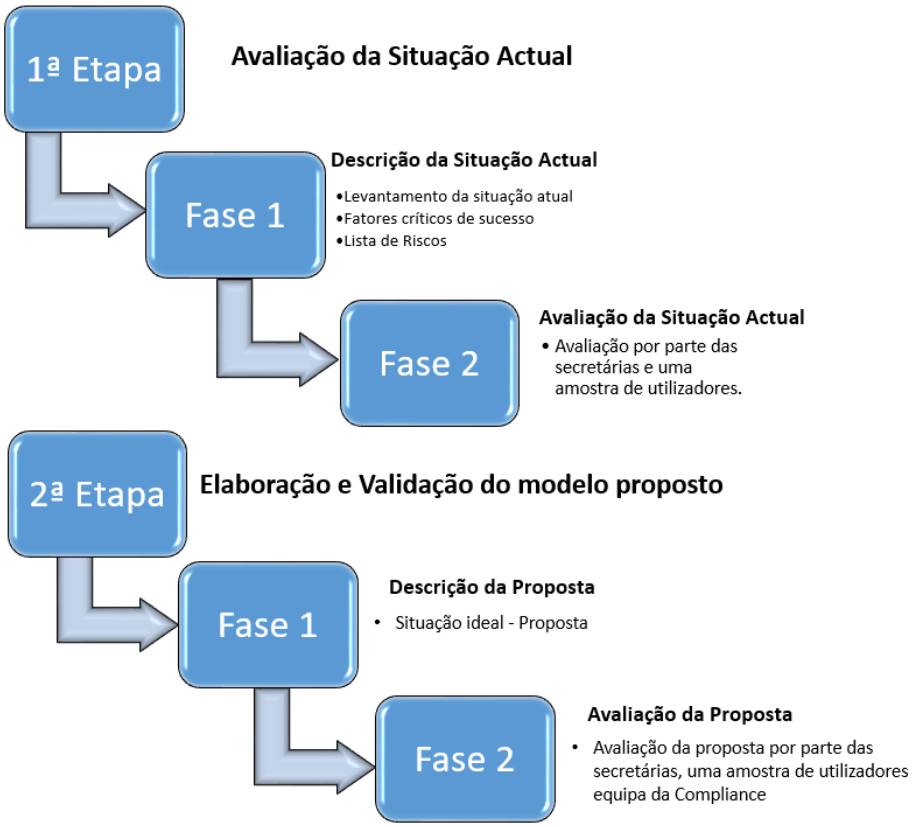


Figura 12 - Fases da metodologia seguida (elaboração própria)

Na primeira fase da primeira etapa procurou-se efetuar a avaliação da situação atual da organização através da sua caracterização atual, a identificação de alguns fatores críticos de sucesso e do levantamento dos riscos identificados pela equipa da Compliance tendo em consideração o modelo atual.

Foi aplicada a metodologia do *focus group*, desenvolvida em sessões de brainstorming. Através desta metodologia procurou-se proceder ao levantamento e análise da situação envolvendo os principais «atores» com responsabilidade, neste domínio, ao nível organizacional conforme anexo 2.

Os participantes no *focus group* foram escolhidos pela sua responsabilidade organizacional, pelo impacto no domínio do sistema de informação e na gestão dos acessos e pela experiência e conhecimento que possuem. Participaram os seguintes elementos, nomeadamente:

- Manager da área de Segurança da Informação;
- Diretor da Fraude / Risco;
- Diretor da área de segurança de informação;
- Manager da equipa de UAM;
- Secretárias;
- Diretor de RH; e
- Alguns utilizadores finais.

O objetivo da escolha de cada um dos profissionais anteriormente indicados foi agregar e obter a perceção das diversas perspetivas existentes em relação à segurança da informação:

- O diretor da fraude /risco pois é o responsável por decidir que acessos são considerados um risco para a empresa e a que utilizadores devem ser atribuídos. A equipa do deste diretor é responsável pela aprovação de todos os acessos considerados como acessos de segurança.
- O diretor da área da segurança da informação pois tem o conhecimento de todas as aplicações e quais as que representam um maior risco.
- O manager da equipa de UAM pois conhece o sistema de gestão de acessos, é responsável pela principal área de criação de acessos da empresa e tem um conhecimento muito real das necessidades dos utilizadores.
- As secretárias, pois, utilizam diariamente a ferramenta de gestão de acessos para desempenhar muitas das suas funções e têm uma maior perceção das dificuldades e problemas assim como do que deve ser alterado para que o seu trabalho possa ser agilizado.
- O diretor dos RH pois tem um conhecimento geral de todo o trabalho diário realizado pelas secretárias e as suas necessidades.

- Os utilizadores finais, pois, a forma como são atribuídos os acessos é um pouco demorada, tentamos desta forma verificar o que acham que deveria ser alterado.

A adoção da metodologia do *focus group* deveu-se ao facto de estar a ganhar cada vez mais espaço no domínio da investigação em sistemas de informação e ser um método que pode ser combinado com outros métodos de pesquisa. Os resultados obtidos são efetivos fornecendo informações sobre o que as pessoas pensam, sentem e consideram relevante nas ações a tomar perante um determinado assunto ou problema.

Segundo Wilkinson (2004), o *focus group* é uma discussão informal acerca de um determinado tópico entre indivíduos selecionados. O *focus group* é diferente das entrevistas em grupo, uma vez que as interações grupais são tratadas explicitamente como "dados de pesquisa" (Ivanoff & Hultberg, 2006). Os participantes são escolhidos porque são capazes de fornecer contribuições valiosas para a pesquisa. A discussão entre os participantes fornece aos pesquisadores a oportunidade de ouvir questões que podem não surgir da sua interação com os pesquisadores sozinhos (Gaiser, 2008).

Apresenta como vantagens a possibilidade de observar profundamente a interação, elementos profundos e um vasto conteúdo de visões, opiniões, experiências, comportamentos e atitudes dos participantes (Berg, 2001) (Morgan, 1996) (Queirós & Lacerda, 2013); fornece características psicológicas e socioculturais, conscientes, semiconscientes ou inconscientes (Berg, 2001) (Queirós & Lacerda, 2013); gera um consenso de ideias, questões, tema e soluções devido ao efeito sinérgico (Berg, 2001); gera dados comparativos entre as experiências e pontos de vista em vez de dados individuais (Morgan, 1996); não é estático, ou seja, é flexível; e o moderador é a chave para o sucesso do estudo, pois é ele que controla as intervenções e retira as ideias chaves do estudo (Reddy, SD).

Como desvantagens podem ser mencionadas que as ideias mais sensíveis podem não ser discutidas. O moderador controla a discussão consoante a sua experiência e a heterogeneidade de indivíduos pode condicionar os resultados, ou seja, como normalmente os grupos de discussão não são muito grandes as discussões podem tornar-se mais restritas (Reddy, SD).

Na segunda fase da primeira etapa, após as sessões de brainstorming, foi efetuado, através de um questionário às secretárias e a uma amostra de utilizadores, um levantamento mais detalhado, tendo em vista perceber com maior pormenor o processo de perfilagem existente atualmente na empresa.

O recurso ao questionário teve em vista facilitar a caracterização atual da situação no que respeita às práticas de gestão de acessos atendendo ao número elevado de utilizadores. Para tal procurou-se analisar as seguintes dimensões:

- Facilidade e rapidez na atribuição de acessos;
- Segurança na atribuição de acessos
- Importância da revisão de acessos

As questões específicas colocadas em cada dimensão podem ser verificadas no anexo 3.

Na primeira fase da segunda etapa foi proposta uma alteração ao modelo atual com base nos resultados da primeira etapa. Na segunda fase, pretendeu-se uma nova validação, junto novamente, das secretárias, de uma amostra de utilizadores consultar e da equipa de Compliance de forma a conseguirmos perceber se esta proposta se adequa melhor às necessidades organizacionais e se proporciona uma minimização dos riscos associados à segurança da informação. Para tal, através da listagem de risco enunciados pelo *focus group* avaliar-se-á, numa escala de likert, o grau de concordância que uma eventual adoção do modelo poderá trazer relativamente à minimização potencial dos riscos identificados.

O recurso ao questionário teve em vista facilitar a validação da proposta no que respeita às práticas de gestão de acessos atendendo ao número elevado de utilizadores. Para tal procurou-se analisar as seguintes dimensões:

- Facilidade e rapidez na atribuição de acessos;
- Segurança na atribuição de acessos
- Importância da revisão de acessos

As questões específicas colocadas em cada dimensão podem ser verificadas no anexo 4.

4. Avaliação da Situação Atual

4.1. Descrição da Situação atual

De forma a conseguirmos descrever a situação atual, efetuaram-se três reuniões com os diferentes intervenientes no processo (anexo 2). Atualmente todos os acessos são atribuídos pelas secretárias de forma manual e individual aos utilizadores através de uma ferramenta de gestão de acessos. É nesta ferramenta que é feita toda a gestão dos acessos da empresa. Podemos consultar o fluxo no anexo 5.

É uma aplicação transversal a toda a empresa sendo utilizada com diferentes abordagens por:

- Áreas de criação - de forma a aprovisionar os acessos das aplicações pelas quais são responsáveis;
- Secretárias - para pedirem os acessos para os utilizadores e consultarem as informações dos seus *assisted users*;
- *Managers* - para consultarem os seus dados e o dos seus *managed users* e para efetuarem algumas aprovações de acessos que necessitem de aprovação do *manager*;
- Aprovadores específicos - para poderem aprovar / rejeitar os acessos dos quais são aprovadores específicos (estes aprovadores podem ser um utilizador ou uma área);
- Diretores - para consultarem os seus dados e o dos seus *managed users* e para efetuarem algumas aprovações de acessos que necessitem de aprovação do diretor;
- Utilizadores finais - para poderem consultar os seus dados e o status dos seus acessos.

Conforme podemos verificar nas reuniões de *focus group* (anexo 2) esta forma de atribuição de acesso gera alguns problemas, nomeadamente:

- Trabalho repetitivo por parte das secretárias da organização, na medida em que estas têm de atribuir todos os acessos de forma manual, utilizador a utilizador, independentemente do número de acessos (sejam apenas 5 ou 300);
- O catálogo de acessos que existe na ferramenta de gestão de acessos por vezes não é claro a nível de nomenclatura dos acessos e muitos não têm uma descrição que possa ser consultada, o que pode levar a que sejam solicitados / atribuídos acessos indevidamente.
- Quando os utilizadores alteram a sua função ou a sua equipa, muitas vezes ficam com acessos que pertenciam à sua função anterior pois estes têm de ser retirados um a um pela secretária e por vezes isso não acontece, o que pode gerar falhas de segurança, na medida em que podemos ter utilizadores a aceder a aplicações às quais já não deveriam ter acesso
- Os acessos considerados de segurança não são revistos quando o utilizador muda de função ou equipa, o que também pode levar a uma grande falha na segurança, ou seja,

podemos ter utilizadores a aceder a informações que não deviam ou a entrar em pisos para os quais já não deveriam ter acesso.

Quando um utilizador muda de funções, é efetuado um controlo chamado de *moovers*. Este controlo consiste no envio de um email ao novo manager do utilizador com todos os acessos que o utilizador tem atualmente, para que o manager possa validar se o utilizador precisará de todos os acessos para o desemprenho da sua nova função e é atribuído um prazo de 10 dias para que o manager responda ao email, caso contrário todos os acessos serão mantidos.

Pretende-se estudar uma solução para reduzir este trabalho repetitivo por parte das secretárias e reduzir as falhas de segurança. Será proposta uma solução para que estas situações sejam ultrapassadas ou pelo menos reduzidas.

4.1.1. Fatores críticos de sucesso

Durante o estudo nas reuniões de *focus group* foram identificados diversos fatores críticos de sucesso (anexo 2) nomeadamente, o aumento da produtividade, a eliminação de riscos, por exemplo, ter um utilizador com um acesso ativo que já não necessita para o desempenho das suas atuais funções pode representar um risco muito grande para a empresa, a reengenharia estratégica, a reengenharia de processos de negócios, menores custos, por exemplo, ter um utilizador parado diversos dias ou mesmo horas devido ao facto de não ter acessos pode representar um custo muito elevado para a empresa e incremento de performance nos processos de negócio.

Fatores críticos de sucesso podem ser considerados fatores que contribuem mais que outros para o sucesso de uma organização. Pela mensuração destes fatores podemos avaliar desempenhos de forma a reunir informações que serão cruciais na seleção de novas estratégias a implementar.

Segundo Rockart (1979) define o que são os FCS, enquanto indicadores claros que podem orientar o rumo do negócio para o sucesso. Neste sentido e segundo Freire (2008), as empresas deverão definir os referidos fatores críticos de sucesso, tendo em conta os seus objetivos, analisando de forma clara as estratégias de concretização dos mesmos, para que se evitem resultados inferiores ao estipulado, mas que permitam, caso assim se verifique, reformular ou enveredar por diferentes caminhos para a implementação prática e com sucesso das referidas estratégias, partindo sempre da premissa que a não concretização dos mesmos poderá dar a entender ao mercado que o esforço da empresa é inferior ao previsto, sendo prejudicial para a sua continuidade, na atual conjuntura económica.

4.1.2. Lista de Riscos

No decorrer de uma das reuniões com a equipa da Compliance (consultar atas das reuniões no anexo 2), foi-nos fornecida a seguinte lista de alguns riscos identificados pela Compliance em relação ao processo atual da gestão de acessos:

- Acesso indevido a informação pessoal sensível;
- Acesso indevido a informação de clientes;
- Acesso não autorizado aos sistemas permitem que transações fraudulentas, maliciosas ou não intencionadas sejam efetuadas;
- Acessos não autorizados podem prejudicar a performance dos sistemas;
- Acessos não autorizados podem afetar a fiabilidade dos dados;
- Acessos físicos ao hardware oferece oportunidade para o acesso não autorizado aos sistemas e dados;
- O acesso físico deve ser restrito a pessoas autorizadas de modo a minimizar a perda ou dano de aplicações e dados;
- Em caso de desastre ou falha humana grave as informações criticas do negócio podem não ser recuperadas;
- Os níveis de serviços de terceiros devem ser definidos de acordo com as necessidades da empresa;
- Os níveis de serviços de terceiros devem ser autorizados e geridos de forma regular para garantir que o desempenho atinja os objetivos esperados;
- Alterações não autorizadas ou mal testadas podem gerar falhas graves na integridade dos controlos que suportam os relatórios internos;
- Utilizadores não autorizados podem ter acesso a sistemas e/ou subsistemas (elementos de rede, sistemas de mediação, entre outros) e podem ser capazes de modificar dados (sms, entre outros);
- Os acessos lógicos devem ser restritos a pessoas autorizadas para que não existam mudanças não autorizadas;
- A falta de conhecimento do que algumas aplicações fazem ou dão acesso representa um risco muito elevado;
- Possibilidade de perca ou dano no inventário devido a acessos indevidos;
- Deve ser efetuada a alteração de função do utilizador para evitar acessos indevidos;
- Utilizadores com acessos atribuídos pelas equipas diretamente nas aplicações sem estarem devidamente certificados no sistema de gestão de acessos representam um risco elevado;
- Utilizadores alocados a equipas incorretas representa um risco elevado;

- Deverá ser feita uma revisão regular da listagem de acessos considerados de segurança.

Esta lista de acessos, serviu para que pudéssemos identificar algumas das lacunas e riscos existentes no modelo atual, conseguindo desta forma na nossa proposta otimizar alguns pontos.

4.2. Análise situação atual

Ao analisarmos as respostas dadas pelos utilizadores ao questionário, existem algumas questões de descontentamento que são mais evidentes:

- 77% dos utilizadores responderam que discordavam que os acessos fossem atribuídos de forma rápida;
- 76% discordam que os acessos são atribuídos de forma eficaz;
- 38% discordam que o processo de atribuição de acessos é um processo simples; e
- 55% discordam plenamente quando a questão é referente á facilidade na alteração dos acessos por utilizador quando este muda de funções.

Conseguimos verificar também que existe um problema claro com a nomenclatura atual dos acessos, pois 75% dos utilizadores discordam plenamente na questão referente à facilidade de encontrar os acessos pretendidos na ferramenta de gestão de acessos. Além desta constatação, existe também uma preocupação por parte dos utilizadores na falta de revisão de acessos quando existe uma mudança de funções (48%) e na questão sobre a existência de falhas de segurança na atribuição dos acessos (76% concordam plenamente) o que representa muitos dos riscos de segurança levantados pela Compliance.

Nº	Questões	Discordo Plenamente	Discordo	Concordo	Concordo Plenamente
1	A ferramenta de gestão de acessos é simples de utilizar	6%	25%	22%	48%
2	Os acessos são atribuídos de forma rápida	16%	77%	7%	0%
3	Os acessos são atribuídos de forma eficaz	19%	76%	5%	0%
4	É fácil encontrar o acesso que se pretende na ferramenta de gestão de acessos	75%	15%	10%	0%
5	O processo de atribuição de acessos é o correto	28%	51%	19%	2%
6	O processo de atribuição de acessos é simples	13%	58%	25%	5%
7	O processo de remoção de acessos é simples	4%	38%	58%	0%
8	A alteração de acessos é fácil quando um utilizador muda de funções	55%	37%	8%	0%

9	Deveria ser feita uma revisão dos acessos do utilizador quando este muda de funções	6%	16%	30%	48%
10	Considera que existem falhas de segurança na atribuição de acessos	0%	7%	17%	76%

Tabela 1 - Quadro representativo das respostas ao questionário 1

Segundo o quadro apresentado acima, podemos concluir que os utilizadores em geral, estão descontentes com o modelo atual de perfilagem implementado na empresa e a Compliance muito preocupada com os riscos atuais de segurança na atribuição dos acessos.

De acordo com as conclusões apresentadas, será apresentada uma proposta de melhoria na segunda etapa deste estudo.

5. Elaboração e validação do modelo proposto

5.1. Descrição da Proposta

Após o estudo feito através da metodologia *focus group*, será proposta uma solução que incide sobre uma metodologia da criação de perfis funcionais, ou seja, os utilizadores passarem a ser agrupados em equipas funcionais dependendo da sua área e função dentro da empresa.

Os principais objetivos da nova proposta serão tentar mitigar os riscos identificados pela Compliance no ponto 4.1.2 e tentar dar resposta às dificuldades dos utilizadores, detetadas no questionário da fase dois da primeira etapa do estudo (anexo 3).

Para efetuar esta alteração consideramos que devem existir 4 fases distintas:

- **Fase 1:**
  - Definição de um plano de *onboarding* - nesta etapa deverá ser definido um plano de projeto e indicado um SPOC por área, ou seja, é nomeada apenas uma pessoa por área para ser o ponto de contacto com a equipa de projeto;
  - Deverá existir uma reunião com os SPOC de todas as áreas para que fiquem a par do projeto e o que é pretendido por parte deles;
  - Deverá ser efetuada uma extração de todos os utilizadores por área - nesta etapa deverá ser solicitada uma extração de todos os utilizadores da empresa (internos e externos) separados por área onde estão inseridos. Este ficheiro será dividido por área e enviado aos SPOCs das áreas identificados anteriormente;
  - A área deverá agrupar os utilizadores por função e definir o nome da Equipa Funcional a que devem pertencer. Este nome terá algumas regras:
    - Deverá ter no máximo 60 caracteres pois é o número máximo que o sistema de RH suporta;
    - O nome deve ter a seguinte nomenclatura - Iniciaisdaarea_Nome pretendido para a equipa funcional Exemplo: NW_Manager.).

- **Fase 2:**
  - A divisão das equipas deverá ser enviada à equipa de *Technology Security Office – Processes* (TSO) - nesta etapa a equipa deverá extrair todos os acessos dos utilizadores por área e entregar à equipa de projeto;
  - A equipa de projeto reúne-se com os SPOC das áreas e verificam, equipa a equipa os acessos que pretendem manter e eliminar/adicionar ás equipas;

- Deverá ser enviada à equipa TSO – Processes e á equipa de auditoria a listagem com os utilizadores, as suas respetivas equipas e os acessos que os SPOC pretendem que a equipa venha a ter;
- A equipa TSO – Processes deverá validar os acessos a atribuir a cada equipa de forma a verificar se existem acessos que não fazem sentido serem atribuídos aquela equipa, se existem acessos que são incompatíveis entre si ou se estão a ser atribuídos acessos considerados de segurança a uma equipa inteira, ou seja, é efetuada uma análise de SOD (Auditoria de acessos e segregação de funções);
- A equipa de auditoria efetua deverá efetuar uma validação a nível de risco de acordo com as regras de SOD's;
- Caso existam algumas questões sobre o pedido de acessos, serão pedidas algumas justificações ao SPOC em relação a alguns acessos, para que se consiga perceber se os acessos são mesmo necessários e se devem ser atribuídos a um conjunto de utilizadores;
- Após a receção das respostas de justificação por parte do SPOC, as equipas de segurança e auditoria deverão propor o pacote de acessos final a implementar;
- Será efetuada pela equipa de projeto uma reunião com os SPOC para que estes possam aprovar os pacotes finais.

- **Fase 3:**
  - Será efetuado um briefing pela equipa de projeto junto dos SPOC antes da migração dos utilizadores para as equipas funcionais;
  - Será efetuado um planeamento da criação das equipas junto da equipa TSO – Processes;
  - A equipa TSO – Processes efetuará a parametrização da equipa funcional no sistema de gestão de acessos;
  - Esta parametrização será refletida na ferramenta dos RH;
  - Será agendada uma fase de piloto, onde será selecionado apenas um ou dois utilizadores (dependendo da dimensão da equipa) para efeitos de monitorização dos processos. Durante esta fase, que terá a duração de cerca de quatro dias úteis, os utilizadores escolhidos para esta fase, perderão automaticamente todos os acessos que não façam parte dos acessos que compõem a sua equipa funcional, para que desta forma se consiga detetar se existe algum acesso em falta e proceder à correção imediata da equipa.

- **Fase 4:**
  - Após o término da fase de piloto e obtida a aceitação por parte das equipas, a equipa de projeto solicitará à equipa TSO – Processes que sejam atribuídos os restantes

utilizadores á equipa funcional, ou seja, a equipa entra em produção ou processo de BAU. Nesta fase os acessos que não fazem parte da equipa, ficam de forma automática agendados para serem removido ao fim de 30 dias;

- Assim que as equipas entrem nos processos de BAU, as equipas funcionais passam a ser geridas por um *owner* e contribuidor previamente definido para cada equipa funcional. Nesta fase, os *owners* e contribuidores poderão efetuar as alterações que pretendem à sua equipa funcional, no entanto, essas alterações passaram sempre pelas aprovações das equipas de segurança e equipas de auditoria / risco.

  O *owner* será sempre um colaborador internos e o contribuidor será sempre uma secretária.

  O contribuidor pode apenas sugerir alterações aos acessos das equipas funcionais (adição ou remoção de acessos).

  O *owner* poderá também sugerir alteração de acessos (adição/remoção) mas terá que aprovar todas estas alterações para que o processo possa passar para a próxima fase de aprovações.

Na figura 13, apresentamos um resumo das fases indicadas acima, para uma melhor compreensão da proposta e no anexo 6 apresentamos os diagramas da proposta.

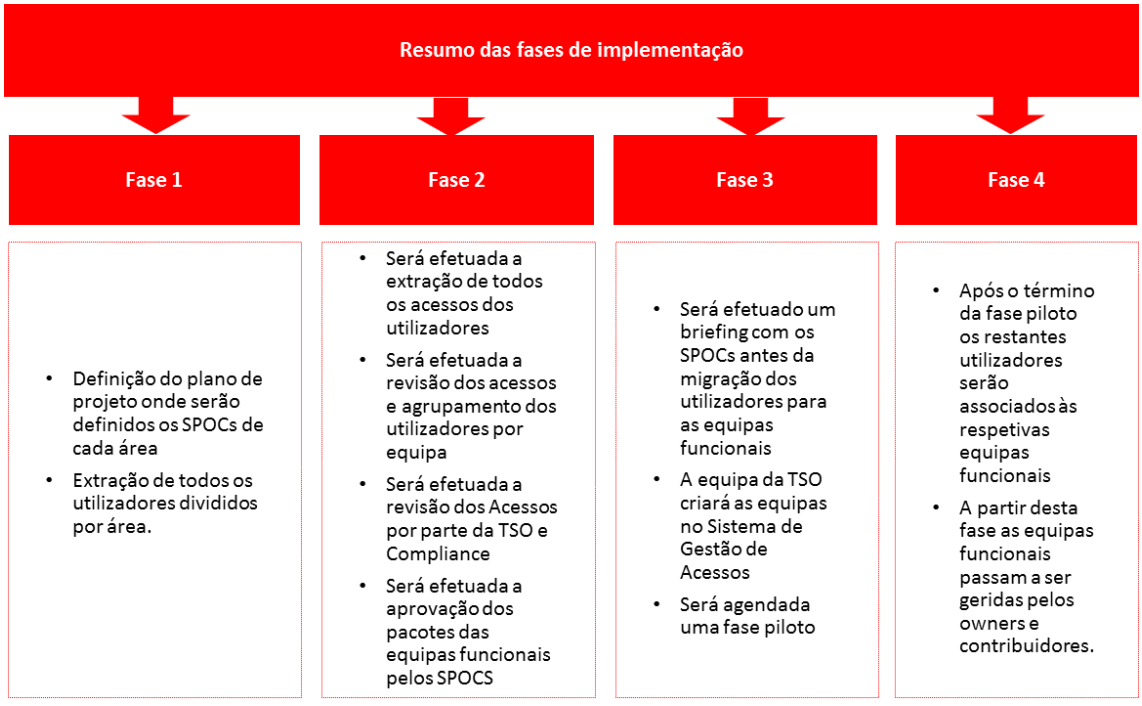


Figura 13 - Resumo das fases de implementação da proposta (elaboração própria)

Para conseguirmos dar resposta à questão 10 do questionário efetuado “Deveria ser feita uma revisão dos acessos do utilizador quando este muda de funções”, propomos que o processo existente de *moovers* seja alterado.

Sempre que um utilizador mude de perfil funcional, deverá ser efetuada uma revisão de todos os seus acessos de segurança pelos aprovadores específicos dos acessos e não pelos seus managers, deverá ser atribuído um prazo de 10 dias para resposta e no caso de ausência da mesma os acessos deverão ser removidos.

Todos os acessos que pertencem ao perfil funcional anterior serão removidos no prazo de 30 dias.

Em relação à questão da nomenclatura referida na questão 3, a revisão deverá ser efetuada no âmbito do projeto de GDPR.

5.2. Avaliação da Proposta

De forma a analisarmos se a proposta apresentada vai de encontro ao pretendido foi efetuado um novo questionário. Neste questionário além das secretárias e amostra de utilizadores que responderam ao questionário anterior, incluímos também a equipa de Compliance (5 membros) de forma a verificarmos se alguns dos riscos apresentados por eles poderão ser mitigados com esta nova proposta.

Para a constituição do novo questionário foram abordados os temas a da facilidade da atribuição de acessos, a rapidez da sua atribuição, segurança e a sua revisão na alteração de funções, criação de equipas funcionais, alteração ao processo dos *moovers* e importância das aprovações dos acessos e incluídas algumas questões referentes à segurança, considerando este novo cenário de atuação evidenciado na proposta.

5.2.1. Análise da validade da proposta de solução

Ao analisarmos as respostas dadas pelos utilizadores ao questionário, podemos verificar que este novo modelo apresenta melhorias significativas em diversas das questões apresentadas.

- 64% dos utilizadores concordam plenamente que a atribuição de acessos tende a ser mais rápida em comparação com os 7% que concordavam com o processo atual;
- 85% concordam plenamente que o processo de atribuição de acessos se afigura mais simples, em comparação aos 5% que concordavam com o processo atual.

A questão que continua a apresentar lacunas e que não será resolvida nesta fase da proposta é a da questão 3 que se refere à nomenclatura e que só deverá ser estudada uma nova posteriormente.

Verificamos que em algumas questões, existem alguns utilizadores que não estão totalmente de acordo com a proposta do novo modelo, nomeadamente na questão do fluxo de aprovação (22% discorda e 7% discorda plenamente), pois é um ponto que causa algum desconforto, apesar de na situação atual também existir o processo de aprovações, na nova proposta os intervenientes preferiam não ter um fluxo de aprovações, pois acaba por fazer com que o processo de atribuição de acessos possa ser um pouco mais demorado do que o utilizador pretendia, no entanto para obtermos um nível maior de segurança este fluxo de aprovação é necessário pois cada interveniente no fluxo de aprovações tem um papel importante para assegurar

a segurança da informação. O *owner* do pacote de acessos, na medida em que valida se os acessos são os necessários para o desempenho das funções da sua equipa; a Compliance, na medida em que vai avaliar os acessos consoante os riscos que apresenta e a TSO, na medida em que valida além dos riscos se os acessos são adequados ás equipas, se podem ser dados em conjunto com alguns acessos que os utilizadores já têm, entre outras.

Nº	Questões	Discordo Plenamente	Discordo	Concordo	Concordo Plenamente
1	Com a nova proposta acha que os acessos poderão ser atribuídos de forma rápida	0%	7%	29%	64%
2	Com a nova proposta acha que os acessos poderão ser atribuídos de forma eficaz	7%	7%	23%	63%
3	Com a nova proposta acha que será mais fácil encontrar o acesso que se pretende na ferramenta de gestão de acessos	71%	18%	11%	0%
4	Com a nova proposta acha que o processo de atribuição de acessos será o mais correto	0%	6%	31%	63%
5	Com a nova proposta acha que o processo de atribuição de acessos será mais simples	0%	0%	15%	85%
6	Com a nova proposta acha que o processo de remoção de acessos será mais simples	0%	4%	19%	78%
7	Com a nova proposta acha que a alteração de acessos será mais fácil quando um utilizador muda de funções	0%	0%	11%	89%
8	Com a nova proposta concorda com a revisão de acessos quando existir uma alteração de funções	0%	4%	0%	96%
9	Concorda com a criação de equipas funcionais propostas na na nova proposta	0%	7%	16%	77%
10	Concorda com o processo de aprovação das equipas funcionais proposta na nova proposta	7%	22%	23%	48%
11	Concorda com a existência de um owner por equipa funcional como proposto na nova proposta	0%	6%	16%	78%
12	Concorda que os contribuidores sejam as secretárias como proposto na nova proposta	6%	7%	27%	59%
13	Concorda que seja feita uma fase piloto como proposto na nova proposta	0%	0%	4%	96%
14	Concorda com a duração da fase de piloto como proposto na nova proposta	0%	33%	8%	59%

15	Acha que este novo modelo contribuirá para uma melhoria na segurança de atribuição de acessos	0%	7%	31%	61%
16	Com este novo modelo a atribuição de acessos a um novo colaborador será mais eficaz e rápida	0%	0%	3%	97%
17	Com a atribuição de equipas funcionais proposto na nova proposta existirá uma menor probabilidade da errada atribuição de acessos	0%	0%	7%	93%
18	Com a revisão de acessos de segurança proposto na nova proposta existirá uma redução dos acessos indevidos para a função	0%	0%	26%	74%
19	Concorda que o fluxo de aprovação proposto na nova proposta servirá para mitigar riscos de segurança	0%	0%	4%	96%

Tabela 2 - Quadro representativo das respostas ao questionário 2

Segundo o quadro apresentado acima, podemos concluir que os utilizadores e a Compliance em geral, concordam com o modelo proposto de perfilagem a implementar na empresa pois vai resolver muitos dos problemas atuais na atribuição de acessos aos utilizadores.

5.3. Ajustes ao modelo proposto

Ao compararmos as respostas iniciais dos utilizadores com as do segundo questionário podemos concluir que existem alguns ajustes a fazer ao novo processo, nomeadamente:

- Revisão da nomenclatura - na medida em que hoje em dia é complicado encontrar o acesso pretendido, o que pode levar o utilizador a solicitar o acesso errado;
- Automatização de acessos – existem muitos acessos que têm área de criação o que pode levar a demoras no processo de atribuição de acessos. Deveria ser revisto o processo de automatização dos acessos;
- Revisão da duração da fase de piloto – 4 dias úteis foram considerados poucos dias para teste de todos os acessos, ou devido a indisponibilidade dos utilizadores escolhidos para esta fase de testes, ou devido aos acessos não terem todos tempo de ser atribuídos;
- Revisão do Fluxo de aprovação – deverá ser revisto o fluxo de aprovação, pois com o novo modelo uma alteração a uma equipa funcional terá que passar pela aprovação do *owner* da

equipa e pela aprovação de mais três equipas Compliance, TSO e UAM o que pode levar a demoras na atribuição de acessos.

6. Conclusões finais

As motivações para a realização deste projeto centraram-se na melhoria do processo de gestão de acessos dada a valorização crescente da área de Segurança da informação.

Através deste projeto foi possível caracterizar a situação atual da organização em estudo e propor uma melhoria de forma a tentar agilizar o processo de gestão de acessos dos utilizadores e mitigar alguns dos riscos identificados previamente.

A metodologia de *focus group* afigurou-se relevante para a comparação em profundidade da necessidade existente e do problema sentido.

Concluímos através deste projeto que a segurança da informação é uma temática cada vez mais importante no dia a dia das organizações, na medida em que a informação é cada vez mais classificada com um dos bens mais importantes que a organização tem e que pode ser decisiva a nível da vantagem competitiva.

Para que a informação seja utilizada da forma mais correta é necessário implementar politicas de segurança como indicamos neste projeto, de forma a assegurar que esta é utilizada apenas por quem tem permissão para aceder e que possa desta forma ser utilizada da melhor forma.

Implementando politicas de segurança, as empresas conseguem mitigas muitos dos riscos que enfrentam diariamente. Neste projeto tentou-se apresentar uma proposta que permita à organização uma gestão mais efetiva dos acessos, onde conseguem ter um maior controlo de que cada utilizador apenas acede ás informações que necessita para as suas funções diárias. Com a criação de equipas funcionais, os acessos passam a ser segregados por funções, o que leva a um maior controlo dos acessos. Existe também um novo fluxo de aprovações de forma a tentar reduzir os erros de serem solicitados acessos incorretos para o desempenho das funções dos utilizadores.

Este fluxo de aprovações vai passar por um *owner* da equipa funcional, que será por norma um manager da equipa e que vai ter uma noção clara das necessidades da sua equipa, passará também pela aprovação da equipa da Compliance que poderá analisar os riscos de atribuir alguns acessos a determinadas equipas e pelas equipas de TSO, na medida em que podem verificar se os acessos podem ser dados ou não aquele conjunto de utilizadores(validando incompatibilidades de acessos entre si, ou incompatibilidades de acessos com as equipas que os estão a solicitar).

Com esta nova solução, serão reduzidos os riscos de segurança, os utilizadores não terão acessos de forma indevida e a gestão de acessos terá a todos os níveis uma gestão mais efetiva e um maior controlo das falhas de segurança, uma vez que cada utilizador apenas poderá pertencer a uma única equipa funcional.

Acreditamos que com a nossa proposta, conseguimos colaborar para uma melhoria da gestão de acessos dos utilizadores e que conseguimos trazer mais valias a nível da mitigação de alguns riscos identificados durante o estudo.

7. Limitações e trabalho futuro

Estamos conscientes que apesar do nosso contributo o estudo realizado carece de continuidade e deve ser aprofundado. Existem algumas limitações que irão exigir uma reavaliação dos processos, pois todos os acessos que a equipa de segurança e auditoria consideram como acessos de segurança, não serão atribuídos em equipas funcionais, mas pelo método antigo, ou seja, utilizador a utilizador, ou seja, a proposta apresentada não poderá ser implementada na sua totalidade.

Esta lista terá que ser revista para que se consiga obter o menor número de exceções possíveis, só desta forma a gestão de acessos poderá ser mais eficaz e mais segura.

É necessário rever a nomenclatura de todos os acessos e tentar obter junto das áreas uma descrição para todos os acessos que se encontram na ferramenta de gestão de acessos para que seja mais fácil para o *owner* ou contribuidor conseguir perceber o acesso que está a atribuir e se se enquadra no pretendido.

Deverá efetuar-se desenvolvimento na ferramenta de gestão de acessos e na ferramenta de recursos humanos para garantir uma maior flexibilidade ao utilizador para a criação e atribuição de equipas na ferramenta de gestão de acessos (*self-service*).

Deverão ser abrangidos os utilizadores que existem no grupo, ou seja, utilizadores que não se encontram em Portugal, mas que por muitas vezes precisam de aceder aos servidores e aplicações de Portugal.

Todo o processo deve ser revisto de forma a obedecer às novas regras de proteção de dados que deverão estar implementadas até maio de 2018 (GDPR).

Referências Bibliográficas

Beal, Adriana. Gestão Estratégica da Informação: Como transformar a informação e a TI em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas,2004

Berg, B. L. (2001). Focus group interviewing. In B. L. Berg (Ed.), Qualitative research methods for the Social Sciences (Vol. 4, pp. 111-132). Needham Heights: Pearson.

Caldwell Tracey & Steve Johnson – ISSO/IEC 27001 Certification from APMG – Qualifications to help you understand and apply the information security standard, april 2014 (imagem das normas)

Cardoso Júnior, Walter Felix. Inteligência empresarial estratégica. Tubarão:Ed. Unisul, 2005.

Cisco (SD) What is a Firewall? Disponível em https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Committee Draft for Vote. (2008). IEC 31010 Ed. 1.0: Risk Management – Risk Assessment Techniques. International Electrotechnical Commission

Dantas, Leal Marcus (2011), Segurança da Informação: Uma abordagem focada em Gestão de Riscos, Livro Rápido, Olinda – PE

Deming WE. Qualidade: a revolução da administração.São Paulo:Marques Saraiva, 1990

Edmiston, A H. (2007). The role of systems and applications monitoring in operational risk management, BT Technology Journal; Ipswich 25.1 (Jan), 68-78

Faisal, M. N.; Banwet, D.K. & Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. Journal of Enterprise Information Management, 20 (6), 677-699

Freire, A. (2008). Estratégia - Sucesso em Portugal. 12ª edição, Lisboa: Verbo

Garcia, J.L. (2015). A critique of the information economy in the era of digital media. Universidade de São Paulo; artigo disponível em http://hdl.handle.net/10451/20137

Gaai/Ipad -Instituto Português de Apoio ao Desenvolvimento – Glossário de Auditoria,2009

Integrity Consulting & advisory, 27001, SD Sistema de Gestão de Segurança da Informação, portal informativo, disponível em https://www.27001.pt/index.html

ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems - Overview and vocabulary

ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management

ISO/IEC 27007:2013 Information technology — Security techniques — Guidelines for information security management systems auditing

Ivanoff, S.D. and Hultberg, J. (2006) 'Understanding the Multiple Realities of Everyday Life: Basic Assumptions in Focus Group Methodology', Scandanavian Journal of Occupational Therapy, 13

Knapp, E.M. (1998). Knowledge management. Business and Economic Review, 44 (4). July – September

Leal, Rhand (2016) Segregação de funções em seu SGSI de acordo com a ISO 27001 A.6.1.2, disponível em https://advisera.com/27001academy/pt-br/blog/2016/11/23/segregacao-de-funcoes-em-seu-sgsi-de-acordo-com-a-iso-27001-a-6-1-2/

Morgan, D. L. (1996). Focus Groups. Annual Review of Sociology, 22. Disponível em: http://www.jstor.org/stable/2083427

Padoveze, Clovis Luís. Sistemas de Informações Contábeis – Fundamentos e Análise 2.ed., São Paulo; Atlas ,2000

Piropo, B (2014) Bitcoin: encriptação dos dados, disponível em :http://www.techtudo.com.br/artigos/noticia/2014/01/bitcoin-encriptacao-dos-dados.html

Pinto, A. (2005). Sistemas de Gestão Ambiental: Guia para a sua implementação. (1ª ed.). Lisboa: Edições Sílabo

Queirós, P., & Lacerda, T. (2013). A importância da entrevista na investigação qualitativa In I. Mesquita & A. Graça (Eds.), Investigação qualitativa em desporto (Vol. 2). Porto: Centro de Investigação Formação Inovação e Intervenção em Desporto. Faculdade de Desporto. Universidade do Porto.

Ralph, M. Stair e George W. Reynolds. Princípios de sistemas de informação: uma abordagem gerencial. 4a ed. Rio de Janeiro: LTC, 2002.Rasmussen, M. (2006). Taking Control of IT Risk, Forrester Research Inc, February

Reddy ,Chitra, "Focus Groups Meaning". Adaptado de https://content.wisestep.com/focus-groups-features-advantages-disadvantages/)

Rockart, J. (1979). Chief Executives Define Their Own Data Needs. Harvard Business Review, 57,

81-83.

Sêmola, Marcos, Gestão da Segurança da Informação: Uma visão executiva, Rio de Janeiro:Campus., 2003

Serrano, A. & Fialho, C. (2005). Knowledge Management – The New Organizations Paradigm. Lisbon: FCA – Information Publishing) *(In Portuguese)*

Silva, Claudiano J. (2017) Ciclo de vida de Desenvolvimento seguro – Artigo revista Pentest Magazine, disponivel em https://pt.linkedin.com/pulse/ciclo-de-vida-desenvolvimento-seguro-artigo-revista-j-da-silva

Silva Pedro Tavares, Hugo carvalho e Catarina Botelho Torres – Segurança dos Sistemas de informação – gestão estratégica da segurança empresarial, centro atlantico.pt,2003

Vala, C. M. S. (2013) Market orientation as a way to gain competitive advantage in organizations. ESTG - Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria. Available at http://hdl.handle.net/10400.8/1144 (In Portuguese)

Wilkinson, S. (2004). Focus groups: a feminist method. In S. N. Hesse-Biber, & M. L.

Yaiser (Eds.). Feminist perspectives on social research (pp. 271-295). New York: Oxford University Press.

Anexos

Anexo 1

Controlos de referência ISO27001

ISO/IEC 27001:2013(E)

Annex A
(normative)

Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5 Information security policies		
A.5.1 Management direction for information security		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5	Information security in project management	*Control* Information security shall be addressed in project management, regardless of the type of the project.
A.6.2 Mobile devices and teleworking		
Objective: To ensure the security of teleworking and use of mobile devices.		

Table A.1 *(continued)*

A.6.2.1	Mobile device policy	*Control* A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
A.6.2.2	Teleworking	*Control* A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
A.7 Human resource security		
A.7.1 Prior to employment		
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.		
A.7.1.1	Screening	*Control* Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.1.2	Terms and conditions of employment	*Control* The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.
A.7.2 During employment		
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
A.7.2.3	Disciplinary process	*Control* There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
A.7.3 Termination and change of employment		
Objective: To protect the organization's interests as part of the process of changing or terminating employment.		
A.7.3.1	Termination or change of employment responsibilities	*Control* Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
A.8 Asset management		
A.8.1 Responsibility for assets		

Table A.1 *(continued)*

Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets	*Control* Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2	Ownership of assets	*Control* Assets maintained in the inventory shall be owned.
A.8.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
A.8.1.4	Return of assets	*Control* All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
A.8.2 Information classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classification of information	*Control* Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3	Handling of assets	*Control* Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.3 Media handling		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
A.9 Access control		
A.9.1 Business requirements of access control		

Table A.1 *(continued)*

Objective:	To limit access to information and information processing facilities.	
A.9.1.1	Access control policy	*Control* An access control policy shall be established, documented and reviewed based on business and information security requirements.
A.9.1.2	Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
A.9.2	**User access management**	
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9.3	**User responsibilities**	
Objective: To make users accountable for safeguarding their authentication information.		
A.9.3.1	Use of secret authentication information	*Control* Users shall be required to follow the organization's practices in the use of secret authentication information.
A.9.4	**System and application access control**	
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy.
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

Table A.1 *(continued)*

A.9.4.3	Password management system	*Control* Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.4	Use of privileged utility programs	*Control* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.9.4.5	Access control to program source code	*Control* Access to program source code shall be restricted.
A.10 Cryptography		
A.10.1 Cryptographic controls		
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
A.10.1.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2	Key management	*Control* A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
A.11 Physical and environmental security		
A.11.1 Secure areas		
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1	Physical security perimeter	*Control* Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms and facilities shall be designed and applied.
A.11.1.4	Protecting against external and environmental threats	*Control* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
A.11.1.5	Working in secure areas	*Control* Procedures for working in secure areas shall be designed and applied.
A.11.1.6	Delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Table A.1 *(continued)*

A.11.2 Equipment		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1	Equipment siting and protection	*Control* Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
A.11.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.11.2.5	Removal of assets	*Control* Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	*Control* Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
A.11.2.7	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.11.2.8	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.12 Operations security		
A.12.1 Operational procedures and responsibilities		
Objective: To ensure correct and secure operations of information processing facilities.		
A.12.1.1	Documented operating procedures	*Control* Operating procedures shall be documented and made available to all users who need them.
A.12.1.2	Change management	*Control* Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

Table A.1 *(continued)*

A.12.1.3	Capacity management	*Control* The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4	Separation of development, testing and operational environments	*Control* Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Controls against malware	*Control* Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
A.12.3 Backup		
Objective: To protect against loss of data.		
A.12.3.1	Information backup	*Control* Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1	Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4	Clock synchronisation	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.
A.12.5 Control of operational software		
Objective: To ensure the integrity of operational systems.		
A.12.5.1	Installation of software on operational systems	*Control* Procedures shall be implemented to control the installation of software on operational systems.
A.12.6 Technical vulnerability management		
Objective: To prevent exploitation of technical vulnerabilities.		

Table A.1 *(continued)*

A.12.6.1	Management of technical vulnerabilities	*Control* Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
A.12.6.2	Restrictions on software installation	*Control* Rules governing the installation of software by users shall be established and implemented.
A.12.7 Information systems audit considerations		
Objective: To minimise the impact of audit activities on operational systems.		
A.12.7.1	Information systems audit controls	*Control* Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.
A.13 Communications security		
A.13.1 Network security management		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network controls	*Control* Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	Security of network services	*Control* Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
A.13.1.3	Segregation in networks	*Control* Groups of information services, users and information systems shall be segregated on networks.
A.13.2 Information transfer		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1	Information transfer policies and procedures	*Control* Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
A.13.2.2	Agreements on information transfer	*Control* Agreements shall address the secure transfer of business information between the organization and external parties.
A.13.2.3	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.

Table A.1 *(continued)*

A.13.2.4	Confidentiality or non-disclosure agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems		
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.		
A.14.1.1	Information security requirements analysis and specification	*Control* The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	*Control* Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3	Protecting application services transactions	*Control* Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.14.2 Security in development and support processes		
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.		
A.14.2.1	Secure development policy	*Control* Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.2	System change control procedures	*Control* Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
A.14.2.3	Technical review of applications after operating platform changes	*Control* When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4	Restrictions on changes to software packages	*Control* Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
A.14.2.5	Secure system engineering principles	*Control* Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

Table A.1 *(continued)*

A.14.2.6	Secure development environment	*Control* Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.7	Outsourced development	*Control* The organization shall supervise and monitor the activity of outsourced system development.
A.14.2.8	System security testing	*Control* Testing of security functionality shall be carried out during development.
A.14.2.9	System acceptance testing	*Control* Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
A.14.3 Test data		
Objective: To ensure the protection of data used for testing.		
A.14.3.1	Protection of test data	*Control* Test data shall be selected carefully, protected and controlled.
A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.1	Information security policy for supplier relationships	*Control* Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2	Addressing security within supplier agreements	*Control* All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
A.15.1.3	Information and communication technology supply chain	*Control* Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services	*Control* Organizations shall regularly monitor, review and audit supplier service delivery.
A.15.2.2	Managing changes to supplier services	*Control* Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Table A.1 *(continued)*

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	*Control* Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	Planning information security continuity	*Control* The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	Implementing information security continuity	*Control* The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Table A.1 *(continued)*

A.17.1.3	Verify, review and evaluate information security continuity	*Control* The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
A.17.2 Redundancies		
Objective: To ensure availability of information processing facilities.		
A.17.2.1	Availability of information processing facilities	*Control* Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements		
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.		
A.18.1.1	Identification of applicable legislation and contractual requirements	*Control* All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
A.18.1.2	Intellectual property rights	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
A.18.1.3	Protection of records	*Control* Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
A.18.1.4	Privacy and protection of personally identifiable information	*Control* Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
A.18.1.5	Regulation of cryptographic controls	*Control* Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
A.18.2 Information security reviews		
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.		
A.18.2.1	Independent review of information security	*Control* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

Table A.1 *(continued)*

A.18.2.2	Compliance with security policies and standards	*Control* Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3	Technical compliance review	*Control* Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Anexo 2

Atas das reuniões

Reunião Inicial

Intervenientes

- Manager da área de segurança da informação
- Diretor da fraude e risco
- Manager UAM
- Diretor da área de segurança de informação

Temas Abordados

- Revisão do processo de atribuição de acessos
- Identificação de alguns fatores críticos de sucesso
- Visão sobre a situação atual da atribuição de acessos de acordo com os intervenientes.

Principais conclusões

- Identificação dos fatores críticos de sucesso identificados pelos intervenientes
- Identificação da visão geral sobre a situação atual da atribuição de acessos pela visão dos intervenientes
- Recolhidas ideias de melhoria a contemplar na proposta a apresentar

Local: sede

Data: 23-05-2017

Segunda Reunião

Intervenientes

- Secretárias
- Utilizadores

Temas Abordados

- Revisão do processo de atribuição de acessos
- Identificação de alguns fatores críticos de sucesso
- Visão sobre a situação atual da atribuição de acessos de acordo com os intervenientes.

Principais conclusões

- Identificação dos fatores críticos de sucesso identificados pelos intervenientes
- Identificação da visão geral sobre a situação atual da atribuição de acessos pela visão dos intervenientes
- Recolhidas ideias de melhoria a contemplar na proposta a apresentar

Local: sede

Data: 30-05-2017

Terceira Reunião

Intervenientes

- Equipa de Compliance

Temas Abordados

- Identificação de riscos associados ao processo atual de atribuição de acessos
- Visão sobre a situação atual da atribuição de acessos de acordo com os intervenientes.

Principais conclusões

- Recolha da lista de Riscos identificados pela Compliance verificados no processo actual.
- Identificação da visão geral sobre a situação atual da atribuição de acessos pela visão dos intervenientes
- Recolhidas ideias de melhoria a contemplar na proposta a apresentar

Local: sede

Data: 06-06-2017

Anexo 3

Questionário fase 2 da etapa 1

Nº	Questões	Discordo Plenamente	Discordo	Concordo	Concordo Plenamente
1	A ferramenta de gestão de acessos é simples de utilizar	8	32	28	62
2	Os acessos são atribuídos de forma rápida	21	100	9	0
3	Os acessos são atribuídos de forma eficaz	25	99	6	0
4	É fácil encontrar o acesso que se pretende na ferramenta de gestão de acessos	98	19	13	0
5	O processo de atribuição de acessos é o correto	36	66	25	3
6	O processo de atribuição de acessos é simples	17	75	32	6
7	O processo de remoção de acessos é simples	5	50	75	0
8	A alteração de acessos é fácil quando um utilizador muda de funções	71	48	11	0
9	Deveria ser feita uma revisão dos acessos do utilizador quando este muda de funções	8	21	39	62
10	Considera que existem falhas de segurança na atribuição de acessos	0	9	22	99
Total		289	519	258	232

Anexo 4

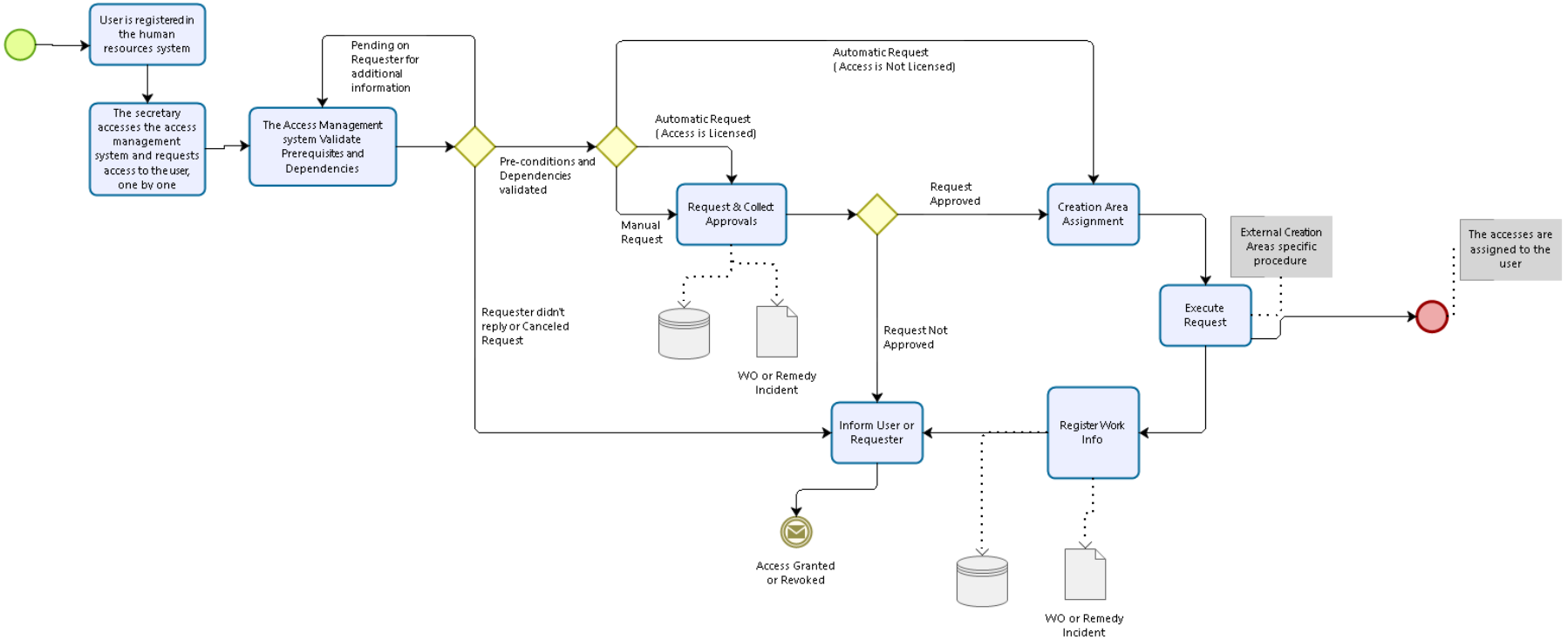
Questionário fase 2 da etapa 2

Nº	Questões	Discordo Plenamente	Discordo	Concordo	Concordo Plenamente
1	Com a nova proposta acha que os acessos poderão ser atribuídos de forma rápida	0	10	39	86
2	Com a nova proposta acha que os acessos poderão ser atribuídos de forma eficaz	9	10	31	85
3	Com a nova proposta acha que será mais fácil encontrar o acesso que se pretende na ferramenta de gestão de acessos	96	24	15	0
4	Com a nova proposta acha que o processo de atribuição de acessos será o mais correto	0	8	42	85
5	Com a nova proposta acha que o processo de atribuição de acessos será mais simples	0	0	20	115
6	Com a nova proposta acha que o processo de remoção de acessos será mais simples	0	5	25	105
7	Com a nova proposta acha que a alteração de acessos será mais fácil quando um utilizador muda de funções	0	0	15	120
8	Com a nova proposta concorda com a revisão de acessos quando existir uma alteração de funções	0	5	0	130
9	Concorda com a criação de equipas funcionais propostas na nova proposta	0	9	22	104
10	Concorda com o processo de aprovação das equipas funcionais proposta na nova proposta	9	30	31	65
11	Concorda com a existência de um owner por equipa funcional como proposto na nova proposta	0	8	22	105
12	Concorda que os contribuidores sejam as secretárias como proposto na nova proposta	8	10	37	80
13	Concorda que seja feita uma fase piloto como proposto na nova proposta	0	0	5	130
14	Concorda com a duração da fase de piloto como proposto na nova proposta	0	44	11	80
15	Acha que este novo modelo contribuirá para uma melhoria na segurança de atribuição de acessos	0	10	42	83
16	Com este novo modelo a atribuição de acessos a um novo colaborador será mais eficaz e rápida	0	0	4	131
17	Com a atribuição de equipas funcionais proposto na nova proposta existirá uma menor probabilidade da errada atribuição de acessos	0	0	10	125

18	Com a revisão de acessos de segurança proposto na nova proposta existirá uma redução dos acessos indevidos para a função	0	0	35	100
19	Concorda que o fluxo de aprovação proposto na nova proposta servirá para mitigar riscos de segurança	0	0	5	130
Total		122	173	411	1859

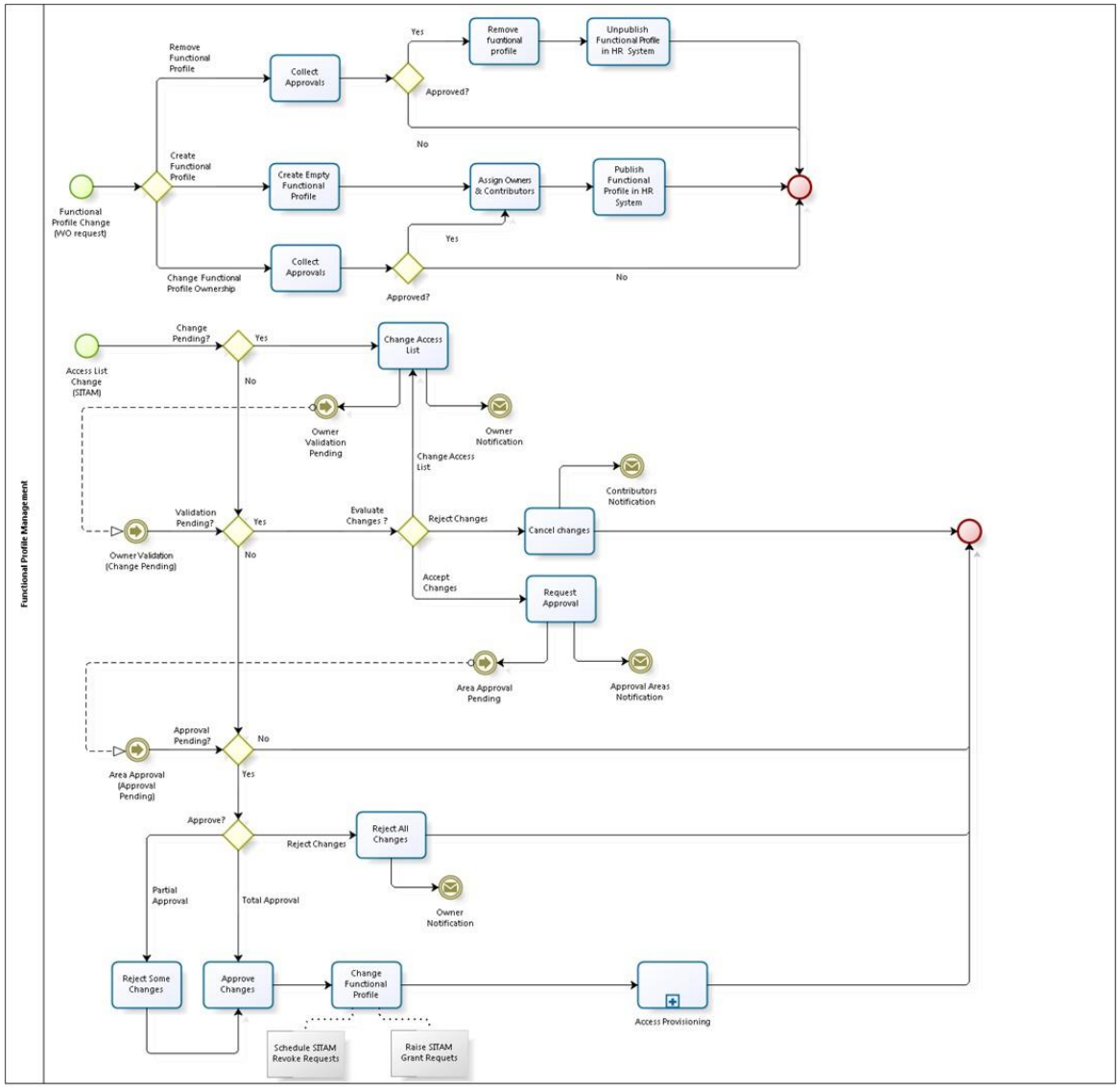
Anexo 5

Diagrama da Situação atual

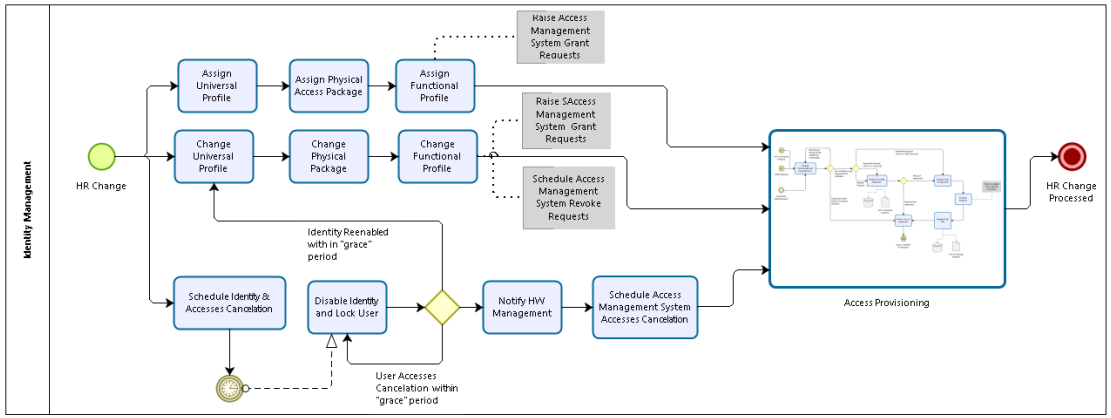


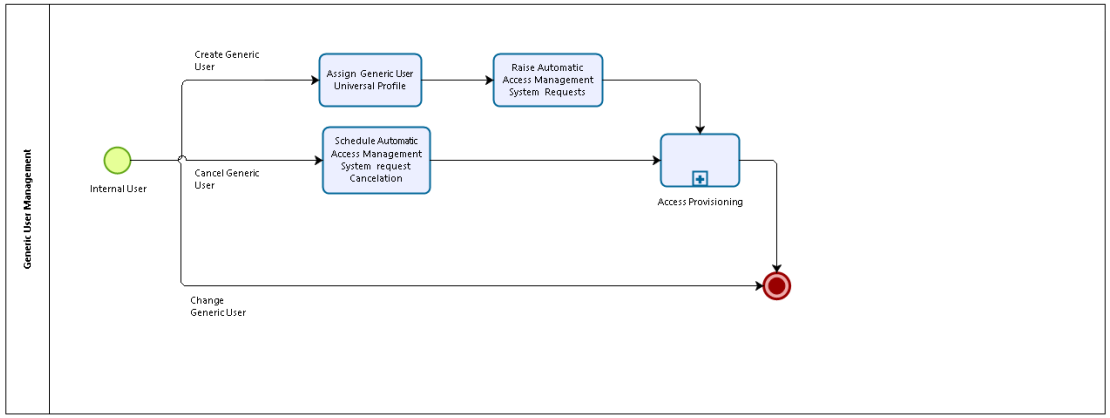
Anexo 6

Diagramas da Proposta - Gestão das Equipas funcionais


Functional Profile Management
Remove Functional Profile
Collect Approvals
Yes
Remove fuctional profile
Unpublish Functional Profile in HR System
Approved?
No
Create Functional Profile
Functional Profile Change (WO request)
Create Empty Functional Profile
Assign Owners & Contributors
Publish Functional Profile in HR System
Yes
Change Functional Profile Ownership
Collect Approvals
Approved?
No
Access List Change (SITAM)
Change Pending?
Yes
Change Access List
No
Owner Validation Pending
Owner Notification
Change Access List
Contributors Notification
Validation Pending?
Yes
Evaluate Changes ?
Reject Changes
Cancel changes
Owner Validation (Change Pending)
No
Accept Changes
Request Approval
Area Approval Pending
Approval Areas Notification
Approval Pending?
No
Area Approval (Approval Pending)
Yes
Approve?
Reject Changes
Reject All Changes
Owner Notification
Partial Approval
Total Approval
Reject Some Changes
Approve Changes
Change Functional Profile
Access Provisioning
Schedule SITAM Revoke Requests
Raise SITAM Grant Requets

Diagramas da Proposta - Top Level





Diagramas da Proposta - Gestão de acessos