

Processos de gestão de informação e Dashboards de suporte à Gestão de Risco

João Miguel Marques Lopes

Dissertação de Mestrado

Orientador na FEUP: Prof. Nuno Soares



Mestrado em Engenharia e Gestão Industrial

2022-07-11

Aos meus pais

Resumo

O presente projeto foi desenvolvido na NOS, que identificou a necessidade de melhoria do processo de monitorização da gestão de acessos. O atual processo recorre excessivamente a atividades manuais, tornando-se lento e difícil de executar. Por um lado, a recolha de dados é demorada e excessivamente repetitiva. Por outro lado, a comunicação é baseada em emails e os gestores de acesso têm a necessidade de exportar, recorrentemente, ficheiros Excel, no qual justificam os acessos atribuídos, enviando o ficheiro preenchido para a direção de auditoria. Por sua vez, a equipa de gestão de risco responsável por este controlo necessita de recolhar os ficheiros enviados por todos os gestores de acessos de forma a atualizar os Dashboards que permitem a análise do processo.

Com o decorrer do projeto, foram desenvolvidos automatismos que agilizam o processo de recolha de dados e foi redesenhado o sistema de comunicação com os gestores de acesso, eliminando a necessidade de emails e trocas de ficheiros Excel, pela implementação de um sistema de alertas. O sistema de alertas fica integrado nos Dashboards enviados aos gestores de acessos, no qual podem verificar o trabalho que é necessário realizar. Por sua vez, os gestores de acesso, justificam e/ou removem acessos diretamente no sistema de gestão de identidades e acessos da empresa, não necessitando de enviar respostas à equipa de gestão de risco. Foram ainda melhorados os Dashboards que permitem visualizar e analisar de forma interativa e dinâmica os dados acerca deste controlo.

Information Management Processes and Risk Management Support Dashboards

Abstract

This project has been developed in NOS, who identified the need to improve the process of access management monitoring. The current process requires an excessive amount of manual work, becoming slow and hard to execute. On one hand, data collection takes too much time and requires a lot of repetitive tasks. On the other hand, communication is based on emails and access managers have the need to frequently export excel files, in which they justify assigned permissions, sending the fulfilled file to the risk department. In addition, the audit team responsible for this control needs to collect the files from every access manager in order to update the Dashboards which allow the process analysis.

With the course of the project, some automatisms that agilize the process of data collection were developed and the system of communication with access managers was redesigned eliminating the need for emails and Excel files exchanges, with the implementation of an alert system. This system is integrated into the Dashboards sent to the access managers in which they can check the work required to be done. Furthermore, access managers justify and/or remove permissions directly on the Identity and Access Management system, erasing the need of sending answers to the risk department. Also, the Dashboards where the data is visualized and analyzed interactive and dynamically were improved.

Agradecimentos

Este projeto não seria possível sem o apoio de um conjunto de pessoas a quem deixo os meus sinceros agradecimentos.

À NOS por todo o apoio na integração na empresa, que me permitiu adquirir uma visão adequada de como a empresa funciona e de toda a dinâmica por detrás dos processos operacionais, e pelo excelente ambiente e condições de trabalho proporcionadas.

De forma geral, a toda a direção de Auditoria, Risco e Compliance que me proporcionou uma experiência extremamente enriquecedora e que contribuiu em muito para o meu desenvolvimento pessoal e profissional.

Em particular, gostaria de agradecer ao David Rebelo que me acompanhou diariamente, de forma incansável e com completa disponibilidade, proporcionando-me uma oportunidade de aprendizagem que supera quaisquer expectativas. Ao Pedro Silva, orientador na empresa, que me acolheu na empresa e acompanhou ao longo do projeto, com total disponibilidade. A todos os colaboradores NOS que de alguma forma se cruzaram no meu percurso, que sempre me apoiaram no meu projeto.

Ao meu orientador da FEUP, Professor Nuno Soares, por toda a disponibilidade e apoio, que nunca desistiu de me incentivar a avançar no trabalho, ainda que, por vezes, tal parecesse impossível, e por toda a paciência e preocupação que teve comigo ao longo do projeto.

Aos meus familiares e amigos que me apoiaram em todos os momentos, pelos quais todo o trabalho faz sentido.

Índice de Conteúdos

1	Introdução	1
1.1	Enquadramento do projeto.....	1
1.2	O grupo NOS	1
1.3	Compliance Corporativa e Monitorização.....	3
1.4	Objetivos do projeto	4
1.5	Metodologia.....	5
1.6	Estrutura da dissertação	6
2	Estado da Arte.....	7
2.1	Big Data	7
2.2	Visualização de dados através de Dashboards	8
2.2.1	Dados, Informação e Conhecimento.....	8
2.2.2	Dashboards e Business Intelligence	8
2.2.3	A escolha do Power BI.....	8
2.3	A segurança e privacidade dos dados	9
2.3.1	O crescente interesse na segurança e privacidade da informação	9
2.3.2	Pilares da Segurança de Dados	11
2.3.3	Sistemas Identity and Access Management	11
3	Processo AS IS de Monitorização de Acessos Lógicos	13
3.1	A gestão de acessos na NOS	13
3.2	A Monitorização dos Acessos Lógicos na NOS	13
3.3	Circularização de Acessos Críticos.....	13
3.3.1	Mapeamento do Processo	14
3.3.2	Indicadores Utilizados.....	20
3.3.3	Conclusões.....	22
3.4	Monitorização de Acessos Remotos	23
3.4.1	Mapeamento do Processo	23
3.4.2	Indicadores Utilizados.....	29
3.4.3	Conclusões	29
3.5	Conclusões gerais sobre a Monitorização de Acessos Lógicos.....	30
4	Processo TO BE de Monitorização de Acessos Lógicos.....	31
4.1	Mapeamento do Processo	31
4.2	Fluxo de Dados	33
5	Implementação do processo	35
5.1	Desenvolvimento do Processo de Recolha e Tratamento de Dados	35
5.1.1	Automatismos para o Acesso aos Dados	35
5.1.2	Estrutura de Dados em Power BI	38
5.1.3	Importação e transformação de dados com o Power Query.....	39
5.2	Desenvolvimento dos Dashboards.....	39
5.2.1	Dashboard 1 – Âmbito	40
5.2.2	Dashboard 2 – Acessos Críticos.....	41
5.2.3	Dashboard 3 – Conformidade de Acessos Críticos	42
5.2.4	Dashboard 4 - Acessos Remotos – Atribuição	42
5.2.5	Dashboard 5 - Acessos Remotos – Utilização.....	43
5.2.6	Dashboard 6 - Conformidade de Acessos Remotos.....	44
5.2.7	Dashboard 7 – Conformidade entre o sistema IAM e o sistema de acessos remotos	45
5.2.8	Dashboard 8 – Gestão de Pendências	46
5.3	Execução	46
5.3.1	Configuração das Ferramentas	46
5.3.2	Recolha e tratamento de Dados	47

5.3.3	Utilização do Dashboard.....	47
6	Conclusões e perspectivas de trabalho futuro.....	48
	Referências	50
7	ANEXO A: Processo AS IS	52
8	ANEXO B: Processo TO BE	90
9	ANEXO C: Manual de Execução	100
10	ANEXO D: Programa em VBA para agregação de dados de utilização.....	109

Siglas

ARC – Auditoria, Risco e Compliance

AS – Auditoria de Sistemas

BI – Business Intelligence

CAC – Circularização de Acessos Críticos

CCM – Compliance Corporativa e Monitorização

CLM – Centralized Log Management

ERM – *Enterprise Risk Management*

IAM – *Identity and Access Management*

KPI – *Key Performance Indicator*

MAR – Monitorização de Acessos Remotos

RC – Risco & Compliance

RGPD – Regulamento Geral da Proteção de Dados

RGU – Unidades Geradoras de Receita (*Revenue Generating Units*)

ROI – *Return on Investment*

S&P – Segurança & Privacidade

SIEM - Security Information and Event Management

SQL – Structured Query Language

VBA – Visual Basic for Applications

Índice de Figuras

Figura 1 - Empresas NOS.....	2
Figura 2 - Estrutura da Direção de ARC	3
Figura 3 - Processo AS IS e TO BE	5
Figura 4 - Dimensões da <i>Big Data</i> (Sagiroglu e Sinanc 2013)	7
Figura 5 - <i>Gartner Magic Quadrant for Analytics and Business Intelligence Platforms</i> (Gartner 2022).....	9
Figura 6 - Processo AS IS CAC - 1º nível.....	15
Figura 7 - Processo AS IS CAC - Recolha e tratamento da informação	16
Figura 8 - Fluxo de Dados AS IS CAC	17
Figura 9 - Processo AS IS CAC - Criação / Atualização dos Dashboards.....	18
Figura 10 - Processo AS IS CAC - Validação ou remoção de acessos	19
Figura 11 - Processo AS IS CAC - Elaboração do Relatório	20
Figura 12 - Dashboard CAC AS IS (1).....	21
Figura 13 - Dashboard CAC AS IS (2).....	21
Figura 14 - Dashboard CAC AS IS (3).....	22
Figura 15 - Processo AS IS MAR - 1º nível.....	23
Figura 16 - Processo AS IS MAR - Recolha e tratamento da informação	25
Figura 17 - Fluxo de Dados AS IS MAR	26
Figura 18 - Processo AS IS MAR - Melhoria dos Dashboards	27
Figura 19 - Processo AS IS MAR - Análise e validação de resultados.....	28
Figura 20 - Processo AS IS MAR - Elaboração do Relatório	29
Figura 21 - Processo TO BE de Melhoria dos Dashboards.....	32
Figura 22 - Processo TO BE de Execução do Controlo	32
Figura 23 - Fluxo de Dados TO BE.....	34
Figura 24 - Ficheiros de Dados em Excel.....	35
Figura 25 - Programa VBA para acessos a relatórios da Base da Dados	36
Figura 26 - Pastas OneDrive.....	36
Figura 27 - Regras no Outlook	37
Figura 28 - Fluxo do <i>Power Automate</i>	37
Figura 29 - Programa VBA para converter .csv em .xls.....	38
Figura 30 - Estrutura de Dados.....	39
Figura 31 - Dashboard 1 - Âmbito	40
Figura 32 - Power BI - Cálculo da Evolução do Indicador X	41
Figura 33 - Power BI - Determinação da seta a aplicar ao Indicador X.....	41
Figura 34 - Dashboard 2 – Acessos Críticos	41
Figura 35 - Dashboard 3 - Conformidade de Acessos Críticos	42

Figura 36 - Dashboard 4 - Acessos Remotos – Atribuição	43
Figura 37 - Dashboard 5 - Acessos Remotos – Utilização	43
Figura 38 - Dashboard 6 - Conformidade de Acessos Remotos	44
Figura 39 - Dashboard 7 – Conformidade entre o sistema IAM e o sistema de acessos remotos	45
Figura 40 - Dashboard 8 - Gestão de Pendências	46
Figura 41 - Exemplo de <i>use cases</i> para os Acessos Críticos	47
Figura 42 - VBA para Agregar Dados de Utilização (1/5).....	109
Figura 43 - VBA para Agregar Dados de Utilização (2/5).....	109
Figura 44 - VBA para Agregar Dados de Utilização (3/5).....	110
Figura 45 - VBA para Agregar Dados de Utilização (4/5).....	110
Figura 46 - VBA para Agregar Dados de Utilização (5/5).....	110

1 Introdução

1.1 Enquadramento do projeto

No século III a.C., acreditava-se que a Biblioteca de Alexandria possuía a totalidade do conhecimento humano até à data. Em 2013, de acordo com o artigo “The Rise of Big Data”, a quantidade de informação existente, *per capita*, era 320 vezes a armazenada nessa biblioteca, num total de 1200 exabytes (10^{18} bytes). Este artigo informa ainda que quantidade de informação tem vindo a duplicar aproximadamente a cada 3 anos (Cukier e Mayer-Schoenberger 2013). Mais recentemente, em 2017, a IBM afirmou que 90% dos dados tinham sido criados nos últimos 2 anos, demonstrando um aumento do crescimento verificado em 2013 (IBM Marketing Cloud 2017).

Por um lado, esta evolução criou a necessidade de utilizar mecanismos de *Business Intelligence* (BI) que permitam visualizar mais facilmente os dados, através da criação de Dashboards interativos e visualmente mais intuitivos. Estes Dashboards permitem expor os dados agregados na forma de tendências, ocorrências, correlações ou variações, para que destes seja possível extrair qualquer informação ou conclusão (Pauwels 2009).

Por outro lado, a informação tornou-se num dos ativos mais importantes das organizações, independentemente do setor de atividade (Colaps 2017). Por este motivo, garantir a segurança dos dados é agora uma atividade essencial na gestão de risco de qualquer empresa. Para o fazer, para além de garantir a integridade dos sistemas informáticos, é necessário fazer uma gestão de acessos adequada, garantindo que os trabalhadores da empresa apenas têm acesso a dados essenciais à realização das suas funções. Isso é garantido através da monitorização contínua (com possível recurso a ferramentas de BI) dos dados armazenados pelos sistemas *Identity and Access Management* (IAM) das empresas, detetando *outliers* e acessos efetuados de forma pouco comum, e analisando posteriormente cada caso (Ion-Petru, Alexandru e Ecaterina 2015).

O presente projeto, no âmbito da Dissertação de Mestrado em Engenharia e Gestão Industrial, foi realizado no grupo NOS enquanto membro da equipa de Compliance Corporativa e Monitorização (CCM), inserida na área de Risco & Compliance (RC), sob a direção de Auditoria, Risco e Compliance (ARC). O projeto consistiu na melhoria do processo de obtenção, tratamento, preservação e apagamento da informação necessária para a gestão de acessos e no desenvolvimento de Dashboards que permitissem identificar acessos indevidamente atribuídos.

1.2 O grupo NOS

O grupo NOS apresenta-se como o maior grupo de comunicações e entretenimento em Portugal, tendo sido fundado em 2013 após a fusão da Optimus com a ZON. Em 2021 foram registados 1 430 milhões de euros de receita e um lucro de 144,2 milhões de euros. O grupo é constituído pela empresa *holding* NOS SGPS e pelas várias subsidiárias, organizadas de acordo com a

atividade, como a NOS Comunicações e a NOS Lusomundo Cinemas, ou a localização, como a NOS Açores e a NOS Madeira, como se pode observar na Figura 1.



Figura 1 - Empresas NOS

Das fontes de receita do grupo destacam-se os serviços de telecomunicações fixa e móvel, os cinemas, a distribuição de audiovisuais e outras receitas provenientes de *joint-ventures*. Deste modo, podem ser definidas 3 áreas de negócio: *Telecom*, *Media & Entertainment* e *Joint-Ventures*.

Na área das telecomunicações, a NOS possui 10,31 milhões de unidades geradoras de receita (RGUs). Destes, 5,35 milhões são clientes móveis, 1,65 milhões são clientes de televisão, 1,78 milhões são clientes de telefone fixo e 1,49 milhões são clientes de internet de banda larga fixa (NOS 2021).

Na área *Media & Entertainment*, destacam-se as 208 salas de cinema em Portugal que registam cerca de 60% das quotas de mercado nacional, tornando a NOS no líder nacional deste segmento. Em 2019, registou-se a venda de 9,27 milhões de bilhetes de cinema, a um preço médio de 5,20€. Em 2020, devido à pandemia, a venda de bilhetes foi reduzida para 2,31 milhões, registando 0 vendas no 2º trimestre devido ao encerramento dos cinemas. Esta área está agora em recuperação, não se esperando que supere os valores de 2019 num futuro próximo.

Por fim, a área das *Joint-Ventures* representa outros negócios, não operados diretamente pelo grupo. Destas destacam-se a DREAMIA, a ZAP e a Sport TV. A DREAMIA é detida, em partes iguais, pela NOS e pela AMC e produz 5 canais distribuídos pela AMC Networks International Southern Europe: Panda, Biggs, Canal Hollywood, Casa e Cozinha e Blast (Dreamia 2022). A ZAP, detida a 30% pela NOS, é o maior operador de TV por Satélite em Angola, sendo ainda provedor de internet e de cinemas e estando também presente em Moçambique (ZAP 2022). Por fim, a Sport TV, detida pela NOS, pela MEO, pela Vodafone e pela Olivedesportos em partes iguais, opera canais de televisão inteiramente dedicados à transmissão de conteúdos desportivos, em Portugal.

Distinguida, de forma recorrente, com prémios como o “Produto do Ano”, “Marca de Confiança” e “Escolha do Consumidor”, a NOS tem quotas de mercado entre os 27,2% e os

38,8% nos vários serviços de telecomunicação prestados (ANACOM 2022). Foi ainda distinguida durante 5 anos consecutivos nos prémios EMEA Contact Center World como melhor serviço ao cliente.

Numa perspetiva financeira, a NOS é uma das empresas com maior capitalização bolsista em Portugal, estando integrada no PSI (*Portuguese Stock Index*). A sua estrutura acionista compreende a Zopt SGPS com 52,15% do capital, a Sonae SGPS com 7,38% e a Mubadala Investment Company PJSC com 5,00%. É ainda de notar que a Sonae SGPS detém 50% da Zopt SGPS, possuindo, por isso, uma participação indireta na NOS de 26,075%, totalizando 33,455% (NOS 2022).

Nos últimos anos, a NOS tem adotado a abordagem de investimento ético, sustentável e socialmente responsável ESG (*Environmental, Social and Corporate Governance*), comprometendo-se a gerar valor não só para os acionistas, mas para todos os *stakeholders*, nomeadamente para os clientes, colaboradores, parceiros e para a sociedade e o planeta, de forma mais geral. Entre outros compromissos, a NOS assumiu aumentar a eficiência energética das suas operações, utilizar fontes renováveis de energia e reduzir a pegada de carbono, direta e indireta.

1.3 Compliance Corporativa e Monitorização

A direção de Auditoria, Risco e Compliance (ARC) tem como objetivo a gestão eficaz dos riscos da NOS, mantendo a informação de riscos atualizada e alinhada com o negócio e com a envolvente externa. A direção é constituída por 3 áreas: Auditoria de Processos (AP), Auditoria de Sistemas (AS) e Risco & Compliance (RC), de acordo com a Figura 2.

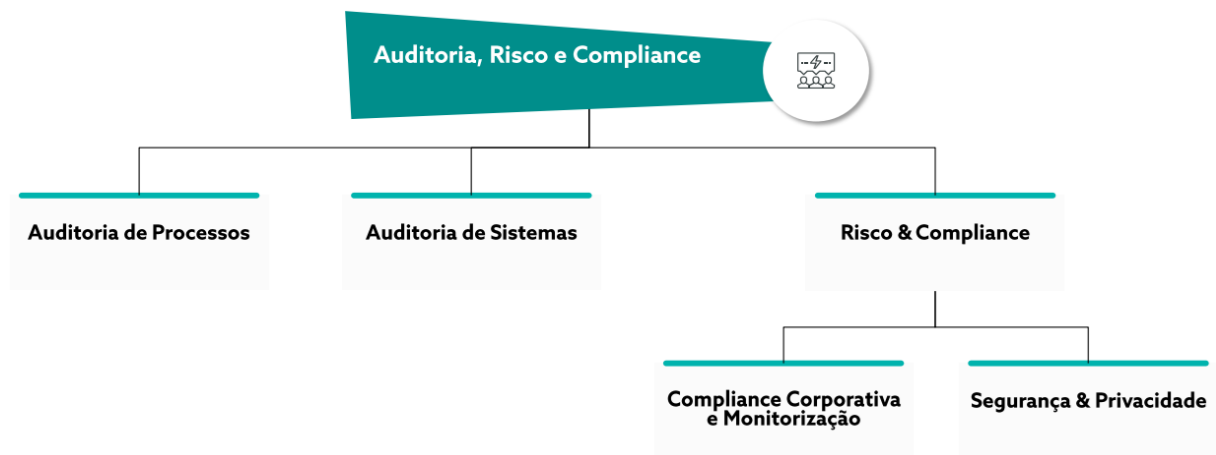


Figura 2 - Estrutura da Direção de ARC

AP e AS exercem a função de Auditoria Interna. Esta função tem como objetivo a avaliação independente da exposição aos riscos dos processos de negócio e dos sistemas de informação e de telecomunicações da NOS e a proposta de soluções de melhoria dos controlos, procurando uma gestão mais eficaz dos riscos de negócio. São ainda responsáveis por monitorizar a evolução do estado dos principais riscos detetados, bem como suportar o comité de ética e assessorar o esclarecimento de dúvidas ou investigar a manifestação de preocupações, tais como incidentes de Segurança & Privacidade.

Por sua vez, RC tem como objetivos a consciencialização, medição, controlo e gestão dos riscos de negócio. Para isto, são implementados controlos que aproximam o nível de risco ao

pretendido pela Comissão Executiva da NOS, e é feito o suporte às diversas áreas da empresa com ferramentas e metodologias para a efetiva mitigação dos riscos.

A área de RC é constituída por duas equipas: Segurança & Privacidade (S&P) e Compliance Corporativa e Monitorização (CCM). RC é responsável por garantir que são cumpridas as obrigações de empresas cotadas em bolsa, bem como os programas de Gestão de Riscos Corporativos (ERM – *Enterprise Risk Management*), de Segurança & Privacidade e os requisitos normativos e legais que a NOS subscreve ou às quais está sujeita. RC é também responsável por assegurar os processos de certificação ISO 27k, ISO 20k, ISO 14k, ISO 9k e ISO 45k e por possibilitar a sua avaliação por auditores internos e/ou externos.

A equipa de S&P assegura o governo da Segurança & Privacidade na NOS e avalia o impacto de alterações de contexto legislativo e regulatório na exposição ao risco. Sempre que necessário, sinaliza a importância de criar ou alterar iniciativas para a gestão desses riscos.

Por fim, a equipa de CCM, que integrei durante a realização do projeto, para além da gestão da compliance corporativa, monitoriza o desvio em relação à tolerância de risco estabelecida, detetando e alertando para situações anómalas, indiciadoras de risco acrescido. Deste modo, é responsável pela monitorização dos acessos lógicos críticos, das compras, dos planos de gestão de crise e do cumprimento dos direitos do cliente no âmbito do Regulamento Geral sobre a Proteção de Dados (RGPD), entre outros.

1.4 Objetivos do projeto

O projeto tem como objetivo a transformação e melhoria dos processos de acesso a informação, manutenção e apagamento relativos a dois controlos existentes na empresa: a Circularização de Acessos Críticos (CAC) e a Monitorização de Acessos Remotos (MAR). Como é demonstrado na Figura 3, a informação referida deverá ser posteriormente integrada num Dashboard único, em Power BI, criando um controlo único, executável mensalmente: a Circularização de Acessos Contínua.

Do lado dos acessos críticos, pretende-se o desenvolvimento de um Dashboard capaz de suportar toda a comunicação entre CCM e as várias direções da empresa, dispensando emails e partilha de documentos Excel que tornam o processo lento e difícil de executar. Pretende-se ainda alargar o âmbito do controlo a toda a empresa.

Do lado dos acessos remotos, o controlo tem sido efetuado numa perspetiva de análise de capacidade dos servidores, devido à necessidade criada pela pandemia, num ambiente de trabalho remoto. Pretende-se, por isso, reorientar o foco da análise para uma perspetiva de controlo de acessos, mantendo, ainda assim, a análise de capacidade.

Pretende-se ainda criar uma análise à conformidade da atribuição de acessos com a Política de Segurança da empresa, quer para os acessos críticos quer para os acessos remotos, inexistente até agora. Esta análise deverá incidir sobre inconsistências na atribuição de acessos críticos e remotos, procurando eliminar qualquer não conformidade existente.

Por fim, e de forma a permitir que a comunicação com as direções ocorra através do Power BI, pretende-se criar uma tabela para o registo de pendências, isto é, alertas identificados pela equipa de CCM e enviados aos gestores de acesso para resolução. Estas pendências devem ser visíveis no Dashboard pelos gestores de acesso, para que as possam resolver.

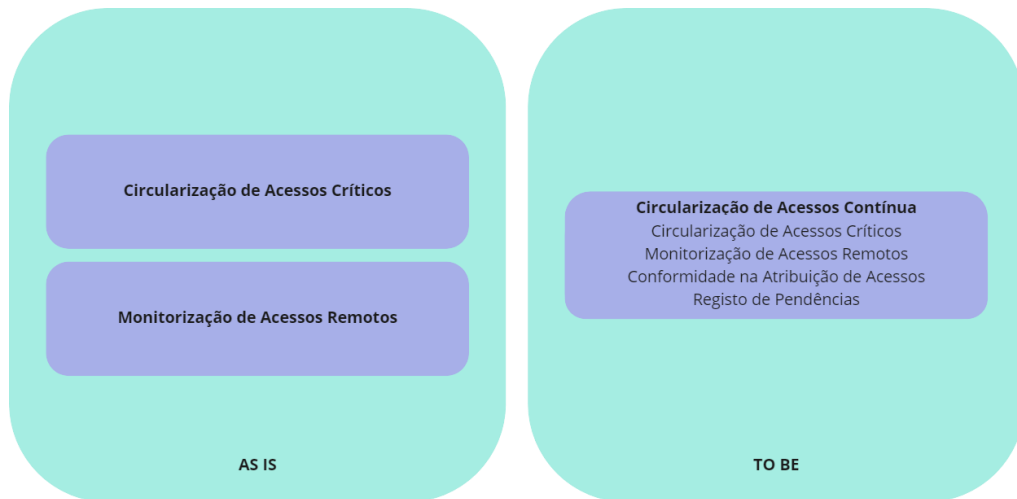


Figura 3 - Processo AS IS e TO BE

1.5 Metodologia

O projeto tem dois clientes, com diferentes características e requisitos: a equipa de CCM, integrada na direção ARC, e os gestores de acesso de todas as direções da empresa. A equipa de CCM tem a necessidade de obter informações globais que permitam inferir acerca da eficácia e eficiência da execução do controlo, atribuindo, por isso, maior relevância a dados agregados e KPI's (*Key Performance Indicators*) que transmitam uma visão geral do trabalho realizado pelos gestores de acesso das várias direções. Por sua vez, os gestores de acesso das várias direções da NOS têm a necessidade de maior detalhe, visualizando cada acesso sob a sua responsabilidade, bem como gráficos que permitam visualizar e filtrar acessos potencialmente indesejados para que possam analisar caso a caso e, sempre que haja necessidade, remover ou alterar acessos no sistema IAM.

Deste modo, e atendendo às diferenças entre clientes do projeto, foram seguidos dois métodos de trabalho no contacto com os diferentes clientes.

Perante a direção de ARC, reuniu-se, diariamente, com a equipa de CCM e a cada duas semanas, com o responsável da área de RC, de forma a avaliar continuamente o trabalho realizado, recolher *feedback*, rever requisitos e validar desenvolvimentos efetuados.

Por sua vez, perante as restantes direções, iniciou-se o projeto com a análise do processo AS IS e com a definição dos requisitos do Dashboard. Para isso, foram realizadas reuniões com 4 das direções com maior número de acessos críticos na empresa. Nestas reuniões questionou-se quais as principais funcionalidades que estas direções gostariam de ver implementadas no novo Dashboard de gestão de acessos. Ainda nas reuniões, foram identificadas ineficiências na execução do processo atual.

Após a definição dos requisitos, foi desenhado o modelo do processo TO BE. Neste foram definidos os principais objetivos de melhoria. Ao nível do processo priorizou-se uma maior automatização do processo de gestão de informação. Ao nível do Dashboard decidiu-se a incorporação de gráficos e indicadores, de acordo com as necessidades das direções. E, por fim, no contacto entre CCM e as direções definiu-se que o email não seria eficiente e deveria, por isso, ser procurada uma alternativa.

Em seguida, iniciou-se o desenvolvimento do novo processo e de todos os programas de suporte a este. Foi utilizado o Power Automate na automatização da recolha de ficheiros recebidos diariamente por email. Utilizou-se VBA (*Visual Basic for Applications*) de forma a executar,

mensalmente, a agregação de dados provenientes de diversas fontes. Como ferramenta de Business Intelligence (BI) utilizou-se o Power BI.

Por fim, executou-se, no mês de Junho, um piloto que envolveu as 4 direções que colaboraram na definição dos requisitos, efetuando-se os ajustes necessários, mediante o *feedback* recebido. Não se tendo verificado dificuldades de maior relevância durante a execução do piloto, o processo será implementado na empresa, sendo executado mensalmente, a partir de julho, envolvendo todas as direções da NOS.

1.6 Estrutura da dissertação

A dissertação será iniciada, no capítulo 2, por uma revisão do estado da arte, com uma breve descrição do conceito de *Big Data*, abordando, em seguida, a utilização de Dashboards como método de visualização de dados. Por fim, abordam-se conceitos relativos à proteção de dados e privacidade.

Em seguida, no capítulo 3, é feita a descrição AS IS do processo de execução da Circularização de Acessos Críticos e da Monitorização de Acessos Remotos, descrevendo ineficiências e oportunidades de melhoria. Feita a análise AS IS, é proposta uma melhoria, no capítulo 4, mapeando o processo TO BE e detalhando as fontes de dados.

É, então, iniciada a descrição da implementação do novo processo, no capítulo 5, detalhando o processo de recolha e tratamento de dados e os programas de suporte desenvolvidos, o desenvolvimento dos Dashboards e as instruções para a execução de todo o processo.

Por fim, no capítulo 6, são avaliadas oportunidades de melhoria futura no processo de Circularização de Acessos Contínua.

2 Estado da Arte

2.1 Big Data

Até 2003, o ser humano criou 5 exabytes (10^{18} bytes) de dados. Em 2013, esta quantidade era criada a cada dois dias (Sagiroglu e Sinanc 2013), prevendo-se que a quantidade total de dados seria de mais de 30 zettabytes (10^{21} bytes) em 2020 (Furht e Villanustre 2016). O conceito de *Big Data* surge quando a complexidade das bases de dados aumenta de tal forma que as ferramentas tradicionais de análise de dados perdem a capacidade de lidar com essa complexidade de forma eficiente. Tal acontece em bases de dados demasiado grandes, com inúmeros campos/colunas, com uma quantidade de entradas/linhas sempre em crescimento e cujos campos apresentam uma considerável variabilidade de formatos (Oussous, et al. 2018).

Deste modo, as 3 principais características destes dados são a variedade, o volume e a velocidade, como se observa na Figura 4 - Dimensões da *Big Data* (Sagiroglu e Sinanc 2013) Figura 4. A variedade está relacionada com a diversidade e quantidade de fontes de dados, bem como os formatos dos dados, que podem ser de 3 tipos: estruturados, não estruturados e semiestruturados. Os dados estruturados são aqueles que podem ser facilmente filtrados e agrupados de forma a serem analisados, como números ou entradas de texto predefinido. Por sua vez, os dados não estruturados representam texto variável, de inserção livre e, por isso, muito difíceis de tratar. Por fim, os dados semiestruturados não apresentam texto predefinido, no entanto, permitem algum agrupamento de dados devido a alguns padrões de texto existentes (Sagiroglu e Sinanc 2013). O volume advém da quantidade de dados criados, armazenados e processados atualmente que, como indicado anteriormente, tem estado em constante crescimento, chegando a valores aproximados de 97 zettabytes (10^{21} bytes) em 2022 (Tredinnick 2022). Por fim, a velocidade relaciona-se com a quantidade de dados transmitidos por unidade de tempo nas empresas, criando fluxos de dados de alta velocidade, muitas vezes em tempo real.

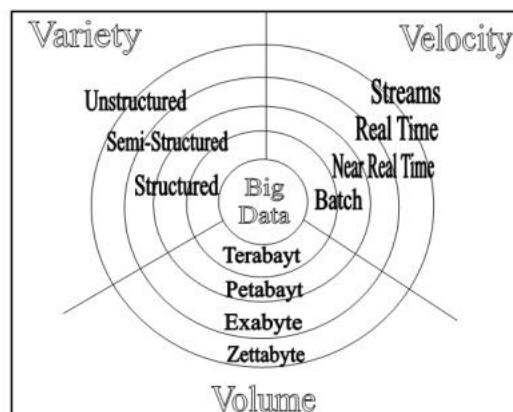


Figura 4 - Dimensões da *Big Data* (Sagiroglu e Sinanc 2013)

O processamento de dados divide-se em 5 fases (Agrawal, et al. 2011):

1. Aquisição e armazenamento de dados
2. Limpeza e extração de informação
3. Integração de dados, agregação e representação
4. Consulta, modelação e análise de dados
5. Interpretação

Geralmente, numa empresa, as fases 1 e 2 são realizadas pelas áreas tecnológicas, responsáveis pela gestão das bases de dados. Por sua vez, as fases 3 e 4 ocorrem ao nível do apoio à gestão, enquanto a fase 5 é desempenhada pelas direções.

2.2 Visualização de dados através de Dashboards

2.2.1 Dados, Informação e Conhecimento

“An ounce of information is worth a pound of data. An ounce of knowledge is worth a pound of information. An ounce of understanding is worth a pound of knowledge.” (Ackoff 1989)

Segundo Ackoff (1989), dados representam propriedades de objetos e eventos, enquanto informação consiste em dados processados. Por sua vez, a informação representa também propriedades de objetos e eventos, mas de forma mais compacta. Assim, os dados, por si só, são inúteis, adquirindo alguma utilidade aquando do seu processamento, tornando-se informação. Ainda assim, esta informação pouca utilidade terá se não for transformada em conhecimento, que produz instruções e desenvolve métodos de execução (“como fazer?”) que promovem a melhoria da eficiência de um processo, e em sabedoria, que permite uma melhor análise estratégica dos processos (“porquê?”) promovendo o seu desenvolvimento e a sua maior eficácia. Denota-se ainda que a eficiência de um processo está associada ao desempenho da sua execução, executando bem o processo de um ponto de vista tático, enquanto a eficácia está associada à execução dos processos corretos para fazer face a um dado problema ou necessidade, de um ponto de vista estratégico (Ackoff 1989).

O processamento de dados descrito no ponto anterior é, então, o processo de criação de informação com base em dados, descrito por Ackoff (1989). Para que a informação produzida neste processo seja facilmente interpretada, é necessário, segundo Tegarden (1999), que a sua visualização permita:

- Extrair informação com base nos dados, de forma visualmente apelativa
- Obter uma visão geral dos dados
- Identificar a estrutura dos dados, bem como padrões, tendências, anomalias e relações entre estes
- Identificar áreas de interesse

Assim, a tomada de decisão é facilitada por estímulos visuais. Isso conduzirá, neste caso, a uma maior eficácia das decisões dos gestores de acesso.

2.2.2 Dashboards e Business Intelligence

Em 2006, o matemático Clive Humby cunhou a famosa expressão: “Data is the new oil.” Mais tarde, Michael Palmer acrescentou: “Data is just like crude. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so must data be broken down, analysed for it to have value.” Isto vem confirmar a mensagem de Ackoff, reforçando que para obter verdadeiro conhecimento, é essencial processar os dados e, posteriormente, analisar a informação.

Nos processos diários de qualquer empresa, são produzidas quantidades enormes de dados, com um grande valor escondido, mas este valor apenas pode ser extraído, transformando esses dados em conhecimento. Para o fazer de forma prática, foram desenvolvidas ferramentas de BI, que permitem às empresas recolher, armazenar, agregar, analisar, relatar e visualizar dados, na forma de informação, por parte do utilizador final: o *decision-maker*, que, neste caso, é o gestor de acessos (Huang 2019).

2.2.3 A escolha do Power BI

Em 2022, pelo 15º ano consecutivo, a Microsoft foi classificada como líder no *Gartner Magic Quadrant for Analytics and Business Intelligence Platforms*, destacando o seu software Power BI dos concorrentes tanto na visão como na capacidade de execução. O Power BI permite

efetuar a preparação dos dados, analisar estes dados de uma forma visualmente apelativa e construir Dashboards interativos (Gartner 2022).



Figura 5 - Gartner Magic Quadrant for Analytics and Business Intelligence Platforms (Gartner 2022)

O Power BI é, então, uma ferramenta de BI, baseada na Azure Cloud, que permite agregar dados de múltiplas fontes, desde *Microsoft Sharepoints*, a *data warehouses*, ou ferramentas mais convencionais, como o Excel (Huang 2019). A importação e processamento dos dados é feita através do Power Query, uma ferramenta integrada no Power BI. Posteriormente, este software permite estabelecer relações entre as diversas fontes de dados numa lógica UML (Unified Modeling Language). Por fim, os Dashboards são construídos numa página própria, que será apresentada ao *decision-maker*.

A Microsoft permitindo a partilha dos Dashboards com todos os utilizadores de um mesmo *Workspace*, permitindo ainda definir perfis de acesso para cada utilizador. Nota-se ainda que este software é atualizado semanalmente, de forma a melhorar continuamente a experiência utilizador.

Os motivos acima descritos, aliados ao facto da NOS possuir licenças de utilização e trabalhar frequentemente com este software, asseguraram a escolha do Power BI como software de BI para o desenvolvimento dos Dashboards.

2.3 A segurança e privacidade dos dados

2.3.1 O crescente interesse na segurança e privacidade da informação

Vivemos na era digital e, com o passar dos anos, aumenta a preocupação com a segurança e a privacidade dos dados por parte do consumidor e dos governos (Presthus e Sørnum 2018). Isto tem-se traduzido num aumento da regulamentação desta área na UE, sendo de destacar a entrada em vigor do RGPD a 25 de maio de 2018 que se diferencia das diretivas que o antecedem por, pela primeira vez, estabelecer coimas para as infrações, em vez de servir apenas como uma

recomendação ou um conjunto de boas práticas a seguir. Consequentemente, as autoridades de proteção de dados dos vários países da UE viram as suas competências e capacidade de atuação reforçadas, iniciando a aplicação de coimas às empresas infratoras (Daigle e Khan 2020).

Por outro lado, as próprias empresas estão a ganhar consciência de que uma melhoria na forma como asseguram a privacidade dos seus dados, pode ter efeitos positivos nos seus resultados financeiros. A Cisco realizou um estudo que envolveu mais de 4700 profissionais de segurança digital em 25 países que relatou que, em 2020, 85% das empresas tiveram um ROI positivo relativamente às suas despesas na segurança e privacidade dos dados, tendo sido superior a 2 vezes em 35% dos casos, e, em média 1,9 vezes. Este estudo reportou ainda um aumento de 100% na despesa das empresas em privacidade face a 2019. Não menos relevante, é ter sido indicado por 79% dos inquiridos que o aumento da regulamentação teve um impacto positivo para a empresa, com apenas 5% a indicar impactos negativos (Cisco 2021).

Deste modo, a segurança dos ativos de informação demonstra-se cada vez mais de maior importância para as empresas, que investem cada vez mais no desenvolvimento de mecanismos que permitam mitigar os riscos associados à sua manutenção. No caso particular da NOS, um dos maiores riscos do negócio das telecomunicações está relacionado com a privacidade dos dados de todos os *stakeholders* da empresa. Este risco é de tal forma relevante que, no relatório e contas de 2021 pode ler-se, na página 134:

“Os riscos de privacidade assumem cada vez maior relevância, associados sobretudo aos requisitos legais e regulamentares sobre proteção de dados pessoais, facto que é transversal a todos os setores de atividade e também aplicável em particular ao setor das comunicações eletrónicas que está sujeito a regulamentação específica sobre segurança e privacidade. Existe o risco da informação sobre dados pessoais de clientes ou colaboradores não estar completamente protegida, de modo a salvaguardar os requisitos legais e o direito fundamental de cada indivíduo decidir quem deve ter acesso aos dados.” (NOS 2021)

Mais à frente, na página 134, concretizam-se ações cujo objetivo é minimizar esse risco:

“Para endereçar estes riscos, a NOS desenvolve e mantém um programa de iniciativas com o objetivo de implementar processos para Proteção de Dados Pessoais, bem como para monitorizar e melhorar continuamente a conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e com outras regulamentações com impacto na privacidade. Destacamos, como exemplos, a revisão/criação de Políticas e Regras de Privacidade, o reforço de controlos e de monitorização sobre os processos para exercício de direitos de titulares de dados pessoais pelos clientes no âmbito do RGPD, assim como o robustecimento contínuo de processos de gestão de cliente (consentimentos, autenticação, etc.). Os colaboradores e parceiros da NOS assumem obrigações de confidencialidade, de sigilo e de proteção de dados pessoais, através da assinatura de termos de responsabilidade e de acordos de tratamento de dados, assim como através da participação nas ações de sensibilização e formação sobre Segurança & Privacidade.” (NOS 2021)

2.3.2 Pilares da Segurança de Dados

De forma a garantir a privacidade e segurança dos dados dos cidadãos, surgiu o conceito de *Privacy by Design*. Este conceito consiste na implementação de princípios de privacidade dos dados na criação (*design*) dos sistemas de informação das empresas. Deste modo, é possível assegurar a privacidade e segurança dos dados sem limitar a eficiência dos sistemas (Romanou 2018).

Em 2009, Ann Cavoukian definiu 7 princípios fundamentais deste conceito. Desde então, estes 7 princípios servem de referência na construção dos mais diversos sistemas de informação. Em seguida serão descritos estes princípios: (Cavoukian 2009)

1. “Proativa não Reativa; Preventiva não Corretiva”
 - A privacidade deve ser garantida de forma preventiva e proativa, não procurando remediar infrações, mas sim impedir que estas ocorram.
2. “Privacidade como Padrão”
 - Os dados devem estar, por definição, protegidos, sem que seja necessário efetuar qualquer ação para que tal aconteça. Essa proteção deverá ser garantida pelo sistema de informação.
3. “Privacidade Incorporada no *Design*”
 - A privacidade deve estar integrada no sistema e não ser uma funcionalidade do sistema. A privacidade deve ser, por isso, uma componente integrada em qualquer funcionalidade do sistema.
4. “Funcionalidade Completa - Soma Positiva, não Soma Zero”
 - A garantia da privacidade deve garantir o cumprimento de todos os objetivos do sistema, sem prejudicar a sua eficiência e, de preferência, melhorando-a.
5. “Segurança de ponta a ponta – Proteção do ciclo de vida”
 - A privacidade deve ser garantida em todas as etapas do processo, desde a sua aquisição até à sua destruição.
6. “Visibilidade e Transparência”
 - O sistema deverá permitir a qualquer parte interessada a verificação independente da sua segurança e privacidade.
7. “Respeito pela Privacidade do Utilizador”
 - O *design* do sistema deve ser pensado com foco no utilizador.

Por sua vez, Samonas e Coss referem como pilares da segurança de dados a confidencialidade, a integridade e a disponibilidade. A confidencialidade garante que os dados apenas são cedidos por quem tem autorização para tal, prevenindo o acesso não autorizado aos dados. Associada à confidencialidade está a privacidade que assegura a proteção da informação, em especial dos dados pessoais dos clientes, colaboradores ou outros. A integridade salvaguarda a exatidão e consistência dos dados, prevenindo a sua modificação, perda ou eliminação acidental ou não autorizada. Associada à integridade está o conceito de não repúdio, que garante que é possível verificar a ocorrência de um evento, bem como identificar inequivocamente o responsável por qualquer operação ou comunicação. Por fim, a disponibilidade assegura o acesso aos dados sempre que necessário, sem demoras indevidas. Associado à disponibilidade estão os conceitos de retenção e resiliência. A retenção assegura que os dados são conservados apenas pelo tempo necessário para o negócio e permitido por lei. A resiliência assegura que os ativos de suporte à informação têm a capacidade de resistir a um incidente e de continuar a disponibilizar os dados (Samonas e Coss 2014).

2.3.3 Sistemas Identity and Access Management

Num contexto de *Big Data*, o acesso a dados deve ser gerido por um sistema de controlo forte que negue qualquer tipo de acesso indevido (Gahi, Guennoun e Mouftah 2016). Neste sentido,

e de forma a assegurar o cumprimento dos vários princípios enumerados no capítulo anterior, as empresas utilizam sistemas de gestão de identidades e acessos (IAM). Estes sistemas têm a finalidade de cumprir e fazer cumprir as políticas e procedimentos de segurança das empresas. Através destes sistemas é possível saber quem tem acesso a que informação e se os acessos atribuídos são apropriados às funções de cada colaborador, monitorizando, de forma apropriada, os acessos e atividades de cada utilizador (Madureira 2010). Assim, um sistema IAM é o *software* onde se efetua a gestão de identidades e a gestão de acessos.

A gestão de identidades é constituída pelos processos de criação, suspensão e inativação de utilizadores, bem como por qualquer alteração efetuada às características de cada utilizador. Por sua vez, a gestão de acessos corresponde ao processo de atribuir ou revogar permissões de acesso a recursos da empresa. De forma a garantir a segurança da informação e minimizar o risco para a empresa, deve ser seguido o “princípio de acessos mínimos”, que indica que apenas devem ser atribuídos os acessos necessários ao desempenho da função de cada utilizador (Madureira 2010).

3 Processo AS IS de Monitorização de Acessos Lógicos

3.1 A gestão de acessos na NOS

No âmbito dos sistemas de informação da NOS, é definido como utilizador qualquer colaborador ou prestador de serviços do grupo NOS registados no sistema IAM (*Identity and Access Management*) da NOS através de um identificador único: *username*.

O sistema IAM é a ferramenta transversal da NOS onde é feito o registo das Identidades e a gestão dos seus acessos lógicos. As identidades podem ser de 4 tipos: interna, externa, aplicacional e *non-worker*, dependendo da forma como se relacionam com a empresa, assim como da morfologia do utilizador. Podem estar num de 4 estados: ativo, suspenso por prova de vida, suspenso e inativo.

No sistema IAM, a cada utilizador estão associadas as posições que este ocupa e as permissões associadas a cada posição, de cada utilizador. Embora geralmente um utilizador ocupe apenas uma posição, este poderá ocupar qualquer número de posições.

Cada par posição-permissão é definido como acesso. A um utilizador poderão ser atribuídas várias permissões, correspondendo, por isso, a vários acessos. Um acesso pode ser atribuído de duas formas: ao perfil ou à identidade. Uma atribuição ao perfil é genérica e transversal a todos os utilizadores que desempenham determinada função. Por outro lado, uma atribuição à identidade é feita individualmente para cada utilizador, permitindo controlar de forma mais eficaz permissões mais críticas. Para que os acessos estejam ativos, o utilizador tem que estar no estado ativo. Caso contrário, os acessos não serão válidos.

O gestor de acessos é o responsável pelos processos de gestão de acessos lógicos das posições existentes na sua direção, sendo designado pelo diretor. Caso este não designe ninguém para a função de gestor de acessos, ele próprio cumprirá essa função.

Por sua vez, os processos de gestão de acessos lógicos têm como propósito garantir a aplicação de regras que visam reduzir os riscos associados ao acesso não autorizado, erro humano, fraude ou má utilização dos acessos aos sistemas de informação da NOS, minimizando o impacto de incidentes e falhas de segurança. Estes processos são regularmente monitorizados pela direção de ARC.

3.2 A Monitorização dos Acessos Lógicos na NOS

A monitorização dos acessos lógicos serve para garantir a correta execução dos processos de gestão de acessos lógicos, intervindo e corrigindo qualquer situação anómala, potencialmente geradora de um risco acrescido. Assim, de forma a proteger a privacidade dos clientes, garantindo a segurança dos ativos de informação e a continuidade do negócio, são regularmente efetuados dois controlos à atribuição e à utilização de acessos lógicos: um incide sobre acessos críticos e outro sobre acessos remotos.

Estes dois controlos têm objetos de estudo, destinatários e bases de dados semelhantes, pelo que deverá ser possível explorar sinergias e melhorar o desempenho do processo de monitorização, agregando estes controlos numa ferramenta única.

3.3 Circularização de Acessos Críticos

Um acesso crítico é qualquer acesso lógico com privilégios de consulta a dados pessoais sensíveis e devem ser, regra geral, atribuídos à identidade. As categorias de acessos críticos são:

- Acesso a dados tráfego de comunicações
 - Através dos sistemas de gestão de cliente e gestão de faturação
- Acesso a gravações de chamadas de *contact centers*
 - Através dos sistemas de gravação de chamadas
- Acesso que permite o apagamento de dados a pedido do cliente
 - Através do sistema de gestão de pedidos de apagamento de dados

De forma a garantir o cumprimento do princípio *need-to-know*, que determina que apenas devem ter acesso a estes dados os utilizadores que deles necessitam para o desempenho das suas funções, a CAC identifica os acessos definidos como críticos pela área de Privacidade & Segurança. Destes são sinalizados aqueles que deverão ser eliminados, por serem redundantes ou desnecessários à execução das funções exercidas por cada um dos utilizadores. Nos casos em que os acessos são necessários, é requerida uma justificação para a sua manutenção, de forma a assegurar que o acesso é efetivamente necessário. Nos casos os acessos são desnecessários ou atribuídos de forma incorreta, é acompanhado e monitorizado o processo de correção.

Historicamente, este controlo era efetuado anualmente pela equipa de CCM, suportado pela análise individualizada de cada fonte de dados em Excel e pelo envio de emails às direções com alertas identificados por CCM na sua análise. O processo de circularização, demonstrava-se lento, difícil de executar e com um âmbito restrito a apenas algumas direções, devido à dificuldade de executar o processo de forma mais abrangente.

Mais recentemente, numa tentativa de agilizar este processo, iniciou-se a utilização do Power BI para apresentar Dashboards com alertas às direções. Estes Dashboards servem para análise dos gestores de acesso, que passam, com esta modificação, a adquirir maior autonomia.

Neste processo, CCM envia um email com o Dashboard aos gestores de acessos das direções a circularizar. Ao receber o email, os gestores de acessos exportam um ficheiro Excel no qual registam justificações individuais para a manutenção de cada acesso a manter ou se propõem a removê-los. Estas justificações são enviadas como resposta ao email da equipa de CCM. Depois de receber as respostas, CCM é responsável por atualizar os Dashboards e rever todas as justificações dadas e assegurar que os acessos não justificados são removidos pelos gestores de acesso.

3.3.1 Mapeamento do Processo

Para uma melhor perceção do processo, foi desenhado o fluxograma apresentado na Figura 6. Trata-se de um fluxograma de 1º nível, que define a sequência de subprocessos necessária para a execução do processo AS IS de CAC.

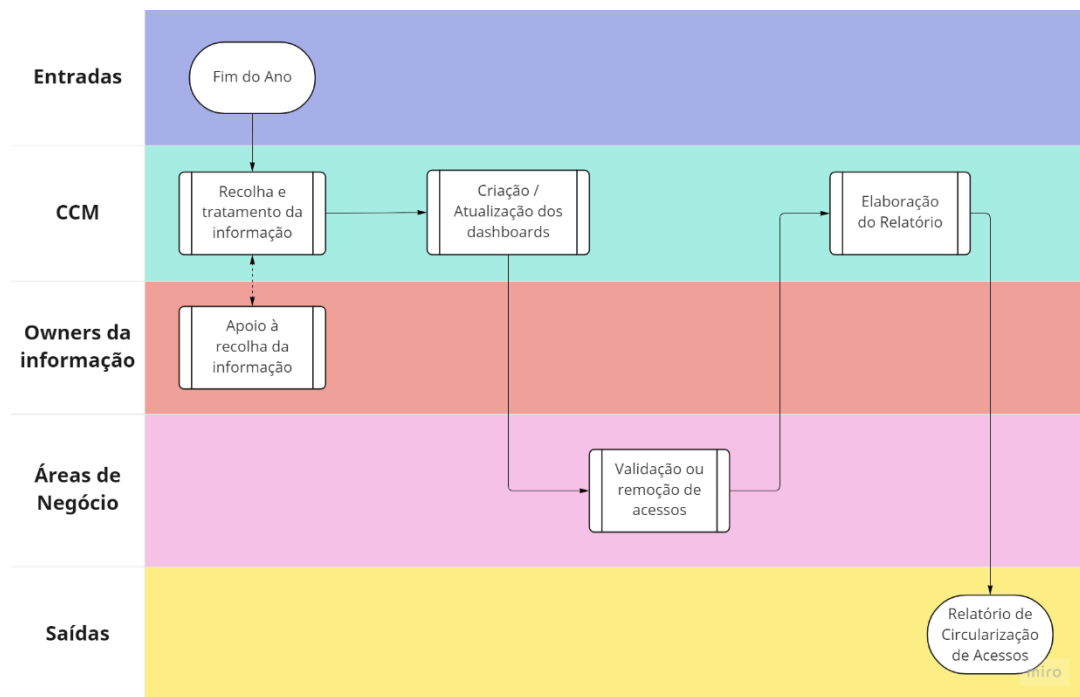


Figura 6 - Processo AS IS CAC - 1º nível

Como se pode verificar, o processo é iniciado, anualmente, por CCM, com a recolha e tratamento da informação. Esta recolha é suportada pelas áreas tecnológicas da empresa.

Como o processo é anual, e só se começou a utilizar Power BI na última CAC, é previsível a alteração significativa das necessidades dos clientes do Dashboard. Deste modo, a Criação / Atualização dos Dashboards é uma etapa necessariamente inserida no processo e ocorre logo após a recolha e tratamento da informação.

Estando os Dashboards criados ou atualizados, são enviados, por email para as várias áreas de negócio. Aí, os gestores de acessos revêm e justificam ou apagam os acessos.

Por fim, é elaborado um relatório. Este relatório tem o formato PowerPoint, com base na informação presente no Power BI, depois de atualizada com as respostas das áreas.

Em seguida, serão mapeados os subprocessos, e definidas, em fluxogramas de 2º nível, as atividades desempenhadas em cada subprocesso. Estas atividades encontram-se mais detalhadas no ANEXO A: Processo AS IS.

Recolha e tratamento da informação

Neste subprocesso, cujas atividades se encontram definidas na Figura 7, ocorre a recolha e preparação da informação necessária ao desenvolvimento dos Dashboards. Como o processo ocorre anualmente e, neste período, geralmente existem variações consideráveis na forma de acesso à informação ou nos requisitos dos gestores de acesso e de ARC, é necessário definir previamente os requisitos, com o apoio das áreas de negócio envolvidas. Nesta etapa, é produzido um documento com os requisitos e um plano de execução do controlo.

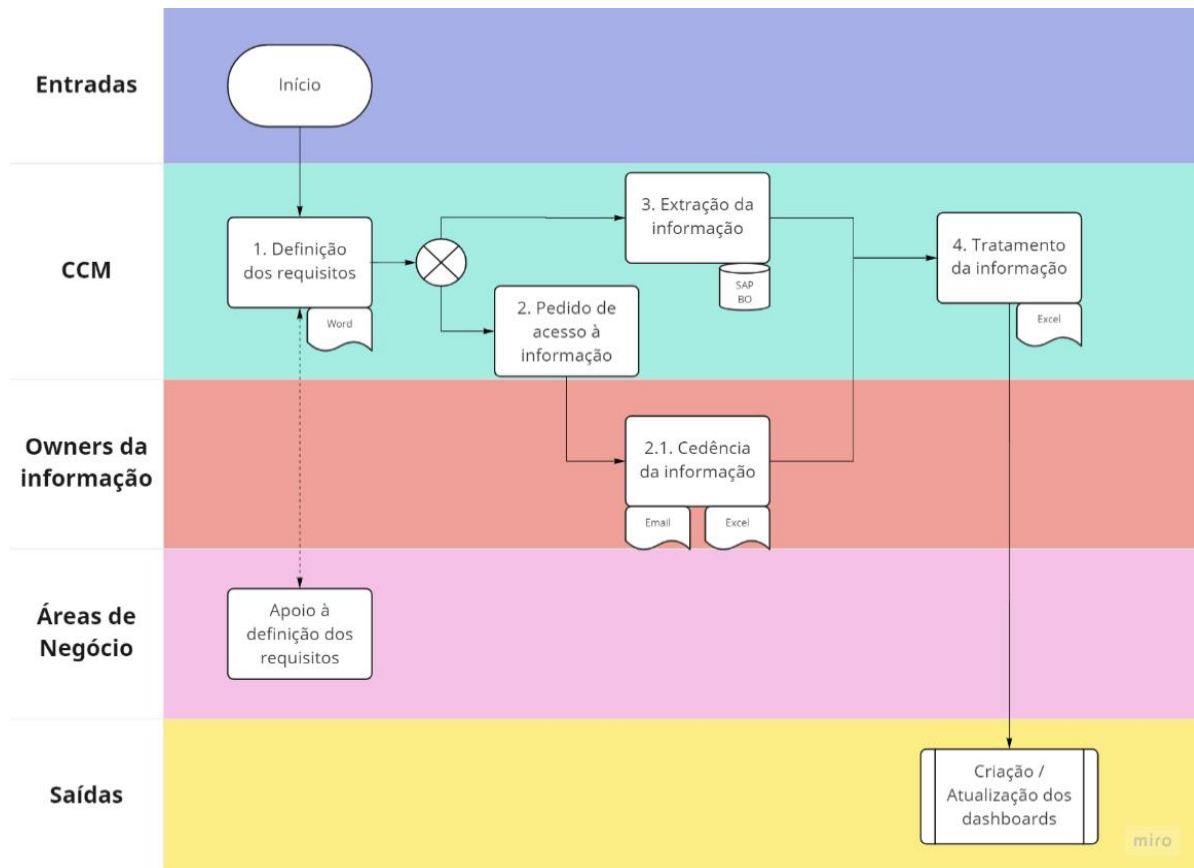


Figura 7 - Processo AS IS CAC - Recolha e tratamento da informação

Estando definidos os requisitos, podem-se distinguir duas categorias de informação: informação acessível pela equipa de CCM e informação não acessível pela equipa de CCM. Assim, dependendo da categoria em causa, é seleccionado um dos caminhos do fluxograma. No primeiro caso, CCM acede diretamente à informação e armazena os ficheiros de dados, geralmente Excel ou CSV, numa pasta partilhada. No segundo caso, é produzido um email pela equipa de CCM, com o pedido de acesso à informação que será enviado para a área responsável por esses dados, geralmente uma área tecnológica.

Os dados acedidos encontram-se indicados na Figura 8. CCM é responsável pela manutenção e atualização dos históricos, que ficam armazenados nas pastas partilhadas da direção de ARC. CCM é ainda responsável por definir e atualizar das permissões elegíveis para a circularização e por extrair, através de SAP BO, a lista de identidades registadas no sistema IAM e a lista de permissões por identidade.

Por sua vez, AS efetua o processamento, em lavastorm, dos dados de utilização das aplicações críticas circularizadas. Após receber o email de CCM com o pedido de acesso a estes dados, AS envia, por email, os dados de utilização destas aplicações, no formato CSV. Nota-se que os registos de cada aplicação crítica possuem campos distintos, ordenados de forma distinta, o que exige algum cuidado no tratamento destes dados.

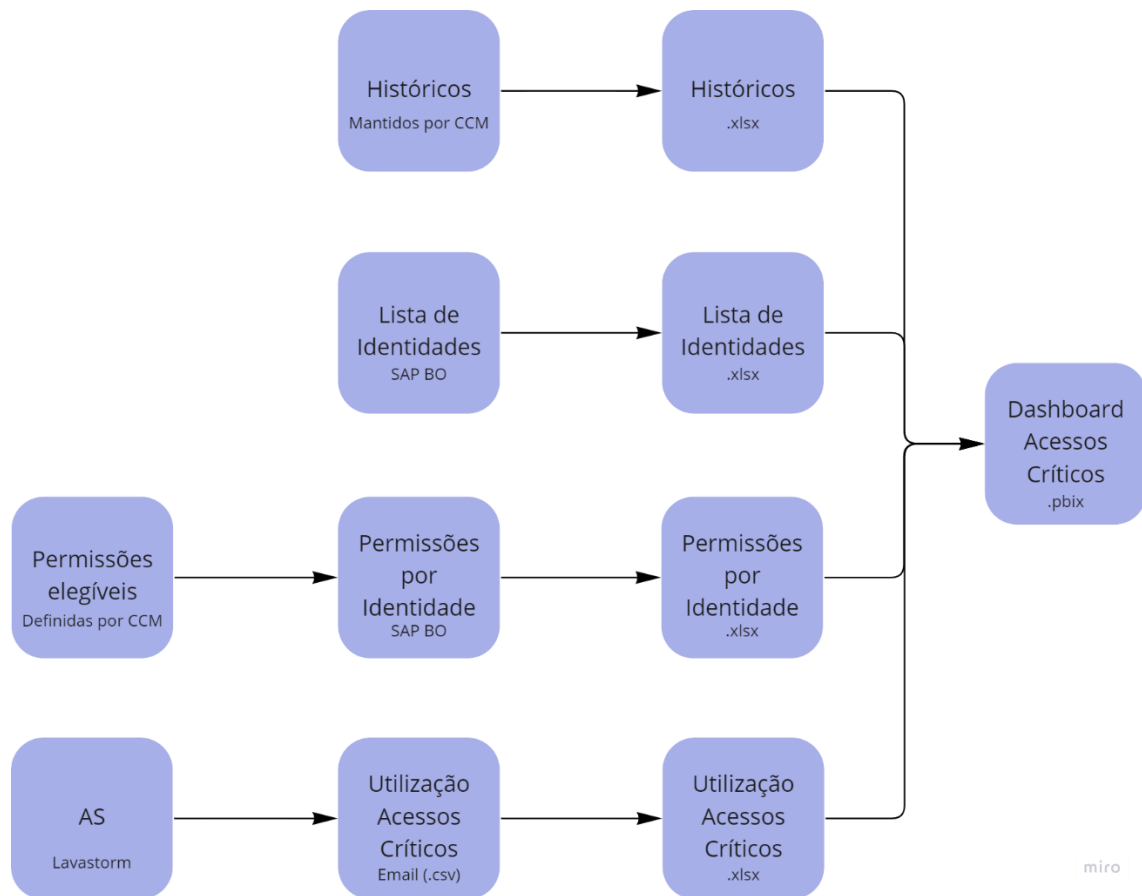


Figura 8 - Fluxo de Dados AS IS CAC

Por fim, as várias fontes de dados são tratadas e normalizadas para que possam ser integradas em Power BI. Esta atividade exige a definição de um padrão para os dados, ao nível dos campos que vão ser utilizados e a ordem desses campos. Isto é particularmente importante no caso dos dados de utilização de acessos críticos que têm múltiplos formatos. Nota-se que esta atividade é manual, podendo ser automatizada, tornando o processo mais rápido e eficiente e menos suscetível a erros.

No final deste subprocesso, é produzida/atualizada uma pasta partilhada da direção de ARC, onde estão disponíveis todos os dados necessários à execução do controlo. O detalhe das várias fontes de informação e dos campos presentes em cada ficheiro de dados encontra-se no ANEXO A: Processo AS IS.

Criação / Atualização dos Dashboards

O subprocesso de Criação / Atualização dos Dashboards inicia-se imediatamente após a recolha e tratamento da informação ser finalizada e as suas atividades estão definidas na Figura 9. A primeira atividade deste processo é o desenho dos Dashboards em Power BI e toda a programação em DAX subjacente à sua construção. Esta atividade é da responsabilidade de CCM, que deverá ter em consideração os requisitos definidos anteriormente, com o apoio das restantes áreas de negócio da empresa. Nesta atividade é produzida a versão inicial dos Dashboards a validar com as áreas de negócio.

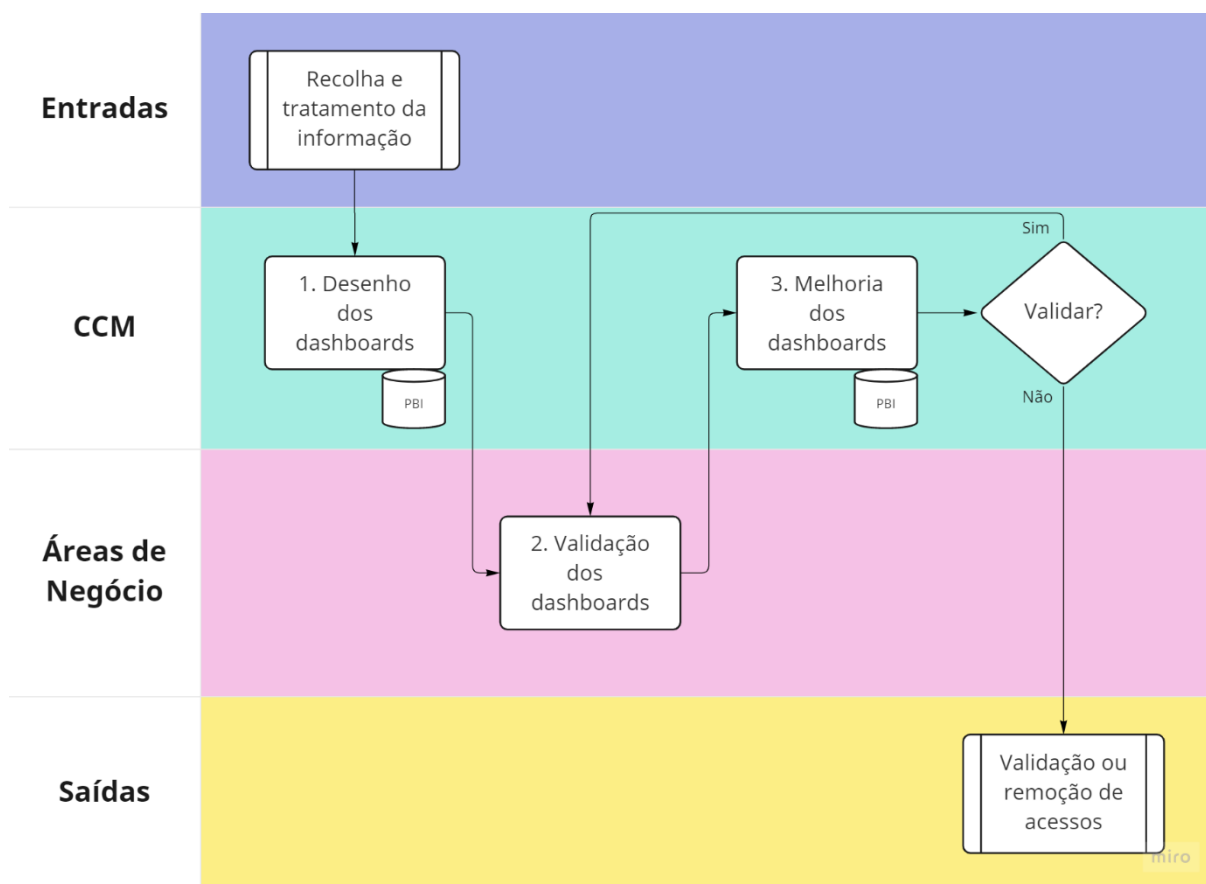


Figura 9 - Processo AS IS CAC - Criação / Atualização dos Dashboards

Em seguida, CCM envia a versão inicial dos dashboards aos gestores de acesso de algumas áreas de negócio. Estes analisam os Dashboards, validando a integridade dos dados e o cumprimento dos requisitos definidos. Nesta atividade são produzidos emails de feedback pelos gestores de acesso, que os enviam a CCM.

Após a validação dos dashboards, a equipa de CCM analisa o feedback recebido pelos gestores de acesso e efetua as alterações necessárias. No final desta atividade, é produzida a versão final dos Dashboards. Nota-se que, caso o feedback recebido por CCM implique mudanças consideráveis, poderá existir a necessidade de revalidar os Dashboards. Essa necessidade será decidida por CCM.

Validação ou remoção de acessos

O subprocesso de Validação ou remoção de acessos inicia-se imediatamente após a Criação / Atualização dos Dashboards ser finalizada e as suas atividades estão definidas na Figura 10. Após a produção dos Dashboards, CCM constrói um email padrão que é enviado aos gestores de acesso das áreas de negócio da empresa. Nesse email estará incluído uma hiperligação de acesso ao Power BI e um conjunto de indicações e alertas gerais. Cada gestor de acessos apenas deverá aceder aos dados relativos à sua direção. Isso é possível através da configuração de perfis no Power BI, por CCM, sendo estes perfis atribuídos aos respetivos gestores de acessos.

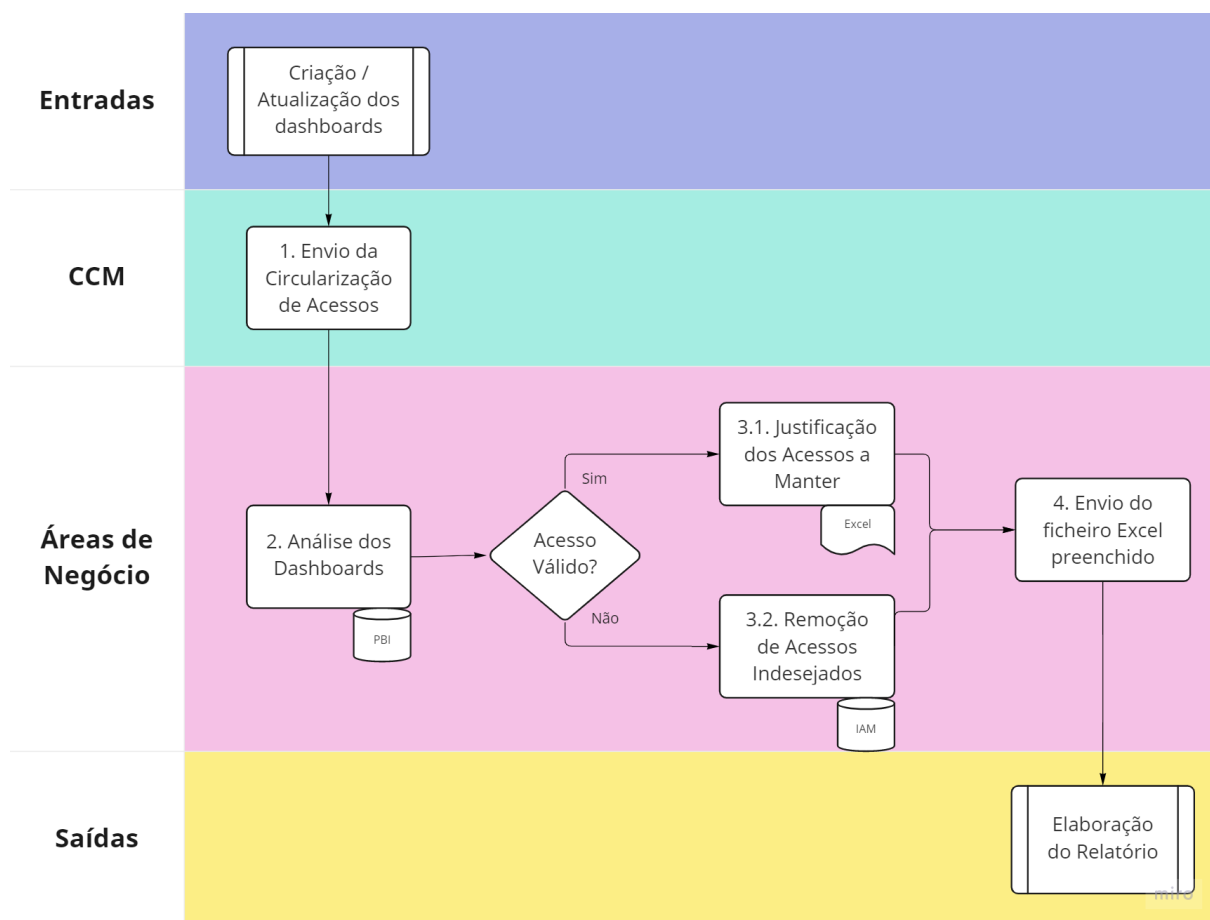


Figura 10 - Processo AS IS CAC - Validação ou remoção de acessos

Após receber o email, o gestor de acessos de cada direção analisa os Dashboards, bem como as indicações de CCM expressas no email. Nesta atividade, o diretor poderá analisar também os Dashboards, dando indicações gerais ao gestor de acessos.

Em seguida, para cada acesso, o gestor de acessos, consultando o diretor e a equipa de CCM sempre que necessário, decide manter ou remover os acessos. Cada acesso que decida manter, deverá ser justificado num ficheiro Excel que deve ser exportado do Power BI. Cada acesso a remover, deverá ser removido no sistema IAM da empresa e indicado no ficheiro Excel que se procederá à sua remoção.

Por fim, é enviado um email a CCM com as justificações para a manutenção de cada acesso a manter e a indicação de que se irá remover os restantes. Com esta informação, CCM poderá elaborar o relatório anual da CAC.

Elaboração do Relatório

O subprocesso de Elaboração do Relatório inicia-se imediatamente após a validação ou remoção de acessos ser finalizada e as suas atividades estão definidas na Figura 11. Depois de receber as respostas das áreas de negócio, CCM atualiza os Dashboards, integrando cada ficheiro Excel recebido no Power BI. Cada ficheiro Excel deverá ser previamente verificado, para garantir que foi devidamente preenchido. Nota-se que esta atividade é bastante demorada e manual, consumindo muito tempo à equipa de CCM.

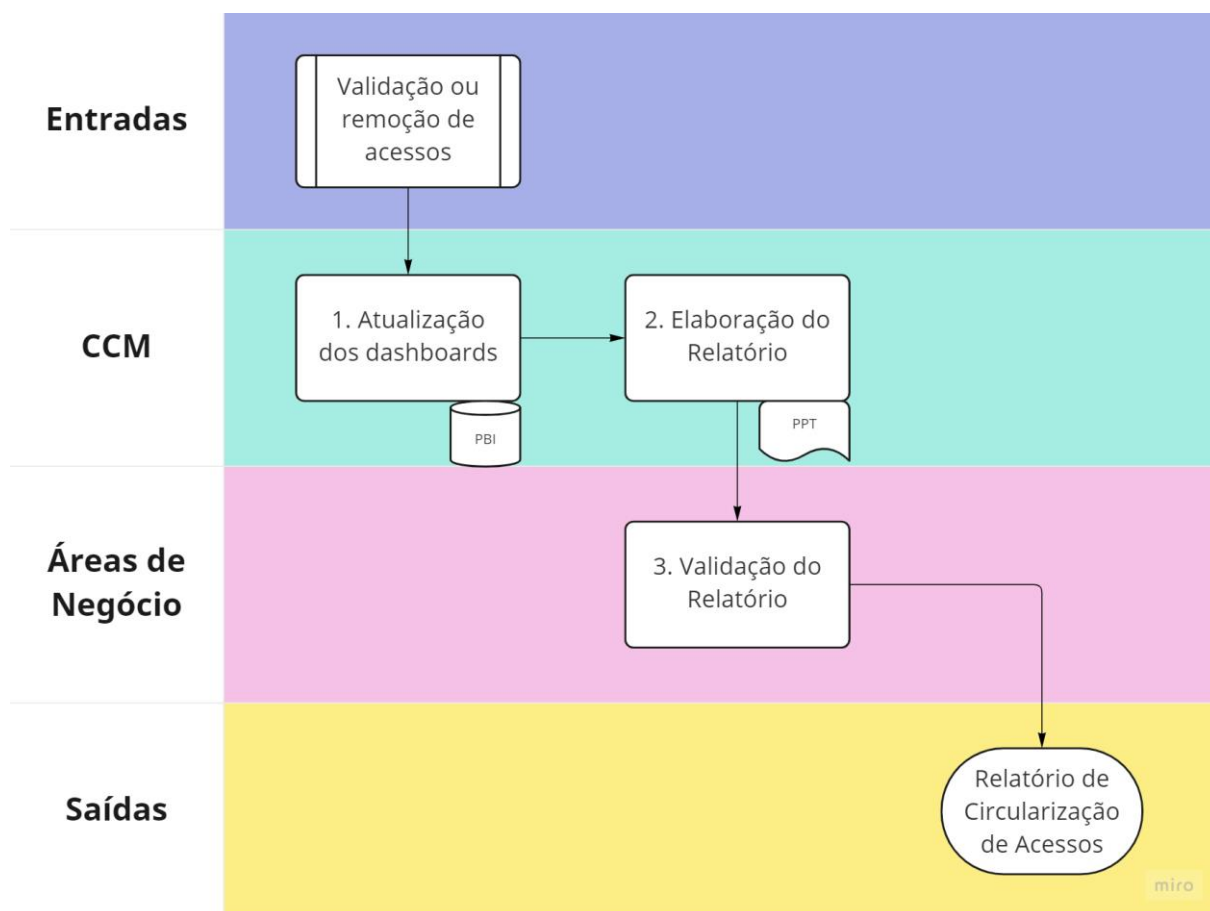


Figura 11 - Processo AS IS CAC - Elaboração do Relatório

Em seguida, CCM elabora um relatório em PowerPoint. Neste relatório são realçados os acessos críticos efetivamente circularizados e os progressos efetuados na eliminação destes acessos quando não são necessários ao desempenho das funções do utilizador. São ainda detalhados os números de acessos não justificados, por aplicação e por direção, bem como a percentagem de utilização de cada justificação.

Por fim, os gestores de acesso validam os dados presentes no relatório, avisando CCM de eventuais erros. No final desta atividade, é finalizado o Relatório de Circularização de Acessos Críticos, que será um documento de ARC, utilizado de forma a verificar se o nível de risco assumido pela empresa, relativamente a acessos críticos, está em linha com o desejado pela comissão executiva.

3.3.2 Indicadores Utilizados

O Dashboard atual, desenhado em Power BI, permite observar:

- Números gerais relativos aos acessos críticos, como o número de aplicações, direções, utilizadores e acessos âmbito da CAC
- O número, detalhado para cada direção, de utilizadores, de acessos (a manter e a eliminar), de acessos sem utilização por aplicação e de acessos circularizados e não circularizados
- O top de finalidades por direção
- A comparação dos números referidos anteriormente com o ano anterior

- O estado da circularização de cada acesso, observando a percentagem de respostas e não respostas por aplicação e por direção
- Filtros, em cada página, por ano da CAC, direção, estado, aplicação, tipo de permissão, código da permissão e utilizador

A Figura 12, a Figura 13 e a Figura 14 demonstram estes indicadores, em 3 páginas criadas no Power BI.

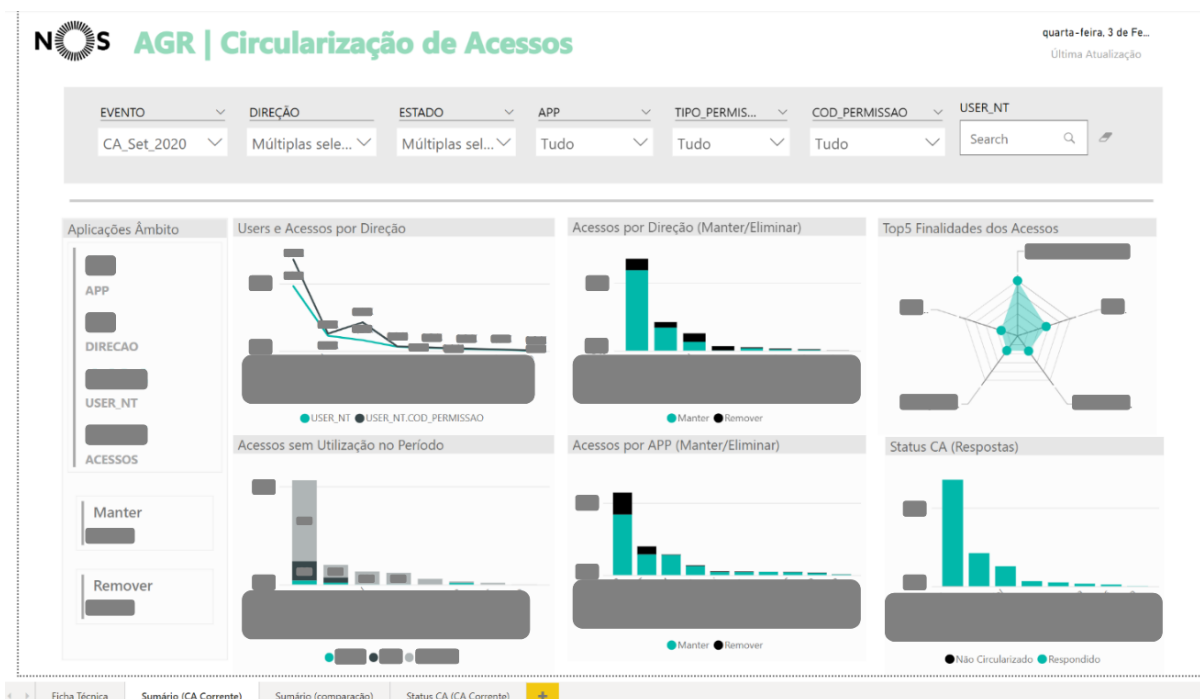


Figura 12 - Dashboard CAC AS IS (1)

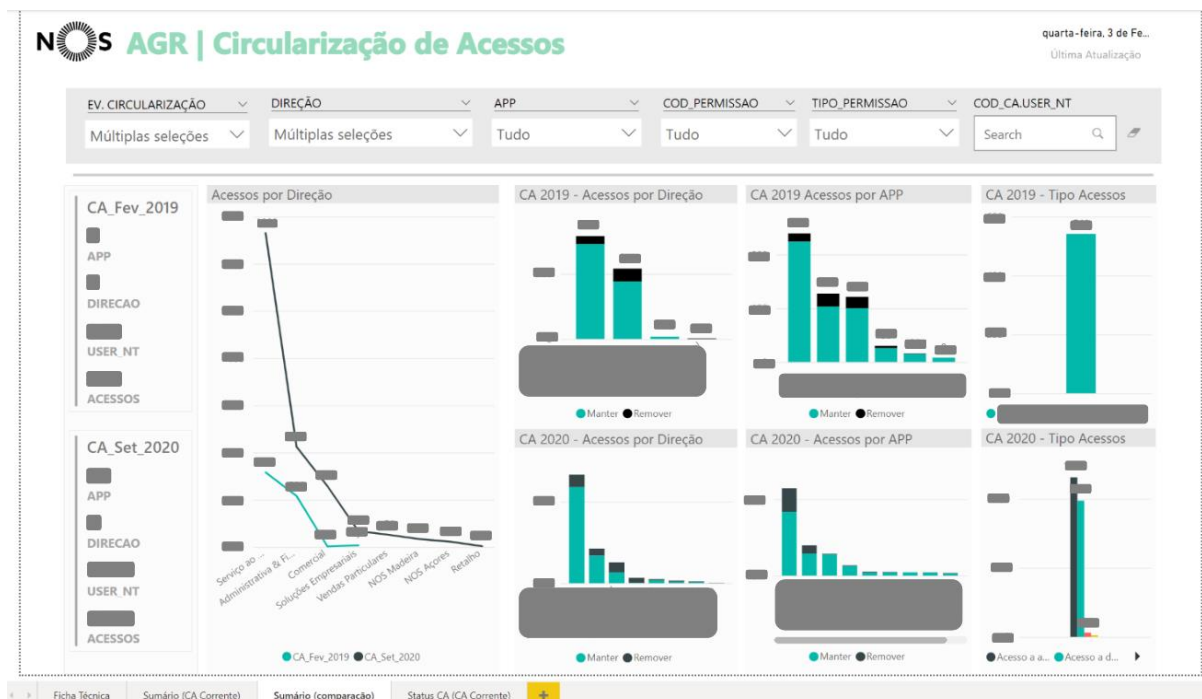


Figura 13 - Dashboard CAC AS IS (2)



Figura 14 - Dashboard CAC AS IS (3)

Para maior detalhe acerca dos indicadores utilizados no Dashboard AS IS, consulte o ANEXO A: Processo AS IS.

3.3.3 Conclusões

Foram identificadas ineficiências em algumas das etapas descritas na Figura 6. Essas ineficiências serão listadas em seguida, de acordo com a etapa na qual ocorrem.

Recolha e tratamento da informação

O processo de recolha de dados, o seu tratamento e a sua importação para Power BI é manual, moroso e repetitivo a cada repetição anual da Circularização de Acessos. Assim, deve ser estudada a possibilidade de automatização total ou parcial deste processo, potenciando dessa forma a sua realização com maior frequência. Se tal for possível, o acesso automatizado, em tempo real, às fontes de informação, permitirá a monitorização contínua dos acessos, com o mínimo esforço por parte de CCM.

Validação ou remoção de acessos

Os diretores e os gestores de acesso tomam a decisão de remover ou de manter, justificando, cada um dos acessos críticos da sua área. Após analisarem o seu dashboard, exportam um ficheiro Excel onde preenchem manualmente as justificações para a manutenção de acessos críticos. As justificações deveriam ser dadas diretamente no sistema IAM e, se possível, automaticamente incorporadas nos dashboards.

Elaboração do Relatório

Os acessos críticos indicados como “não necessários” têm que ser posteriormente removidos, em IAM, pelo gestor de acessos da área respetiva. Esta remoção dos acessos nem sempre acontece e não existe qualquer monitorização da mesma. Deste modo, as reincidências (acessos indicados para remoção que continuam ativos) deveriam ser monitorizadas, emitindo um alerta periódico aos gestores de acesso, gerado após a deteção da ocorrência.

3.4 Monitorização de Acessos Remotos

Um acesso remoto é um acesso lógico que permite o acesso, à distância, aos servidores da NOS, sendo, regra geral, atribuído por perfil e acessível a todos os utilizadores. Estes acessos, apesar de serem de utilização mais generalizada do que os acessos críticos, pelos utilizadores da NOS, é importante garantir que é atribuído o acesso efetivamente necessário..

O controlo dos acessos remotos é feito através da Monitorização de Acessos Remotos, que foi totalmente reformulada em 2020, devido ao drástico aumento da utilização de acessos remotos que a pandemia Covid-19 provocou. Com este aumento, surgiu a necessidade de monitorizar a utilização dos servidores face à sua capacidade, de forma a garantir que estes suportam as atividades de negócio. Assim, este controlo tinha como foco principal a monitorização de eventuais necessidades de aumento de capacidade dos servidores demonstradas pela utilização diária dos mesmos, não deixando de abordar a atribuição dos acessos remotos.

3.4.1 Mapeamento do Processo

De forma semelhante à análise AS IS da CAC, foi desenhado o fluxograma apresentado na Figura 15 com o objetivo de perceber melhor o processo de execução da Monitorização de Acessos Remotos. Trata-se de um fluxograma de 1º nível, que define a sequência de subprocessos necessária para a execução do processo AS IS de Monitorização de Acessos Remotos.

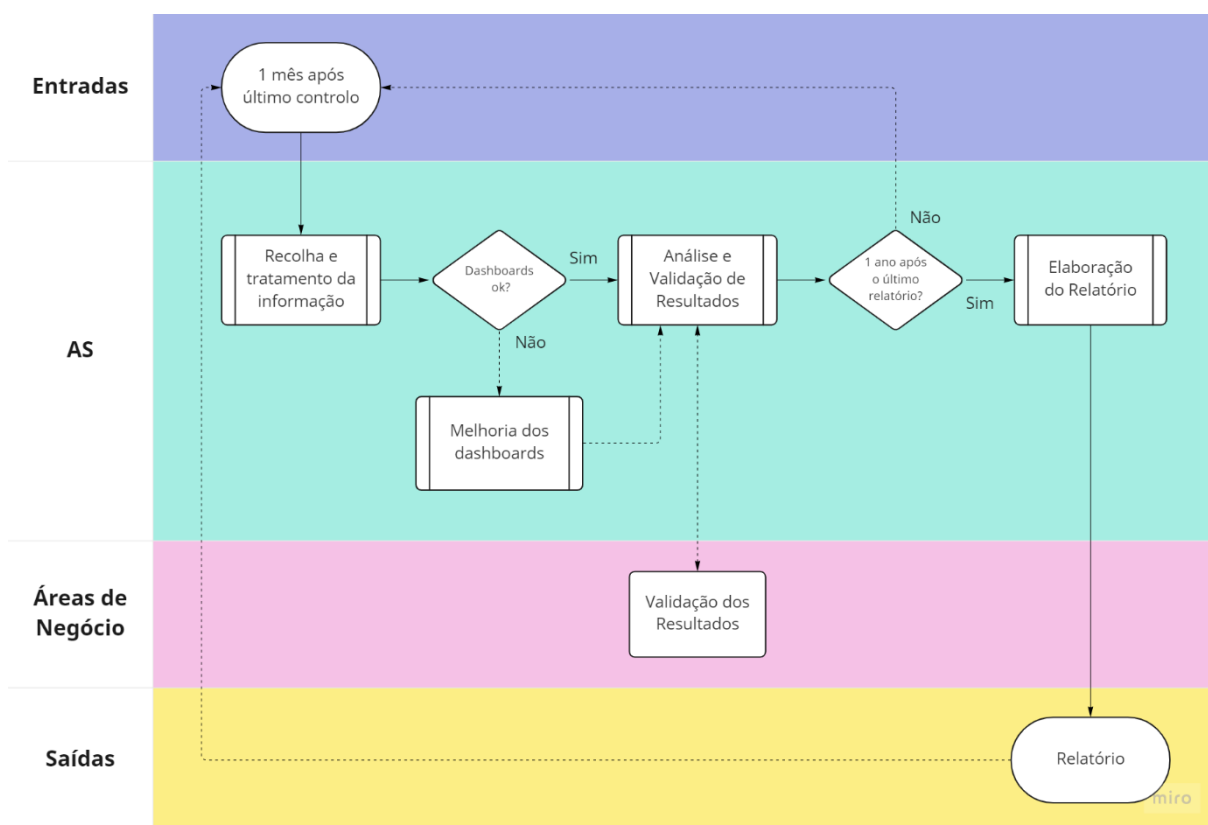


Figura 15 - Processo AS IS MAR - 1º nível

Como podemos observar, existe desde logo uma diferença significativa entre este controlo e o anterior: a recorrência é mensal e não anual. Isto implica que cada execução efetuada não seja significativamente diferente da anterior. Por outro lado, a execução mensal implica também que este controlo seja mais ágil de executar e os processos de execução já estejam a ser realizados

com alguma facilidade. Nota-se ainda que este processo é efetuado atualmente por AS e não por CCM.

O processo inicia-se, então, com uma recorrência mensal, 1 mês após a última ocorrência. A primeira etapa do processo é a recolha e tratamento da informação. Esta etapa permite produzir uma pasta partilhada que agrega todos os documentos necessários à execução do controlo, devidamente normalizados e acessíveis pelo Power BI.

Após recolhida e tratada a informação necessária, AS avalia a necessidade de alterar ou criar indicadores nos Dashboards e, caso necessário, procede à sua melhoria. Não é expectável que a recorrência de desenvolvimentos dos Dashboards seja mensal, pelo que esta etapa será de importância secundária no processo de execução do controlo.

Assim, em situação normal, após recolhida e tratada a informação, procede-se à análise e validação de resultados. Nesta etapa, as áreas de negócio podem colaborar na validação dos dados. Por fim, ocorre a realização de um relatório anual. Esta etapa apenas ocorre a cada 12 ocorrências do controlo e produz um documento em PowerPoint com conclusões acerca do impacto do controlo na empresa.

Em seguida, serão mapeados os subprocessos, e definidas, em fluxogramas de 2º nível, as atividades desempenhadas em cada subprocesso. As atividades encontram-se detalhadas no ANEXO A: Processo AS IS.

Recolha e tratamento da informação

Neste subprocesso, cujas atividades se encontram definidas na Figura 16, ocorre a recolha e preparação da informação necessária ao desenvolvimento dos Dashboards. Este processo é consideravelmente mais simples que o homólogo da CAC por dois motivos. Em primeiro lugar, não há necessidade de rever os requisitos da informação a obter, dado que este é um controlo mensal, pelo que não ocorrerão alterações significativas ao modo de acesso à informação. Em segundo lugar, a AS é independente no acesso a todos os dados que necessita, não existindo a necessidade de efetuar pedidos de acesso a áreas tecnológicas detentoras da informação. Estas duas diferenças tornam este subprocesso exequível em apenas um dia, enquanto que na CAC o processo pode demorar semanas e está suscetível a vários atrasos. Estes atrasos podem ocorrer tanto pela dificuldade em recolher requisitos de algumas direções da empresa, como por dificuldades em contactar alguma área tecnológica detentora de informação necessária, ou por demora ou incorreções na entrega desta informação.

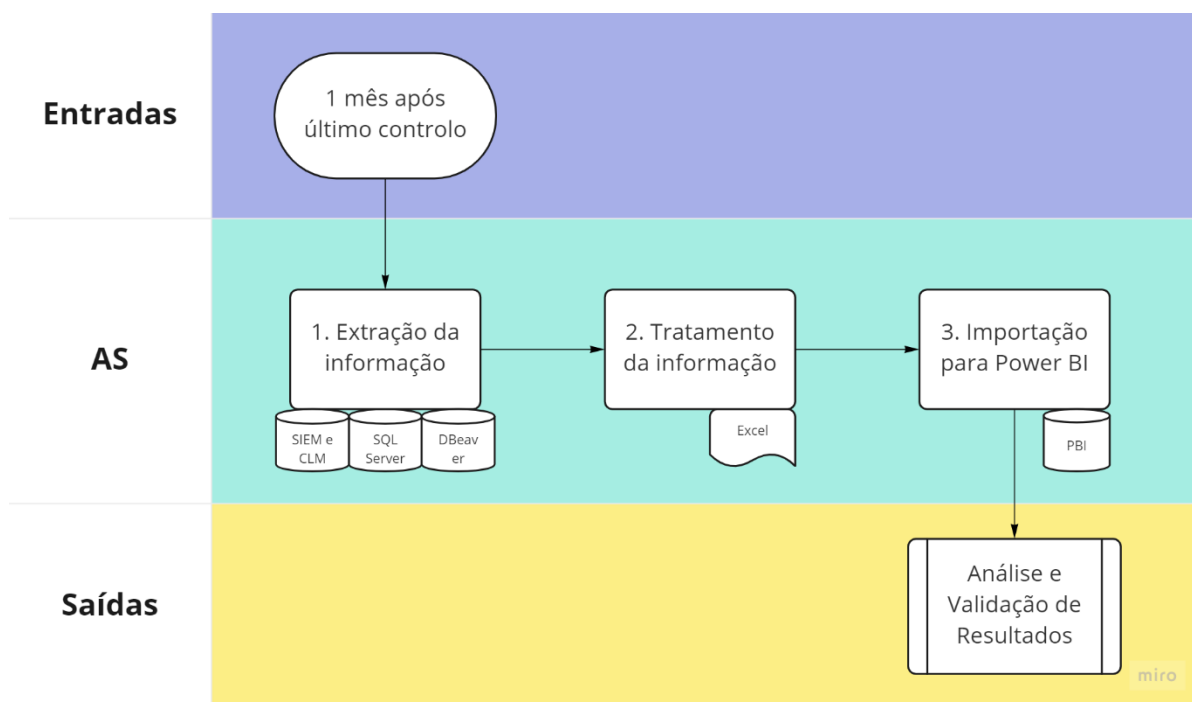


Figura 16 - Processo AS IS MAR - Recolha e tratamento da informação

Deste modo, AS extrai, de forma independente, a informação de que necessita. Em seguida procede ao seu tratamento, normalizando o formato dos ficheiros e ordem pela qual os campos aparecem, no caso de dados do mesmo tipo. Por fim, verifica se o Power BI consegue aceder e importar os dados, corrigindo eventuais erros.

Os dados acedidos encontram-se indicados na Figura 17. Os dados de utilização das VPNs vêm do sistema SIEM (*Security Information and Event Management*) e os dados de utilização da VDI vêm do sistema CLM (*Centralized Log Management*). Os restantes dados vêm da base de dados da empresa, extraídos por ferramentas de extração de dados com recurso à linguagem SQL (*Structured Query Language*).

Nota-se que os dados de utilização das VPNs e da VDI são ficheiros Excel diários, pelo que cada mês terá cerca de 30 ficheiros de cada. Deste modo, a agregação das utilizações diárias das VPNs e da VDI é um trabalho manual pouco eficiente e passível de ser automatizado. Por sua vez, os dois acessos à base de dados criam apenas um ficheiro cada, não sendo difícil nem demorado agregar ambos num ficheiro único, não representando por isso um ponto crítico do processo.

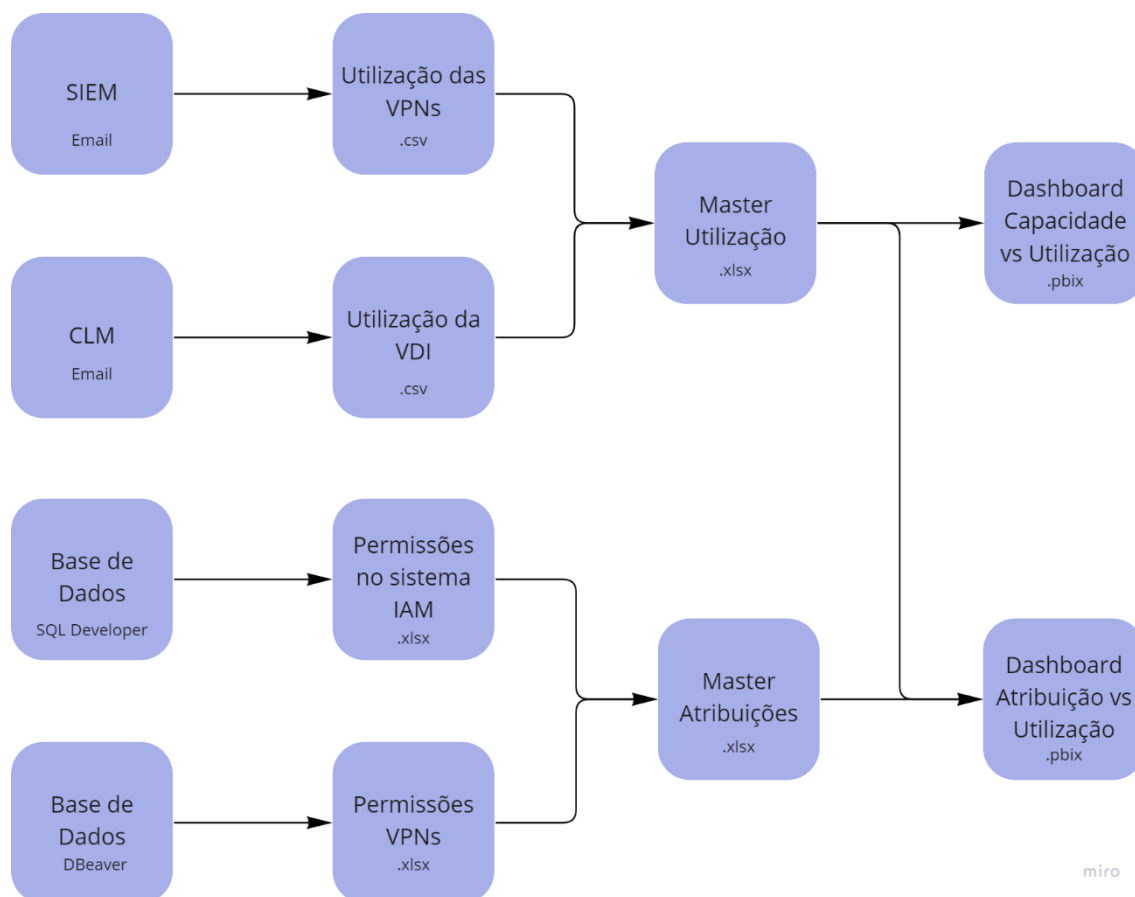


Figura 17 - Fluxo de Dados AS IS MAR

No final deste subprocesso, é produzida/atualizada uma pasta partilhada da direção de ARC, onde estão disponíveis todos os dados necessários à execução do controlo. O detalhe das várias fontes de informação e dos campos presentes em cada ficheiro de dados encontra-se no ANEXO A: Processo AS IS.

Melhoria dos Dashboards

Sempre que exista a necessidade de melhoria dos Dashboards, ocorrerá este subprocesso, descrito na Figura 18, onde se procederá à melhoria das funcionalidades existentes e/ou desenvolvimento de novas funcionalidades. A primeira atividade a ocorrer é a definição dos requisitos do controlo, com o apoio das várias áreas de negócio. Nesta atividade AS produz notas das reuniões com as áreas de negócio e uma lista de requisitos a implementar.

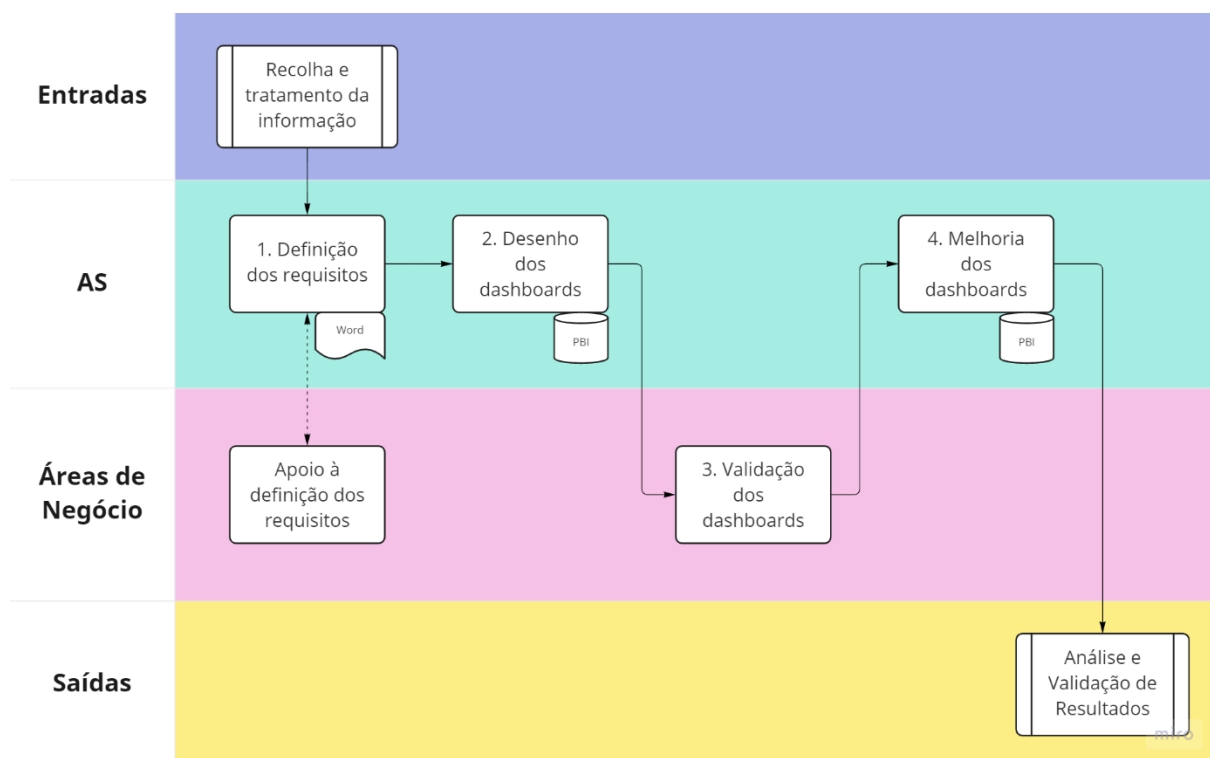


Figura 18 - Processo AS IS MAR - Melhoria dos Dashboards

Seguidamente, AS desenha uma nova versão dos Dashboards, em Power BI, de acordo com os requisitos definidos. Esta nova versão poderá incluir novos indicadores e/ou alterações a indicadores já existentes. No final desta atividade, a nova versão dos Dashboards produzida é enviada para as áreas de negócio.

Por sua vez, as áreas validam os Dashboards, comunicando, sempre que necessário, com AS, de forma a garantir a compreensão dos desenvolvimentos efetuados. No final desta atividade, AS reúne o feedback das várias áreas de negócio e efetua pequenos ajustes aos Dashboards. Após efetuar estes ajustes, é produzida a versão final dos Dashboards, encerrando este subprocesso.

Análise e validação de resultados

Neste subprocesso, cujas atividades se encontram definidas na Figura 19, AS analisa os Dashboards e valida as conclusões com o apoio das áreas de negócio. Na análise dos Dashboards é importante distinguir a análise da comparação entre capacidade e utilização da análise da comparação das atribuições com a utilização, devido ao propósito das mesmas. A análise da comparação entre a capacidade e a utilização tem o objetivo de indicar às áreas tecnológicas se existe uma necessidade de aumento da capacidade dos servidores para suportar a utilização atual. Por outro lado, a análise da comparação das atribuições com as utilizações pretende identificar inconsistências na atribuição de acessos e identificar quem tem acessos atribuídos sem utilização. Neste último caso, os clientes do controlo são as várias direções da empresa, enquanto no primeiro são apenas as áreas técnicas.

Por fim, são enviadas as conclusões aos respetivos clientes. Estes validam a informação recebida e relatam algum erro ou problema que detetem, para correção imediata de AS. Ao concluir esta atividade, será produzido um documento com as conclusões da análise, o plano de ação e outras decisões tomadas.

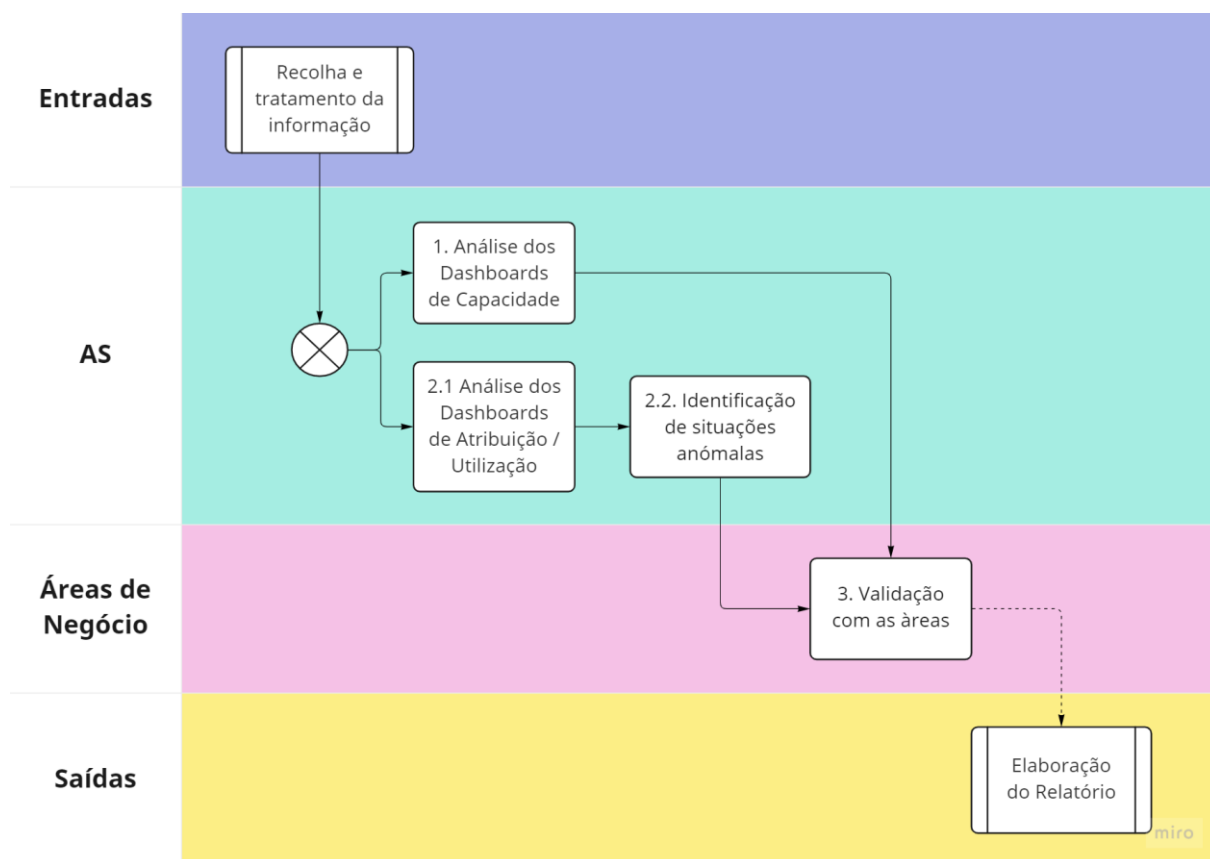


Figura 19 - Processo AS IS MAR - Análise e validação de resultados

Elaboração do Relatório

Por fim, o subprocesso de Elaboração do Relatório inicia-se, anualmente, após a análise e validação de resultados ser finalizada e as suas atividades estão definidas na Figura 20. Este relatório consiste num PowerPoint que realça conclusões de alto nível das últimas 12 análises realizadas, correções efetuadas ao longo deste período e o plano para os meses seguintes.

Este subprocesso é simples e inclui apenas duas atividades. Em primeiro lugar, AS elabora o relatório e envia-o para as várias áreas de negócio envolvidas. Estas avaliam a correção dos dados e validam os mesmo, indicando eventuais erros. No final desta atividade, é finalizado o Relatório de Monitorização de Acessos Remotos, que será um documento de ARC, utilizado de forma a verificar se o nível de risco assumido pela empresa, relativamente a acessos remotos, está em linha com o desejado pela comissão executiva.

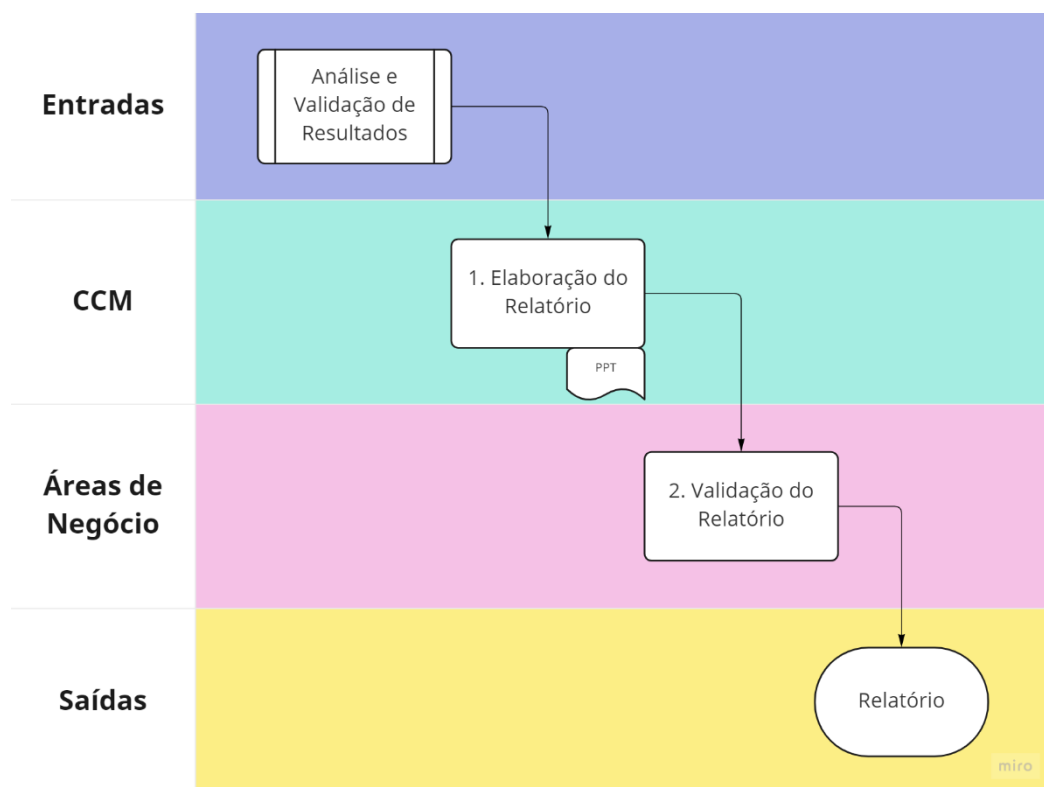


Figura 20 - Processo AS IS MAR - Elaboração do Relatório

3.4.2 Indicadores Utilizados

O Dashboard atual, desenhado em Power BI, tem dois tipos de indicadores principais: indicadores que comparam a capacidade dos servidores à efetiva utilização dos acessos e indicadores que comparam atribuições à utilização desses acessos. Os primeiros são:

- Número de utilizações diárias da VPN Corporativa
- Capacidade da VPN Corporativa
- Número de utilizações diárias da VPN Tecnológica
- Capacidade da VPN Tecnológica
- Número de utilizações diárias da VDI Checkpoint
- Capacidade da VDI Checkpoint

Dos indicadores que comparam atribuições à utilização dos acessos atribuídos, destacam-se:

- Número de acessos remoto com e sem utilização nos últimos 3 meses por tipo de VPN
- Número de colaboradores cuja última utilização ocorreu há mais de 60 dias
- Número de colaboradores cuja última utilização ocorreu há mais de 30, mas menos de 60 dias
- Percentagem de acessos atribuídos através de perfil funcional e de agregador adicional
- Número de acessos atribuídos por tipo de VPN

3.4.3 Conclusões

No contexto atual de alívio das medidas de contenção da pandemia, com os colaboradores a regressar parcialmente aos escritórios e após o grande investimento da empresa nos servidores, a falta de capacidade destes deixou de ser um risco à continuidade do negócio. Deste modo, tornou-se menos relevante monitorizar a utilização dos acessos remotos face à sua capacidade.

Por outro lado, as principais ineficiências do processo prendem-se com a fraca automatização do mesmo, algo que poderia ser desenvolvido. algumas ineficiências do sistema de gestão de acessos, entre as quais:

- O modelo do sistema IAM ser complexo, havendo, por isso, equipas com pouco conhecido do modelo, ainda que as áreas demonstrem boa adesão ao processo;
- A remoção de agregadores adicionais quando ocorre a alteração de funções por parte de um utilizador é manual.;
- Não existir a possibilidade de automatizar a remoção imediata de acessos não utilizados há mais de 90 dias caso as áreas demonstrem o queiram fazer;
- Ser frequente a duplicação de canais de acessos remotos;
- A atribuição de acessos remotos ser feita pelas áreas e não por IT, mais capaz de evitar a desnecessária duplicação de acessos que atualmente é comum.

3.5 Conclusões gerais sobre a Monitorização de Acessos Lógicos

Os vários processos de Monitorização de Acessos Lógicos ocorrem de forma independente, implicando contactos regulares com as várias áreas da empresa. Estes contactos podem ser vistos como pouco eficientes para as áreas, no sentido em que exigem diversas respostas (algumas desnecessárias), consumindo um recurso escasso: o tempo. Deveria, por isso, ser considerado o agrupamento destes processos num único, de resposta única por parte das áreas, o mais intuitivo e automatizado possível.

4 Processo TO BE de Monitorização de Acessos Lógicos

Como descrito na Figura 3, pretende-se agregar num só controlo, os dois já existentes, acrescentando a estes uma análise de Conformidade na Atribuição de Acessos e um Registo de Pendências. Deste modo, o novo controlo, denominado de Circularização de Acessos Contínua será constituído pelas seguintes análises:

- Circularização de Acessos Críticos: análise responsável pela identificação e remoção de acessos definidos como críticos pela área de Segurança & Privacidade, que não são necessários à execução das funções exercidas por cada um dos utilizadores. É ainda responsável pela validação dos acessos críticos a manter, havendo um registo da justificação utilizada (Finalidade) para a manutenção destes acessos.
- Monitorização de Acessos Remotos: análise responsável pela deteção, investigação e resolução de problemas na atribuição e/ou utilização de acessos remotos pelos utilizadores.
- Conformidade na Atribuição de Acessos: análise que deteta e corrige problemas de conformidade na atribuição de acessos críticos ou remotos. De entre os possíveis problemas, destacam-se acessos atribuídos ao perfil que deveriam ser atribuídos à identidade dada a sua criticidade, acessos duplamente atribuídos ao perfil e à identidade, acessos críticos sem finalidade definida ou com finalidade inadequada, e a duplicação desnecessária de acessos remotos.
- Registo de Pendências: registo de alertas criados por ARC cuja resolução por parte dos gestores de acesso se encontra pendente. Este registo será um canal de comunicação entre ARC e os gestores de acesso, reduzindo a necessidade de comunicação por email.

4.1 Mapeamento do Processo

De forma a tornar o processo de recolha, integração, agregação e representação de dados num processo ágil, de execução mensal, são necessárias alterações que facilitem a execução do mesmo. Em primeiro lugar, o processo de melhoria dos Dashboards, tornar-se-á num processo paralelo, pois não haverá a necessidade de recorrência mensal do mesmo, não sendo por isso essencial à execução mensal deste controlo. Deste modo, este processo, desenhado na Figura 21, será iniciado sempre que as necessidades sentidas pelas diversas áreas de negócio, incluindo a área de RC responsável pelo controlo, justifiquem o início de um projeto de melhoria dos mesmos. Após iniciado, o projeto seguirá uma metodologia *waterfall*, iniciando-se à redefinição dos requisitos por parte de CCM com recurso a entrevistas às diversas áreas de negócio. Após recolhidos os requisitos, CCM irá desenvolver o processo de recolha de dados que sejam necessários de acordo com os novos requisitos e cuja recolha ainda não esteja a ocorrer. Em seguida, CCM redesenha os Dashboards de acordo com os novos requisitos e com os novos dados recolhidos. Os novos Dashboards serão então enviados para as áreas de negócio para validação, sendo posteriormente sujeitos a pequenas alterações efetuadas por CCM de acordo com o *feedback* dado pelas áreas aquando da validação. Após CCM efetuar estas alterações recomendadas pelas áreas, a nova versão dos Dashboards estará preparada para ser utilizada na execução mensal do controlo.

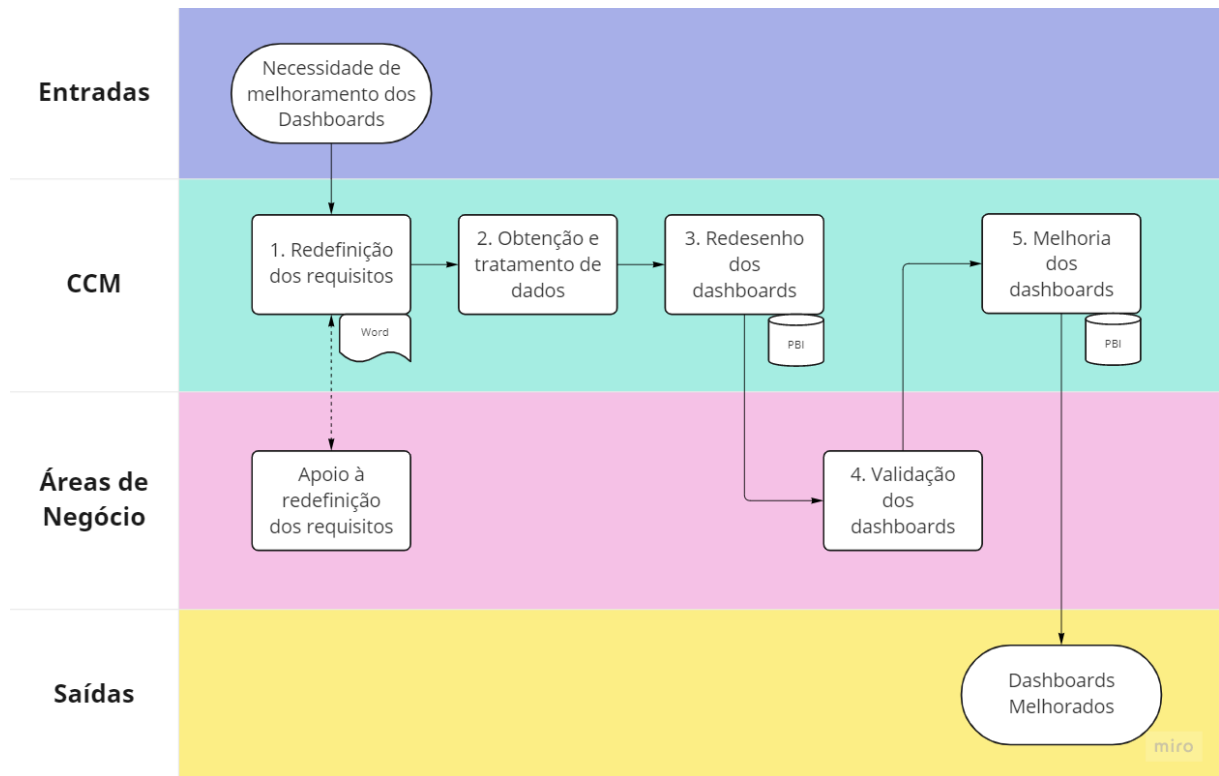


Figura 21 - Processo TO BE de Melhoria dos Dashboards

Por sua vez, o processo de execução do controlo, desenhado na Figura 22, será um processo único e padronizado para as várias análises, ao contrário do que acontecia no processo AS IS. Este processo será iniciado mensalmente, acedendo aos dados, diretamente e indiretamente, de acordo com a acessibilidade destes. Em seguida, os dados são tratados, de forma a agregar dados semelhantes em ficheiros Excel únicos, prontos a importar para Power BI.

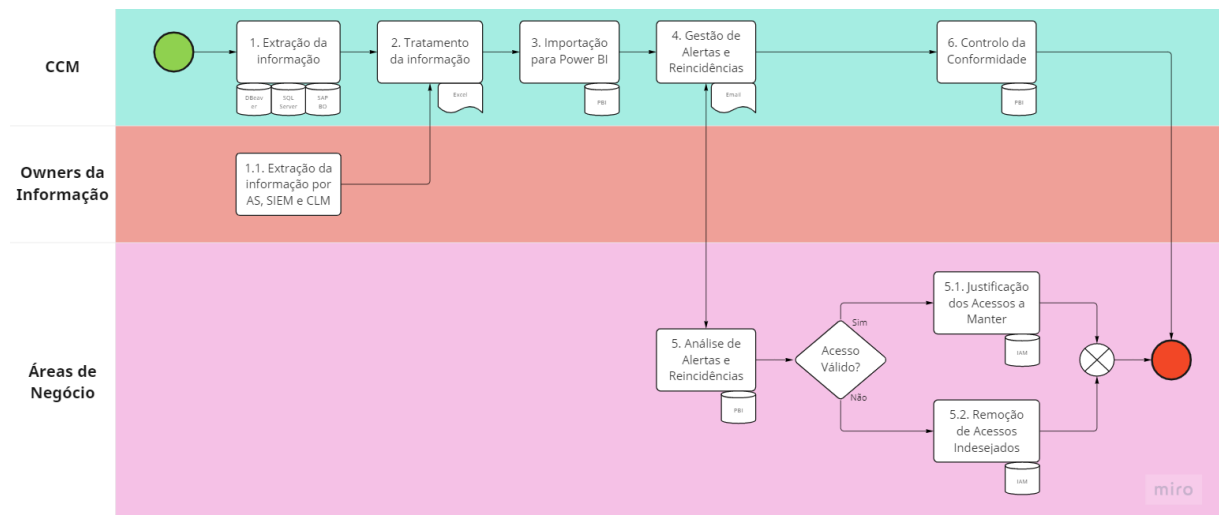


Figura 22 - Processo TO BE de Execução do Controlo

Em seguida, procede-se ao tratamento da informação e a sua importação para o Power BI. Estando os dados devidamente atualizados, é feita, por CCM, a gestão de alertas e reincidências, isto é, são definidas metas a cumprir pelos vários gestores de acessos da empresa. Por sua vez, os gestores de acesso analisam essas metas e validam ou removem acessos em função das mesmas. Em simultâneo, é feito o controlo da conformidade, por CCM, que implementa

iniciativas de resolução de situações de não conformidade no sistema IAM e no sistema de gestão de acessos remotos.

4.2 Fluxo de Dados

O fluxo de dados do novo processo de circularização de acessos resultará, com as devidas alterações, de uma junção do fluxo de dados dos dois processos existentes. Para isso, serão exploradas certas sinergias que minimizam o esforço de execução do processo, como o acesso aos dados das posições e dos acessos no sistema IAM que era feito em duplicado. O fluxo de dados proposto encontra-se detalhado na Figura 23.

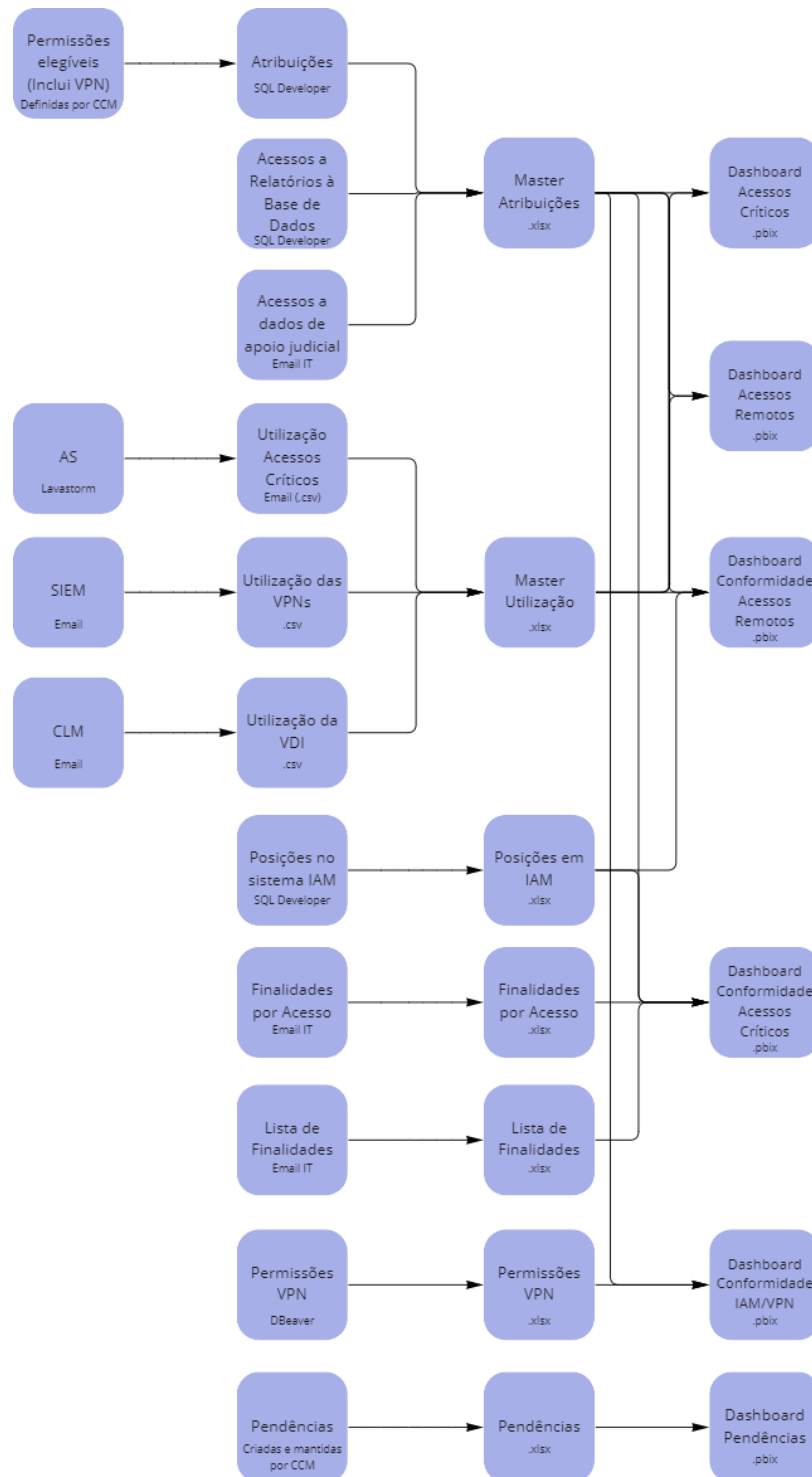


Figura 23 - Fluxo de Dados TO BE

5 Implementação do processo

5.1 Desenvolvimento do Processo de Recolha e Tratamento de Dados

5.1.1 Automatismos para o Acesso aos Dados

De forma a facilitar o acesso aos dados descritos na Figura 23 - Fluxo de Dados TO BE, foram desenvolvidos alguns automatismos. O objetivo destes automatismos é permitir que a atualização dos ficheiros indicados na Figura 24 - Ficheiros de Dados em Excel seja efetuado da forma mais simples possível. Não foram desenvolvidos automatismos para todos os ficheiros, tendo-se dado prioridade ao desenvolvido destes em ficheiros cuja importação de dados era mais demorada e manual. O método de atualização de cada ficheiro aquando da execução mensal do controlo será detalhado abaixo, no capítulo 5.3. Neste capítulo apenas serão descritos os automatismos desenvolvidos.

Name	Type
1. Master Atribuições.xlsx	Microsoft Excel Worksheet
1.1. Acessos a dados de apoio judicial.xlsx	Microsoft Excel Worksheet
1.2. Acessos a relatórios da Base de Dados.xlsm	Microsoft Excel Macro-Enabled Worksheet
2. Master Utilizações.xlsx	Microsoft Excel Worksheet
3. Posições IAM.xlsx	Microsoft Excel Worksheet
4. Finalidades Declaradas.xlsx	Microsoft Excel Worksheet
4.1. Lista de Finalidades.xlsx	Microsoft Excel Worksheet
5. Permissões VPN.xlsx	Microsoft Excel Worksheet
6. Tipos de Permissão.xlsx	Microsoft Excel Worksheet
7. Pendências.xlsx	Microsoft Excel Worksheet
Resumo de Canais VPN.xlsx	Microsoft Excel Worksheet

Figura 24 - Ficheiros de Dados em Excel

Ficheiro 1.2. Acessos a relatórios da Base de Dados

O ficheiro 1.2. é recebido num formato pouco convencional, necessitando de um grande tratamento de dados para que se possa integrar no ficheiro 1, pelo que foram desenvolvidos um conjunto de fórmulas e um programa em VBA que facilitam o tratamento desses dados. Dos campos mais problemáticos deste ficheiro e que requerem, por isso, maior cuidado no tratamento destacam-se:

- o nome do utilizador que, em algumas das linhas, apresenta várias ocorrências, separadas por vírgula ou ponto e vírgula;
- o nome do agregador que, em algumas linhas, não se encontra isolado, sendo seguido pelo sinal “>”, seguido da finalidade;
- a finalidade que, nas linhas em que o campo nome do agregador a inclui, aparece em branco.

Estas particularidades levaram à criação de um manual passo a passo de execução, descrito no Capítulo 5.3, detalhado no ANEXO C: Manual de Execução, e suportado pelo programa VBA apresentado na Figura 25. Este programa desagrega os nomes de utilizador, inicialmente separados por vírgula ou ponto e vírgula, e cria uma linha para cada ocorrência, de forma a normalizar os dados. O ficheiro 1.1. possui também algumas fórmulas semelhantes às do documento 1.2., que facilitam o tratamento da informação, não necessitando de um programa em VBA.

```

Sub TratarDados()
'Percorre os users da página "Dados Trabalhados" e coloca-os em linhas individuais na página "Dados Finais"
Dim LastRow, k, UsersEmLinha As Integer

LastRow = Sheets("Dados Trabalhados").Cells.Find("*", SearchOrder:=xlByRows, SearchDirection:=xlPrevious).Row

k = 2

For i = 2 To LastRow
    UsersEmLinha = Application.WorksheetFunction.CountA(Range(Sheets("Dados Trabalhados").Cells(i, 12), Sheets("Dados Trabalhados").Cells(i, 1000)))

    For j = 1 To UsersEmLinha
        Sheets("Dados Finais").Cells(k, 1) = Sheets("Dados Trabalhados").Cells(i, 11 + j)
        Sheets("Dados Finais").Cells(k, 2) = 
        Sheets("Dados Finais").Cells(k, 3) = Sheets("Dados Trabalhados").Cells(i, 9)
        Sheets("Dados Finais").Cells(k, 4) = Sheets("Dados Trabalhados").Cells(i, 10)
        Sheets("Dados Finais").Cells(k, 5) = Sheets("Dados Trabalhados").Cells(i, 11)
        Sheets("Dados Finais").Cells(k, 6) = Sheets("Dados Trabalhados").Cells(i, 6)
        Sheets("Dados Finais").Cells(k, 7) = Sheets("Dados Trabalhados").Cells(i, 7)

        k = k + 1
    Next
Next
End Sub

```

Figura 25 - Programa VBA para acessos a relatórios da Base da Dados

Ficheiro 2. Master Utilizações

Os registos de utilização dos vários acessos são agregados num ficheiro único: o ficheiro Master Utilizações. Neste ficheiro são associados os acessos (nome de utilizador e nome da permissão) às respetivas aplicações, ao número de utilizações e à data em que estas utilizações foram efetuadas. Previamente à atualização deste ficheiro, são recolhidos dados de cada aplicação, cujos ficheiros são armazenados temporariamente no OneDrive, de acordo com a estrutura indicada na Figura 26.

Name	Type
 Utilizações Críticas	File folder
 VDI	File folder
 VPN	File folder
 Agregar Ficheiros.xlsm	Microsoft Excel Macro-Enabled Worksheet

Figura 26 - Pastas OneDrive

Os dados obtidos dos acessos remotos são de periodicidade diária. De forma a agregar os ficheiros destes dados em duas pastas, uma para os dados das VPNs e outra para os dados da VDI, criaram-se - Regras no Outlook que, de cada vez que um email com os critérios definidos chega, o envia para a pasta adequada, dentro do Outlook. A Figura 27 apresenta um exemplo destas regras.

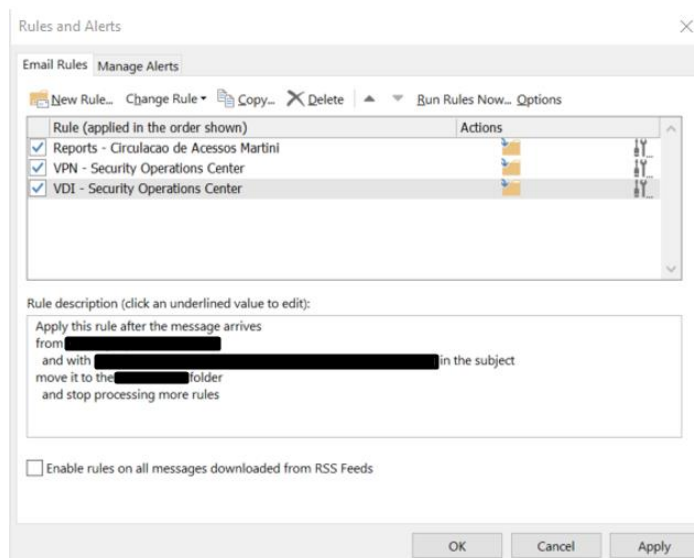


Figura 27 - Regras no Outlook

Em simultâneo, um - Fluxo *do Power Automate*, identifica os emails que chegam a cada uma das pastas do Outlook, descarrega os anexos e guarda-os na pasta adequada no OneDrive. Existe um fluxo para os VPNs e um fluxo para a VDI.

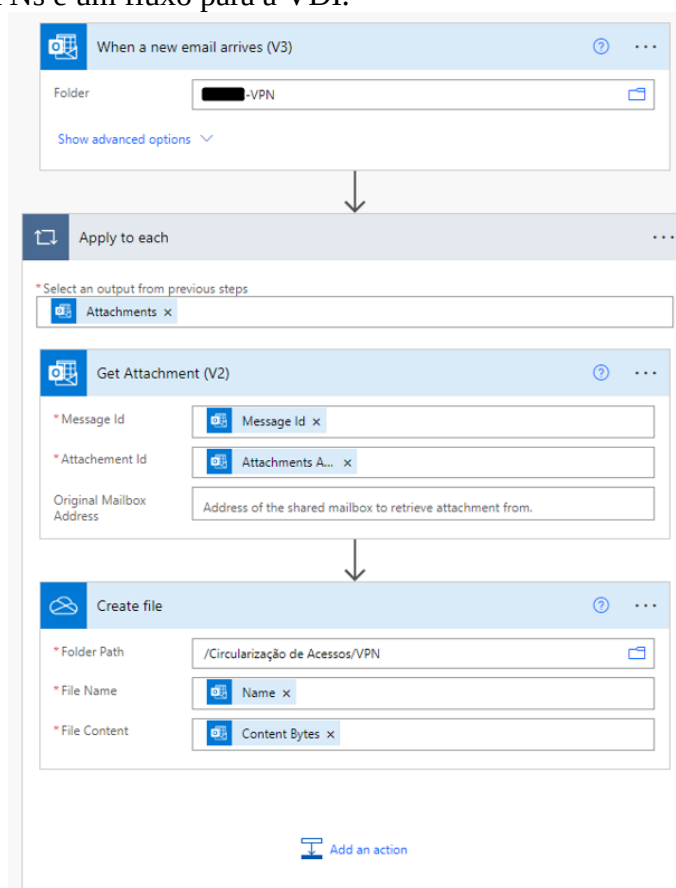


Figura 28 - Fluxo do *Power Automate*

Por sua vez, os dados das aplicações críticas são mensais. Deste modo, não se criou um automatismo para a recolha e armazenamento dos ficheiros Excel, pois o esforço de criação desse automatismo não seria rentabilizado, a curto prazo, pelo tempo poupado na execução manual desta tarefa, não sendo por isso um automatismo prioritário.

Por fim, criou-se um programa em VBA, disponível no ANEXO D: Programa em VBA para agregação de dados de utilização, que agrega os dados de utilização num ficheiro único. Este programa percorre, um a um, os cerca de 60 ficheiros Excel na pasta VDI, abrindo, copiando, e colando os dados de acordo com o formato padrão no ficheiro “Agregar Ficheiros.xlsm”, fechando o ficheiro após cada tarefa. Em seguida, o programa repete a mesma tarefa para os dados das VPNs, aplicando uma regra ligeiramente diferente, pois o formato de origem dos dados ser distinto. Por fim, para cada uma das aplicações críticas é aplicada uma regra própria, que é repetida para o mês atual e para o mês anterior, tendo em conta que se pretende recolher dados dos últimos 2 meses.

Converter CSV em XLS

Os ficheiros de utilizações críticas são recebidos no formato .csv, o que exige a conversão para .xls (Excel) para que os dados possam ser copiados ou trabalhados. De forma a evitar a conversão manual destes ficheiros, criou-se também um pequeno programa apresentado na Figura 29 que, após o utilizador selecionar uma pasta à escolha, abre, converte para .xls e fecha todos os ficheiros .csv existentes dentro dessa pasta.

```
Sub CSVtoXLS()  
    'Ao longo do programa abrem-se diversos ficheiros .xlsx - Esta linha evita que o ecrã esteja constantemente a mostrar os ficheiros a abrir e a fechar  
    Application.ScreenUpdating = False  
  
    Dim xFd As FileDialog  
    Dim xSPath As String  
    Dim xCSVFile As String  
    Dim xWorksheet As String  
  
    xWorksheet = ActiveWorkbook.Name  
    Set xFd = Application.FileDialog(msoFileDialogFolderPicker)  
    xFd.Title = "Select a folder:"  
    If xFd.Show = -1 Then  
        xSPath = xFd.SelectedItems(1)  
    Else  
        Exit Sub  
    End If  
    If Right(xSPath, 1) <> "\" Then xSPath = xSPath + "\"  
    xCSVFile = Dir(xSPath & "*.csv")  
  
    Dim qt As QueryTable  
    Dim newWb As Workbook  
    Dim sFileName As String  
  
    Do While xCSVFile <> ""  
        Application.StatusBar = "Converting: " & xCSVFile  
        Set newWb = Application.Workbooks.Add  
        sFileName = Replace(xSPath & xCSVFile, ".csv", ".xlsx", vbTextCompare)  
        Set qt = newWb.Worksheets(1).QueryTables.Add(Connection:="TEXT;" & _  
            xSPath & xCSVFile, Destination:=newWb.Worksheets(1).Range("A1"))  
        With qt  
            .FieldNames = True  
            .TextFileStartRow = 1  
            .TextFileParseType = xlDelimited  
            .TextFileOtherDelimiter = vbTab 'set your delimiter here  
            .Refresh  
        End With  
        newWb.SaveAs sFileName, FileFormat:=51  
        newWb.Close  
        xCSVFile = Dir  
    Loop  
  
    'Ao longo do programa abrem-se diversos ficheiros .xlsx - Esta linha reverte o bloqueio efetuado anteriormente à visualização do trabalho efetuado pelo VBA  
    Application.ScreenUpdating = True  
    MsgBox "Tarefa Concluída!"  
End Sub
```

Figura 29 - Programa VBA para converter .csv em .xls

5.1.2 Estrutura de Dados em Power BI

Os 7 ficheiros de dados enumerados na Figura 24 são importados para Power BI e relacionam-se de acordo com a Figura 30. A negrito encontram-se as chaves primárias de cada tabela, estando sublinhadas as chaves secundárias. Nota-se que as pendências não estão relacionadas com nenhum dos restantes dados, por se tratarem de um registo independente, por parte de CCM, de alertas por resolver por parte dos gestores de acesso das várias direções.

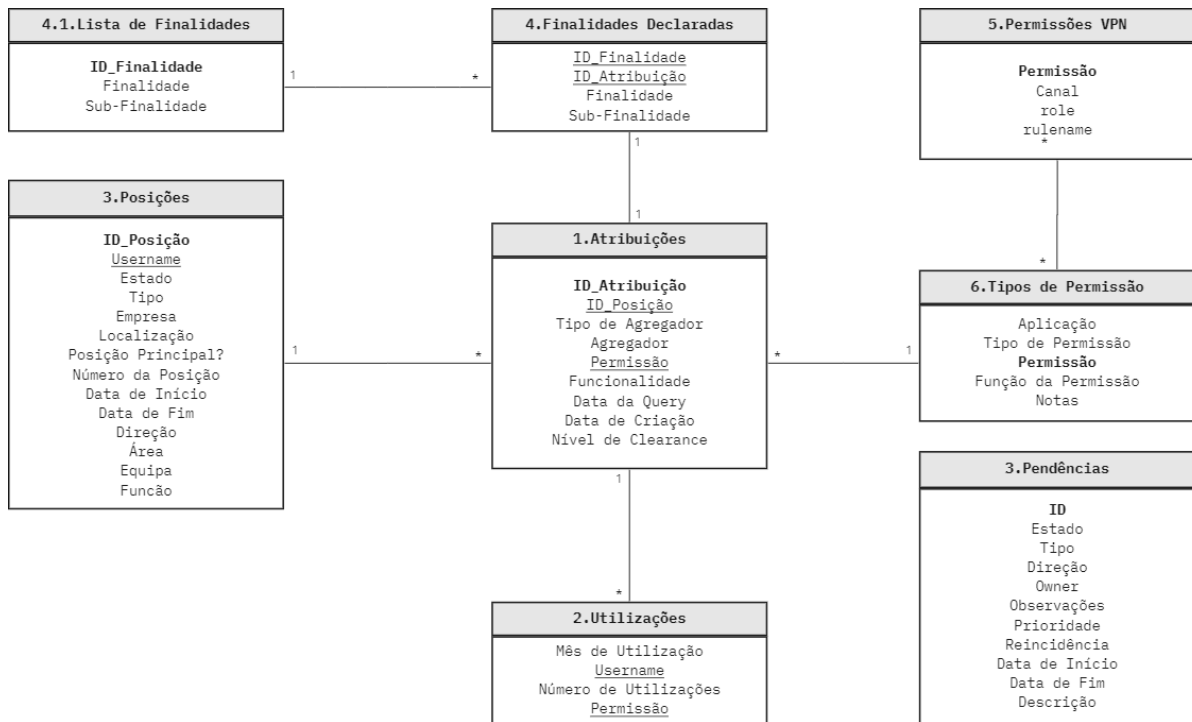


Figura 30 - Estrutura de Dados

5.1.3 Importação e transformação de dados com o Power Query

Cada um dos ficheiros indicados na Figura 24 foi associada ao Power BI, pelo que qualquer modificação efetuada nesses ficheiros, será atualizada no Power BI, de acordo com as regras de importação e transformação estabelecidas, bastando para isso carregar no botão “atualizar”. A maioria dos ficheiros foi importada sem qualquer tratamento em Power Query. As exceções são os ficheiros das Atribuições, das Utilizações e das posições.

No ficheiro das Atribuições apenas foram removidas as linhas em branco. No ficheiro de Utilizações foi adicionada uma coluna com o número do mês da utilização, calculado a partir da data registada, que irá ser utilizada mais tarde para determinação do mês anterior e do mês atual e agregação de dados para cada caso. Por fim, a data foi normalizada, excluindo-se a hora, por não ser necessária e porque em alguns dados, esta não estava registada. No ficheiro das Posições, removeram-se as posições de utilizadores cujo estado era inativo.

5.2 Desenvolvimento dos Dashboards

Como indicado anteriormente, foram desenvolvidos Dashboards com recurso ao software *Power BI*. Para a criação destes Dashboards, foram criadas colunas e medidas nas diversas fontes de dados importadas. Tendo em conta o elevado número de colunas importadas, colunas criadas e medidas criadas, de forma a manter organizada a lista de campos no *Power BI* e facilitar o acesso a cada tipo de campo, para as colunas importadas manteve-se o nome de origem, para as colunas criadas acrescentou-se, como prefixo, um ponto (“.”) e para as medidas criadas acrescentou-se, como prefixo, dois pontos (“..”). Nos próximos capítulos serão referidas algumas dessas colunas e medidas, consideradas mais relevantes para a compreensão dos Dashboards. Para maior detalhe acerca das mesmas, consultar o ANEXO B: Processo TO BE.

5.2.1 Dashboard 1 - Âmbito

A página apresentada na Figura 31 oferece uma visão global dos acessos da empresa, mostrando os totais e o detalhe para os acessos críticos e para os acessos remotos. Nos totais são observados o número de utilizadores, de direções, de aplicações e de parceiros da empresa.

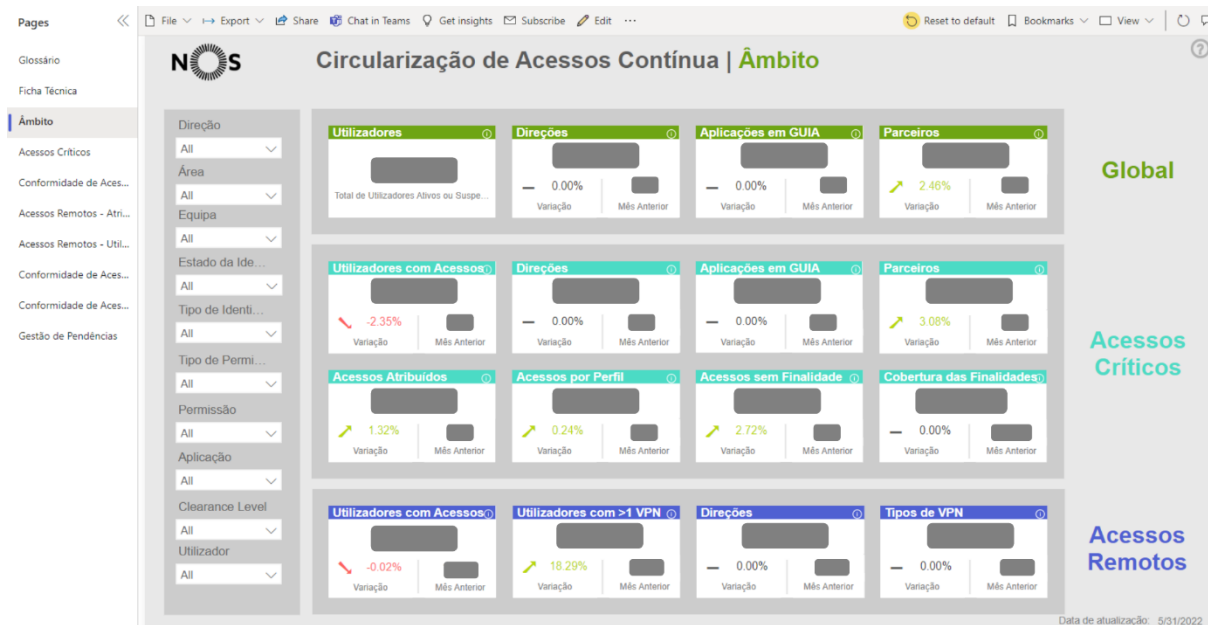


Figura 31 - Dashboard 1 - Âmbito

Para os acessos críticos, detalha-se o número de utilizadores que possuem algum destes acessos, bem como o número de direções, aplicações e parceiros a estes associados. Detalha-se também o número de acessos atribuídos (que pode ser mais do que um por utilizador) e quantos destes são atribuídos ao perfil e quantos não têm finalidade definida. É também mostrado um indicador (cobertura das finalidades) que indica qual a percentagem de finalidades definidas no ficheiro “4.1. Lista de Finalidades” que é utilizada para justificar estes acessos.

Para os acessos remotos, detalha-se o número de utilizadores que possuem algum destes acessos, bem como o número de direções a associadas a estes. É também indicado o número de acessos remotos existentes (Tipos de VPN) e quantos utilizadores possuem mais do que um destes tipos.

Para cada indicador é ainda calculada a variação face ao mês anterior e apresentada através de uma seta, uma percentagem e uma cor (verde ou vermelha). Tanto a cor como a seta variam de forma dinâmica perante o valor em causa. Para efetuar estes cálculos e apresentar estes valores de forma dinâmica foram criados, para cada indicador 2 medidas no Power BI, uma para a evolução do indicador e outra para relacionar uma seta crescente ou decrescente de acordo com o valor do indicador de evolução. A fórmula de cálculo destas 2 medidas está exemplificada nas figuras abaixo (Figura 32 e Figura 33) para um indicador genérico: Indicador X. Sempre que necessário, foram aplicados filtros diretamente no indicador para auxiliar este cálculo.

```

1 ..INDICADOR_X_Evolution =
2 (CALCULATE(
3     DISTINCTCOUNT('Atribuições'[INDICADOR X]),
4     'Atribuições'[.Data] IN { "Mês Atual" } )
5 -CALCULATE(
6     DISTINCTCOUNT('Atribuições'[INDICADOR X]),
7     'Atribuições'[.Data] IN { "Mês Anterior" }
8 ))/CALCULATE(
9     DISTINCTCOUNT('Atribuições'[INDICADOR X]),
10    'Atribuições'[.Data] IN { "Mês Anterior" }
11 )

```

Figura 32 - Power BI - Cálculo da Evolução do Indicador X

```

1 ..INDICADOR_X_Arrow = IF([..INDICADOR X Evolution]>0,UNICHAR(10138),IF([..INDICADOR X Evolution]<0,UNICHAR(10136),UNICHAR(8722)))

```

Figura 33 - Power BI - Determinação da seta a aplicar ao Indicador X

5.2.2 Dashboard 2 - Acessos Críticos

A página apresentada na Figura 34 permite analisar a quantidade de utilizadores e de acessos por cada direção. No caso dos acessos, são ainda detalhados por aplicação e por tipo. Do lado direito, é ainda possível observar o número de acessos não utilizados nos últimos 30 e 60 dias, por direção (gráficos de cima) e por aplicação (gráficos de baixo). Nota-se que, de cada vez que é utilizada a direção, em qualquer Dashboard, é permitido o *drill down* por área e por equipa. Esta metodologia de *drill down* é também aplicada a outras variáveis, sempre que os dados o permitem.

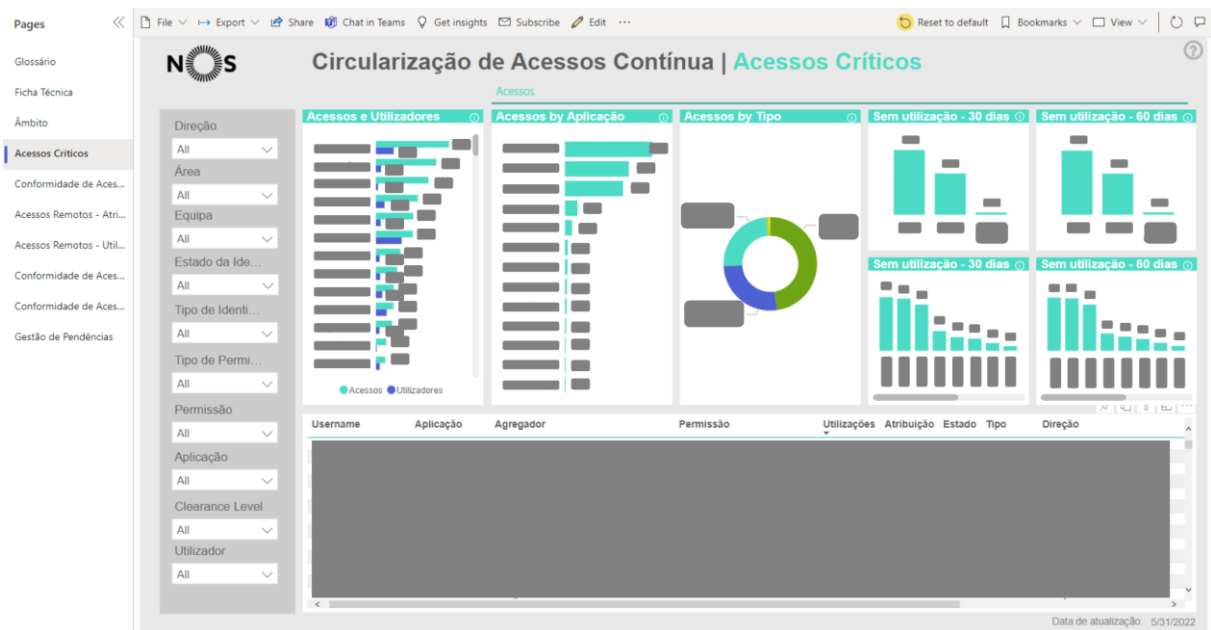


Figura 34 - Dashboard 2 – Acessos Críticos

Por fim, em baixo, vê-se, em detalhe, uma lista de acessos, com as suas características. Esta lista será filtrada sempre que o gestor de acessos selecionar uma categoria de acessos em algum dos gráficos acima, permitindo uma navegação intuitiva e facilitada. Esta lista estará disponível na maioria dos Dashboards para permitir a visão detalhada dos acessos em análise.

De forma a determinar quais as atribuições sem utilização, a 30 e 60 dias, criaram-se duas novas colunas (Utilizações30 e Utilizações60) na tabela de Atribuições que somam as utilizações registadas na tabela Utilizações, por cada acesso (par Utilizador, Permissão). No primeiro caso, a soma efetua-se após aplicação de um filtro para o mês mais recente (mês atual), não existindo qualquer filtro no segundo caso, dado que apenas irão ser importados para Power BI dados relativos aos últimos 2 meses. De forma a permitir a associação das utilizações do mês atual com as atribuições do mesmo mês, foi criada uma coluna na tabela Atribuições (Data) que, de acordo com a data proveniente da base de dados (CAL_DAT), indica se a atribuição é referente ao “Mês Atual” ou ao “Mês Anterior”. Por sua vez, a mesma lógica foi aplicada na tabela Utilizações com a criação de uma coluna para a “Data” que permite a associação das atribuições com as utilizações.

5.2.3 Dashboard 3 - Conformidade de Acessos Críticos

Na página apresentada na Figura 35 podem ser observadas as finalidades registadas no sistema IAM como justificação para a atribuição de acessos críticos, bem como os acessos sem finalidade definida. Mais à direita observam-se outros problemas de conformidade, progressivamente de menor relevância, começando pelas atribuições duplicadas, isto é, atribuídas simultaneamente ao perfil e à identidade, e pelos acessos críticos atribuídos ao perfil, tendo em conta que, por norma, devem ser atribuídos à identidade. Em seguida, observam-se o número de acessos por direção atribuídos a utilizadores de parceiros em acreditação. Por fim, identificam-se acessos a aplicações financeiras fora das direções financeiras, que, por norma, não é expectável. Estes dois indicadores foram criados de acordo com uma necessidade demonstrada por gestores de acessos de direções financeiras.

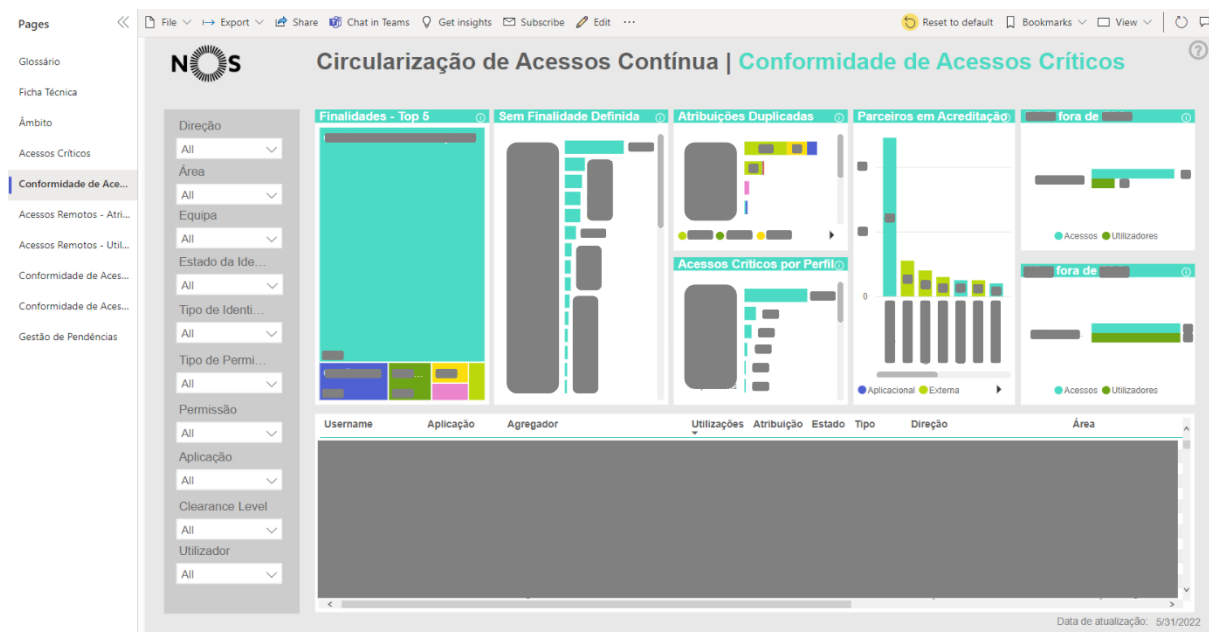


Figura 35 - Dashboard 3 - Conformidade de Acessos Críticos

5.2.4 Dashboard 4 - Acessos Remotos - Atribuição

Na página apresentada na Figura 36 é possível analisar, no primeiro gráfico, o número de utilizadores, por direção, que não utilizaram (a azul claro) e que utilizaram (a azul escuro) acessos remotos nos últimos 60 dias. Em seguida, observa-se o número de acessos remotos por cada aplicação, permitindo identificar aplicações menos relevantes que possam vir a ser descontinuadas, encerrando eventuais acessos obsoletos. Por fim, os últimos dois gráficos

demonstram a quantidade de acessos por direção e por aplicação, dando a percepção ao gestor de acessos, de que aplicações são utilizadas em cada direção, área e equipa.

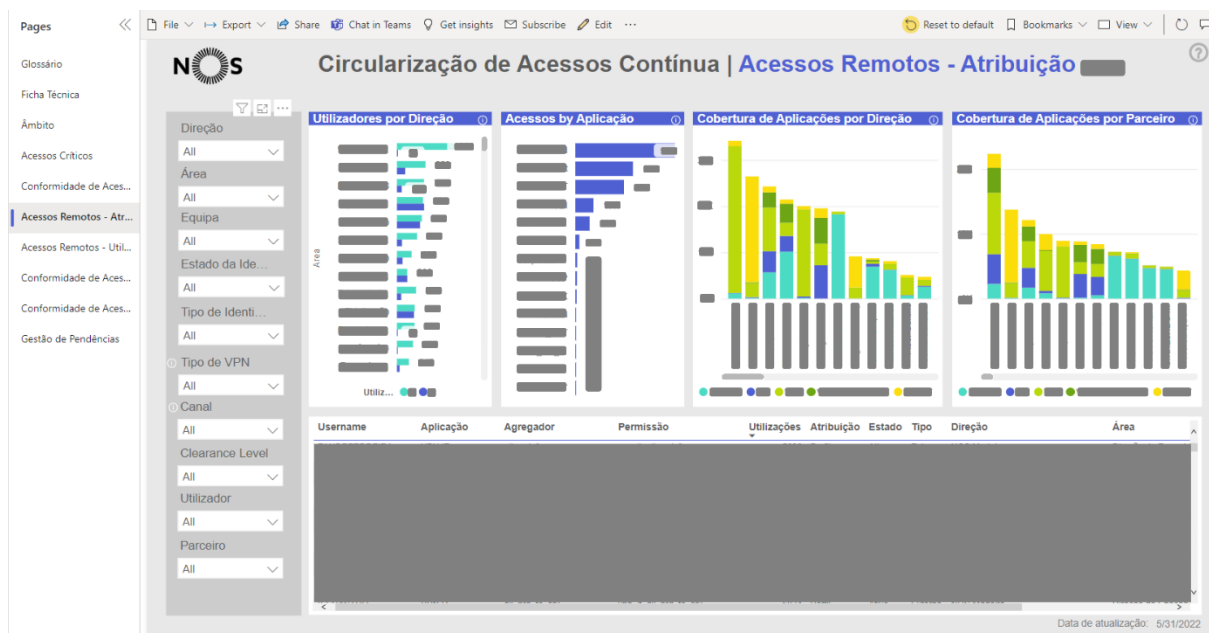


Figura 36 - Dashboard 4 - Acessos Remotos – Atribuição

5.2.5 Dashboard 5 - Acessos Remotos - Utilização

Na página apresentada na figura Figura 37 os acessos remotos são analisados numa perspetiva de utilização. Em primeiro lugar, observa-se o número de utilizadores (com utilização) por cada tipo de acesso remoto. Em seguida, é feito o detalhe deste número, por cada canal, dentro desses tipos de acesso remoto. Nota-se que a cor do tipo de acesso remoto é preservada na análise por canal. No terceiro gráfico, vê-se o número de utilizadores (com utilização), para cada tipo de VPN, por parceiro.

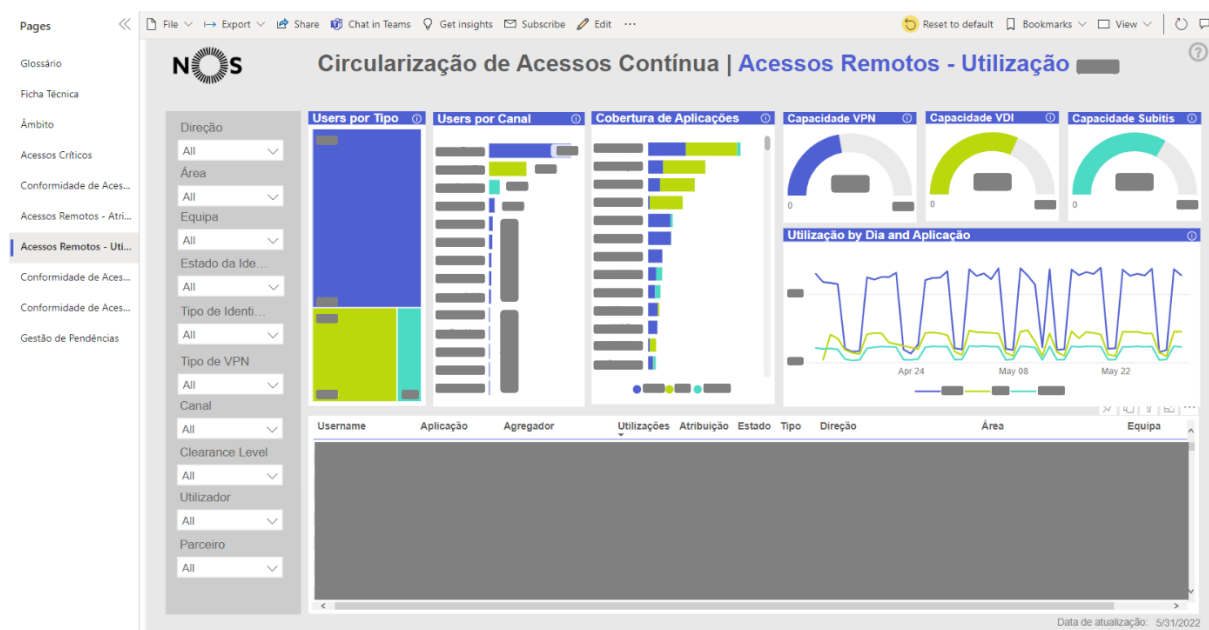


Figura 37 - Dashboard 5 - Acessos Remotos – Utilização

Do lado direito, em cima, é feita uma comparação entre a utilização e a capacidade de cada tipo de acesso remoto, preservando a mesma cor dos gráficos à esquerda. Em baixo, é analisada a evolução diária de utilizações por cada tipo de acesso remoto.

Para permitir a análise da capacidade dos diferentes tipos de acessos remotos, é necessário determinar a necessidade de utilização de cada tipo de acesso. Para o fazer, foi criada a coluna “UtilizaçõesDia”, na tabela de atribuições, que conta o número de utilizadores distintos no último mês, para cada tipo de acesso. Nota-se que este número representa o total de utilizadores que utilizou cada tipo de acesso no último mês, não representando o maior número de utilizações em simultâneo por cada tipo, sendo, por isso, um indicador maior e, por isso, mais conservador do que este último seria. Assim, o indicador utilizado, trata-se de uma estimativa, excessiva, da necessidade de capacidade dos servidores. Ainda assim, apesar de mais exato, o maior número de acessos em simultâneo no último mês não seria calculável com os dados disponíveis, pois não se tem acesso à hora em que a utilização termina.

5.2.6 Dashboard 6 - Conformidade de Acessos Remotos

Nesta página, apresentada na Figura 38, analisa-se a conformidade na atribuição de acessos remotos. No primeiro gráfico, está disponível o número de acessos remotos atribuídos de forma duplicada, isto é, ao perfil e à identidade, em simultâneo. No meio, em cima, identificam-se os utilizadores com 2 e ou 3 ou mais tipos de acessos remotos, identificando-se, em baixo, os acessos remotos atribuídos a pares de tipos que não é expectável que existam em simultâneo. Do lado direito, são apresentados dois gráficos que identificam não conformidades na atribuição de dois tipos de acessos remotos, definidas como tal pela equipa de Segurança & Privacidade. Neste Dashboard, ao contrário do que acontece nos restantes, são apresentadas 3 tabelas, em baixo, em vez de uma única. Isto acontece de forma a permitir que o utilizador aceda ao detalhe de cada acesso de forma independente para cada conjunto de gráficos, devido à sua natureza distinta.

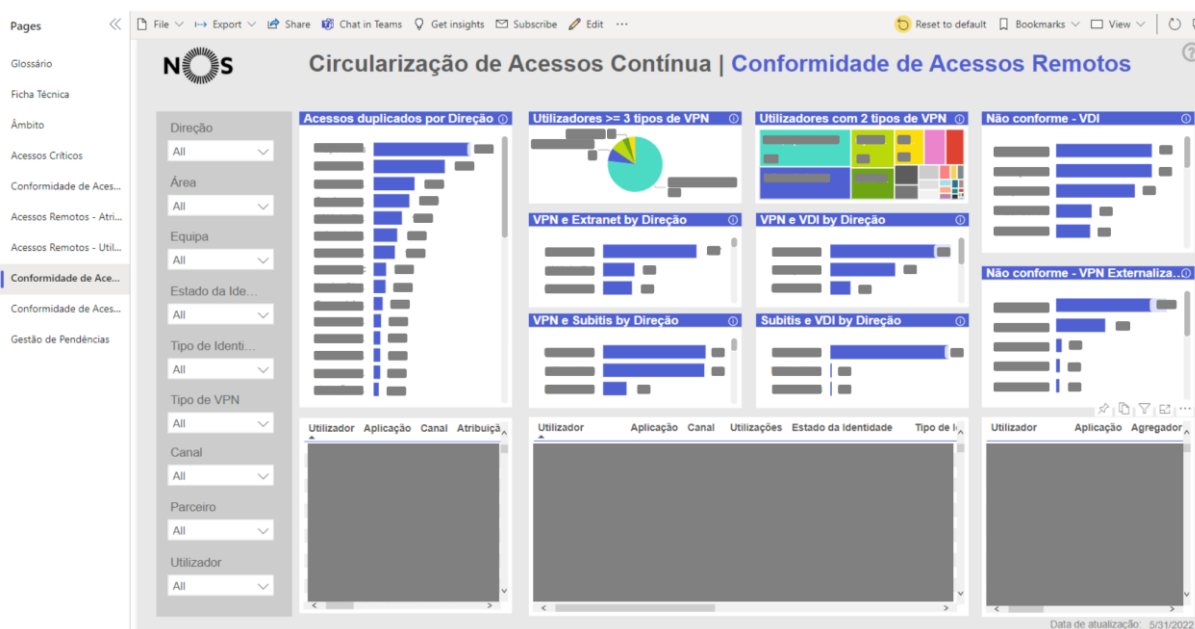


Figura 38 - Dashboard 6 - Conformidade de Acessos Remotos

Para a contagem dos acessos duplicados, foi criada a coluna “AtribuiçãoRedundante” na tabela atribuições que conta, para cada registo nesta tabela, o número de vezes que o utilizador tem atribuído o acesso em causa, para além da atribuição dessa linha. Para a contagem do número de tipos de acessos remotos de cada utilizador, criou-se a coluna “TipoVPN por User” na tabela

utilizações. Esta coluna conta o número de tipos de acessos remotos diferentes, com utilização, para cada utilizador. Para a identificação de acessos a cada par de tipos de acessos remotos, criou-se uma coluna, na tabela Utilizações, para cada um dos 4 pares cuja atribuição de acessos em simultâneo não é expectável. Estas colunas identificam a existência ou não de duplicação neste par de tipos de acessos, contando as ocorrências distintas destes acessos no mês atual. Por fim, de forma a identificar as não conformidades, nos gráficos à direita, criaram-se duas colunas na tabela Atribuições, cada uma com a respetiva regra indicada pela equipa de Segurança & Privacidade.

5.2.7 Dashboard 7 - Conformidade entre o sistema IAM e o sistema de acessos remotos

As permissões de acessos remotos, por regra, são atribuídas no sistema IAM e no sistema de gestão de acessos remotos em simultâneo. No entanto, durante a realização deste projeto detetou-se um volume proporcionalmente grande de permissões atribuídas apenas num dos sistemas. Por um lado, permissões existentes no sistema IAM, sem correspondência no sistema de gestão de acessos remotos, não garantem o acesso aos utilizadores a quem estiverem atribuídos, pelo que, em princípio, serão obsoletos. Por outro lado, permissões existentes no sistema de gestão de acessos remotos, sem correspondência no sistema IAM, garantem o acesso aos utilizadores a quem estiverem atribuídos, sem que este acesso seja visível pelo sistema IAM. Estes acessos, caso existam, como não são visíveis no sistema IAM, não serão monitorizáveis neste controlo. Assim, estes últimos são de maior relevância e prioridade de tratamento pois podem constituir um risco para o negócio.

Deste modo, esta página, apresentada na Figura 39, apenas tem interesse para as direções tecnológicas, que irão garantir a correspondência das permissões definidas no sistema IAM com as permissões definidas no sistema de acessos remotos. Assim, caso se confirme a obsolescência destas permissões, estas devem ser eliminadas, em ambos os sistemas, ou, caso se verifique a necessidade de manter alguma permissão, esta deve ser criada no sistema em que não existe, de forma a garantir a correspondência.

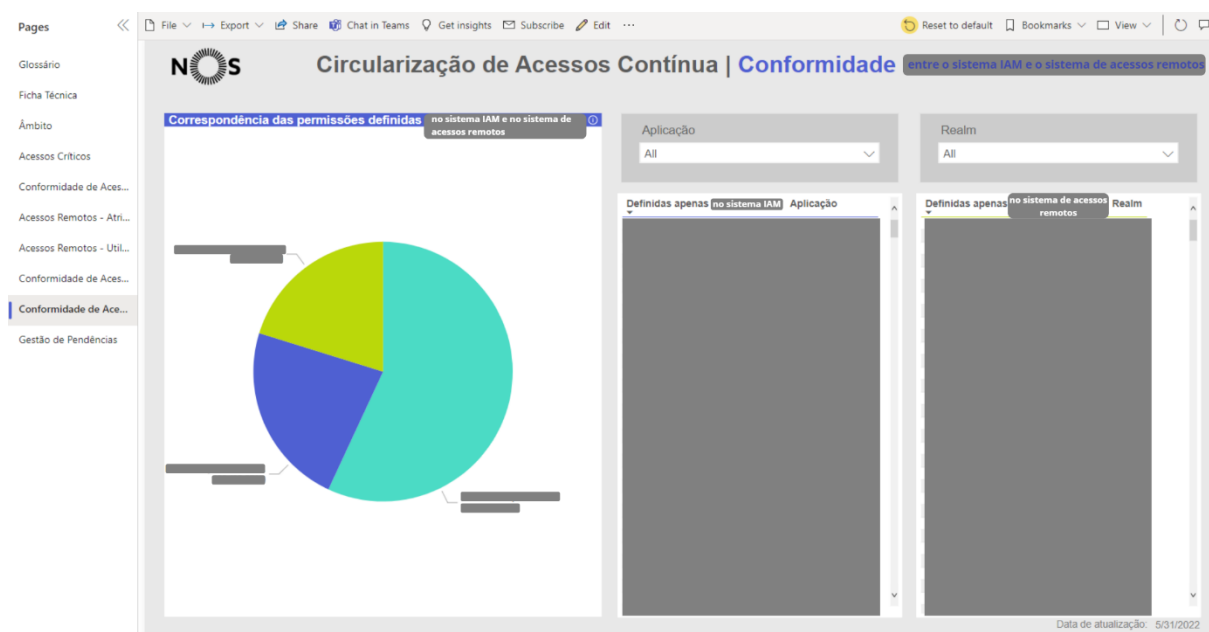


Figura 39 - Dashboard 7 – Conformidade entre o sistema IAM e o sistema de acessos remotos

De forma a efetuar a contagem de cada um dos 3 casos - permissão com correspondência, definida apenas no sistema IAM, definida apenas no sistema de gestão de acessos remotos -

criou-se uma nova tabela. Esta tabela tem 3 linhas, uma para cada um dos casos, e duas colunas, uma em que se define o caso e outra em que se faz a contagem dos casos.

5.2.8 Dashboard 8 - Gestão de Pendências

Por fim, na página apresentada na Figura 40, é feita a comunicação com os gestores de acessos de alertas identificados por CCM e é monitorizada a sua resolução. Os dados que suportam este Dashboard são independentes dos restantes e mantidos manualmente por CCM, não existindo, por isso, necessidade de qualquer tratamento adicional ou criação de novas variáveis ou contadores.

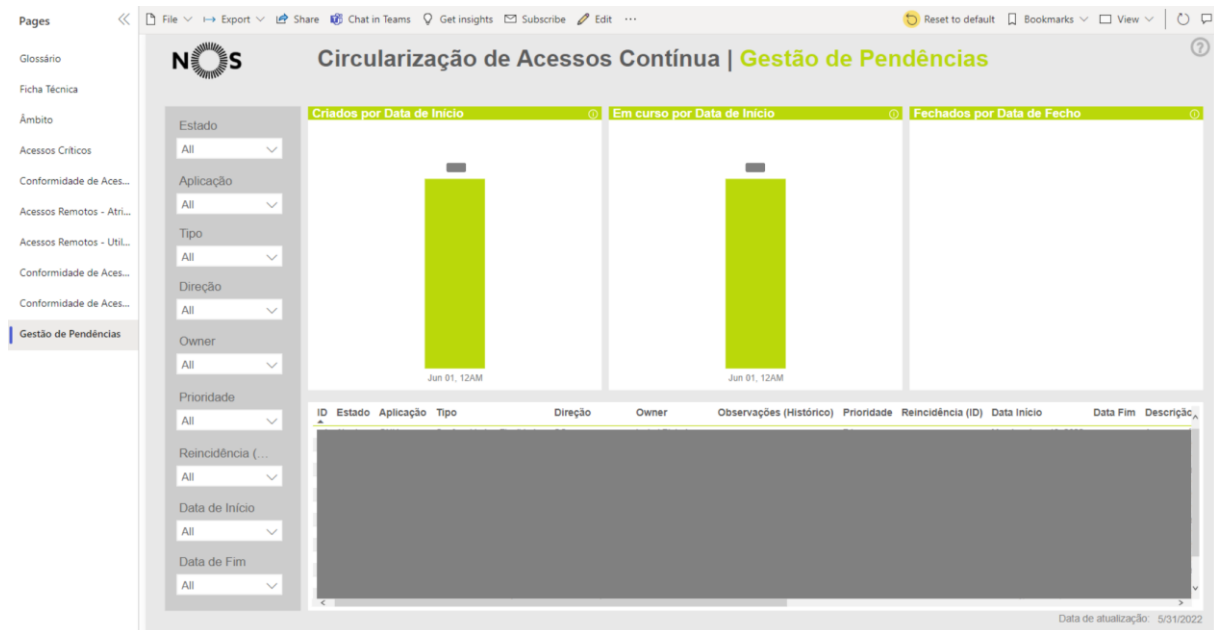


Figura 40 - Dashboard 8 - Gestão de Pendências

5.3 Execução

5.3.1 Configuração das Ferramentas

A configuração das ferramentas a utilizar ocorre de cada vez que o elemento da equipa de CCM que responsável por executar a este controlo é alterado. Esta configuração ocorre de forma a que este consiga proceder à obtenção e tratamento de dados. Para maior detalhe, consultar ANEXO C: Manual de Execução.

É necessário configurar um fluxo, em *Power Automate*, para cada processo de importação de dados de utilização das aplicações. Para cada fluxo criado, é necessário criar pastas em Outlook, com regras a estas associadas que identifiquem emails recebidos e os enviem para a pasta adequada, como demonstrado na Figura 27. É ainda necessário, para cada fluxo, criar uma pasta no *OneDrive*, onde o *Power Automate* irá alojar os ficheiros.

Por fim, no ficheiro “Agrega Ficheiros.xlsx” é necessário editar as localizações dos ficheiros a importar, bem efetuar eventuais alterações a regras de classificação das várias aplicações ou nomes das folhas a importar.

5.3.2 Recolha e tratamento de Dados

De forma a atualizar os dados nos Dashboards, é necessário proceder, mensalmente, à recolha e tratamento de dados. Para isto, a equipa de CCM deve recolher, para as várias aplicações, dados das atribuições e das utilizações dos acessos. Deve ainda recolher os dados relativos às posições dos vários utilizadores na empresa e das finalidades para a atribuição de cada acesso crítico. Sempre que necessário, deve também atualizar o ficheiro das pendências, bem como os ficheiros que categorizam as várias permissões existentes. Na prática, todos os ficheiros indicados na Figura 24 devem ser atualizados. De forma a proceder a esta atualização, a equipa de CCM deverá recorrer ao documento interno, “manual de execução”, disponível no ANEXO C: Manual de Execução.

5.3.3 Utilização do Dashboard

Após garantir a atualização dos dados, a equipa de CCM disponibiliza os Dashboards para os gestores de acessos da empresa, que os devem utilizar de forma a resolver as pendências criadas por CCM, utilizando os *use cases* indicados, para cada página. O gestor de acessos poderá observar os *use cases* de cada página, selecionando, no canto superior direito, o sinal “?”. A título de exemplo, a Figura 41 mostra os *use cases* na análise dos Acessos Críticos.

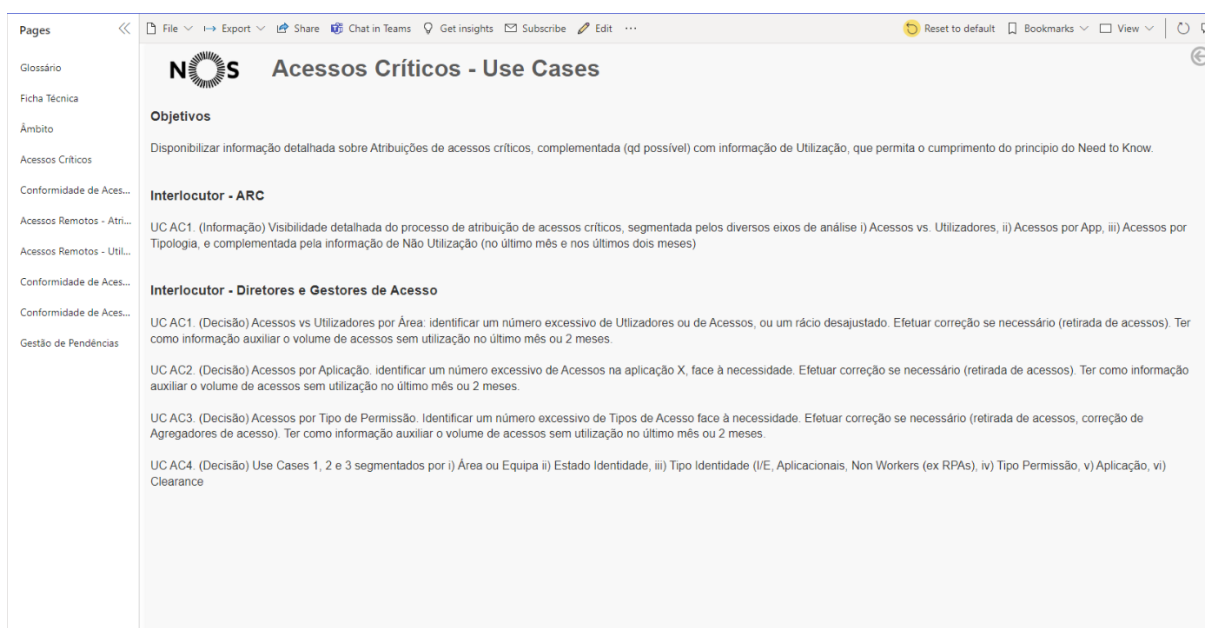


Figura 41 - Exemplo de *use cases* para os Acessos Críticos

Nota-se ainda que cada indicador ou gráfico criado possui, no canto superior direito, um “i” que, ao passar o rato por cima, mostra uma breve descrição do mesmo e eventuais instruções acerca da sua utilização.

6 Conclusões e perspetivas de trabalho futuro

Ao longo do projeto, foram desenvolvidos automatismos que agilizam o processo de recolha de dados e foi redesenhado o sistema de comunicação com os gestores de acesso, eliminando a necessidade de emails e trocas de ficheiros Excel, através da implementação de um sistema de alertas incorporado no Power BI. Foram ainda melhorados os Dashboards que permitem visualizar e analisar de forma interativa e dinâmica os dados acerca deste controlo.

O desenvolvimento do processo de execução da Circularização de Acessos Contínua teve como foco a monitorização dos acessos críticos e remotos, bem como a análise de conformidade na atribuição de ambos os acessos. No entanto, dada a crescente preocupação com a segurança e privacidade de dados e a crescente capacidade computacional alavancada através da utilização de *softwares* de BI como o *Power BI*, será de prever que, no futuro, o âmbito da Circularização de Acessos Contínua seja alargado a mais aplicações utilizadas na empresa, eventualmente tornando-se transversal a todas estas aplicações.

Por outro lado, nota-se que o controlo desenvolvido monitoriza consideravelmente mais aplicações do ponto de vista das atribuições do que é feito na ótica da utilização. Isto acontece porque para alargar o âmbito, ao nível das atribuições, basta modificar a *query* que é feita à base de dados, definindo mais aplicações âmbito. No entanto, para alargar o âmbito, ao nível das utilizações, é necessário, em primeiro lugar, mapear a forma como ocorre o registo destas utilizações, determinando, em seguida, qual a melhor forma de obter e tratar estes dados, para que se possam incorporar no registo normalizado de utilizações presente no ficheiro 2 que se pode observar na Figura 24.

Para além disso, os dados de utilização diária de aplicações exigem o processamento mensal de cerca de 30 ficheiros de dados para cada aplicação âmbito de controlo de utilização. Deste modo, o simples controlo de mais aplicações ao nível da utilização, tornaria impossível executar o controlo mensalmente sem a existência de automatismos. Por este motivo, e como até ao início deste projeto, o acesso e tratamento dos dados era efetuado de forma manual, não se considerou alargar o âmbito do controlo de utilizações.

Os desenvolvimentos efetuados durante a realização deste projeto tiveram sempre em vista a automatização e a facilidade de execução do controlo. Ao desenvolver estes automatismos, existiu ainda o cuidado e preocupação de tornar possível ajustá-los com facilidade para que fossem capazes de processar dados de novas aplicações. Assim, desenvolvimentos futuros deverão procurar alargar a monitorização das utilizações às várias aplicações âmbito da circularização, do ponto de vista das atribuições. Nota-se que, à data da escrita desta conclusão, já foi mapeado o acesso aos registos diários de uma aplicação que permite o acesso a gravações de chamadas de *contact centres*, preparando os vários automatismos para que estes consigam processar estes dados. No entanto, como CCM se encontra a receber os registos diários de utilização desta aplicação há poucos dias, ainda não possui dados suficientes para a integrar na Circularização de Acessos Contínua relativa ao mês de junho. Ainda assim, esta aplicação poderá começar a ser monitorizada em breve.

Por outro lado, o acesso aos dados de atribuições, apesar de simples, requer bastante capacidade computacional devido à quantidade de dados a que a *query* acede. Deste modo, uma possível melhoria futura passaria pela preservação dos dados do último mês, efetuando a *query* apenas ao mês mais recente.

Ao longo do projeto, foram entrevistados vários gestores de acessos, tendo sido identificados alguns problemas de conformidade, como o facto de não ser previsível a existência de acessos a certas aplicações fora de certas direções. No desenvolvimento dos Dashboards foram desenhados gráficos e indicadores que permitem identificar estes problemas. Ainda assim, deverá ser possível identificar mais problemas de conformidade e integrar gráficos e

indicadores nos Dashboards que permitam efetuar a identificação desses problemas. Assim, sugerem-se novas entrevistas aos gestores de acesso realçando a importância de detetar inconformidades. Nestas entrevistas, os gestores de acessos, que estão mais próximos do nível operacional e, por isso, têm maior conhecimento para identificar estas situações, criando regras para a atribuição de acessos. Poderão identificar, por exemplo, finalidades que só fazem sentido em determinadas aplicações ou direções para que se possa incorporar estas regras nos Dashboards.

Por fim, realça-se a importância de validar os dados recebidos das diversas fontes, analisando, sempre que necessário, detalhes que não estejam bem compreendidos. Tal é especialmente relevante sempre que se acedam a novas fontes de dados, alargando o âmbito do controlo.

Referências

- Ackoff, Russell. 1989. "From Data to Wisdom." *Journal of applied systems analysis* 16 (1): 3-9.
- Agrawal, Divyakant, Philip Bernstein, Elisa Bertino, Susan Davidson, Umeshwas Dayal, Michael Franklin, Johannes Gehrke, et al. 2011. "Challenges and Opportunities with Big Data." *Cyber Center Technical Reports*.
- ANACOM. 2022. "Factos & Números."
- Cavoukian, Ann. 2009. "Privacy by design: The 7 foundational principles." *Information and privacy commissioner of Ontario*.
- Cisco. 2021. "Cisco Privacy Benchmark Study." https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf.
- Colaps, Anna. 2017. "Big Data: Is EU Competition Law Ripe Enough to Meet the Challenge?" *60 Years of EU Competition Law: Stocktaking and Future Prospects*.
- Cukier, Kenneth, and Viktor Mayer-Schoenberger. 2013. "The Rise of Big Data: How It's Changing the Way We Think About the World." *Council on Foreign Relations* 28-40.
- Daigle, Brian, and Mahnaz Khan. 2020. "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." *Journal of International Commerce and Economics*. https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf.
- Dreamia. 2022. *Dreamia*. Accessed 2022. <https://dreamia.pt/>.
- Duarte, João Carlos Assunção. 2012. *Dashboard Visual, Uma ferramenta de Business Intelligence*. Dissertação de Mestrado, Porto: Faculdade de Engenharia da Universidade do Porto.
- Furht, Borko, and Flavio Villanustre. 2016. "Introduction to Big Data." *Big Data Technologies and Applications* 3-11. doi:https://doi.org/10.1007/978-3-319-44550-2_1.
- Gahi, Youssef, Mouhcine Guennoun, and Hussein Mouftah. 2016. "Big Data Analytics: Security and privacy challenges." *IEEE Symposium on Computers and Communication (ISCC)* 952-957.
- Gartner. 2022. "Gartner Magic Quadrant for Analytics and Business Intelligence Platforms."
- Huang, Lan. 2019. "Building A Sales Dashboard for A Sales Department by using Power BI." *Laurea University of Applied Sciences*.
- IBM Marketing Cloud. 2017. "10 Key Marketing Trends For 2017."
- Ion-Petru, Cătălin Alexandru, and Mădălina Ecaterina. 2015. "Identity and access management- a risk-based approach." *International Management Conference, Proceedings of the 9th*.
- Madureira, Vitor João Constantino. 2010. *Modelo de Gestão de Identidades e Acessos*. Dissertação de Mestrado, Faculdade de Engenharia da Universidade do Porto.
- NOS. 2022. *NOS - Estrutura Acionista*. Accessed 2022. <https://www.nos.pt/institucional/PT/investidores/nos-em-bolsa/Paginas/estrutura-acionista.aspx>.
- NOS. 2021. "Relatório e Contas."

- Oussous, Ahmed, Fatima-Zahra Benjelloun, Ayoub Ait Lahcen, and Samir Belfkih. 2018. "Big Data technologies: A survey." *Journal of King Saud University - Computer and Information Sciences* 30 (4): 431-448. doi:<https://doi.org/10.1016/j.jksuci.2017.06.001>.
- Pauwels, Koen, Tim Ambler, Bruce H. Clark, Pat LaPointe, David Reibstein, Bernd Skiera, Berend Wierenga, and Thorsten Wiesel. 2009. "Dashboards as a Service: Why, What, How, and What Research Is Needed?" *Journal of Service Research* 175–189.
- Presthus, Wanda, and Hanne Sørsum. 2018. "Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation." *Procedia Computer Science* 138: 603-611. doi:<https://doi.org/10.1016/j.procs.2018.10.081>.
- Romanou, Anna. 2018. "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise." *Computer Law & Security Review* 34 (1): 99-110. doi:<https://doi.org/10.1016/j.clsr.2017.05.021>.
- Sagiroglu, Seref, and Duygu Sinanc. 2013. "Big data: A review." *International Conference on Collaboration Technologies and Systems (CTS)* 42-47. doi:10.1109/CTS.2013.6567202.
- Samonas, Spyridon, and David Coss. 2014. "The CIA strikes back: Redefining confidentiality, integrity and availability in security." *Journal of Information System Security* 10 (3).
- Tegarden, David P. 1999. "Business Information Visualization." *Communications of the Association for Information Systems* 1 (4).
- Tredinnick, Luke. 2022. "Ubiquitous information." *Business Information Review* 39 (1): 9-11. doi:10.1177/02663821221088893.
- ZAP. 2022. ZAP. Accessed 2022. <https://www.zap.co.ao/sobre-a-zap/a-zap>.

7 ANEXO A: Processo AS IS



Monitorização Contínua de Acessos Críticos: Modelo AS IS

1 de Abril de 2022

Aviso: A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS SGPS, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Data:	1 de Abril de 2022	Proprietário:	João Lopes / Compliance Corporativa e Monitorização
Versão:	V2.0	Aprovado por:	
Classificação:	USO INTERNO	Lista de distribuição:	

Monitorização Contínua de Acessos Críticos: Modelo AS IS



Índice

1. Introdução.....	4
1.1. Circularização de Acessos Críticos.....	4
1.1.1. Objetivos.....	4
1.1.2. Âmbito.....	4
1.1.3. Responsabilidades.....	4
1.2. Monitorização de Acessos Remotos.....	5
1.2.1. Objetivos.....	5
1.2.2. Âmbito.....	5
1.2.3. Responsabilidades.....	6
2. Circularização de Acessos Críticos	7
2.1. Aspetos Gerais do Processo	7
2.1.1. Parâmetros do Processo.....	7
2.1.2. Indicadores Utilizados nos Dashboards	7
2.1.3. Fluxograma.....	10
2.1.4. Fluxo de Informação	10
2.2. Recolha e tratamento da informação	11
2.2.1. Tabela RACI	13
2.2.2. Narrativa	13
2.2.3. Fluxograma.....	14
2.3. Criação / Atualização dos Dashboards	15
2.3.1. Tabela RACI	15
2.3.2. Narrativa	15
2.3.3. Fluxograma.....	16
2.4. Validação ou remoção de acessos.....	17
2.4.1. Tabela RACI	17
2.4.2. Narrativa	17
2.4.3. Fluxograma.....	18
2.5. Elaboração do Relatório	19
2.5.1. Tabela RACI	19
2.5.2. Narrativa	19
2.5.3. Fluxograma.....	20
2.6. Conclusões e Ineficiências.....	21
3. Monitorização de Acessos Remotos	22
3.1. Aspetos Gerais do Processo	22
3.1.1. Parâmetros do Processo.....	22

DOCUMENTO USO INTERNO

2/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.1.2. Fontes de Informação.....	22
3.1.3. Fluxo de Informação	23
3.1.4. Detalhe das bases de dados	23
3.1.5. Indicadores Utilizados	24
3.1.6. Fluxograma	28
3.2. Recolha e tratamento da informação	29
3.2.1. Tabela RACI	29
3.2.2. Narrativa	29
3.2.3. Fluxograma	30
3.3. Criação / Atualização dos Dashboards	31
3.3.1. Tabela RACI	31
3.3.2. Narrativa	31
3.3.3. Fluxograma	32
3.4. Análise e Validação de Resultados	33
3.4.1. Tabela RACI	33
3.4.2. Narrativa	33
3.4.3. Fluxograma	34
3.5. Elaboração do Relatório	35
3.5.1. Tabela RACI	35
3.5.2. Narrativa	35
3.5.3. Fluxograma	35
3.6. Conclusões e Ineficiências	36
4. Conclusões Gerais.....	36
5. ANEXO A: Query [REDACTED].....	37
6. ANEXO B: Query [REDACTED] (IAM).....	37
7. ANEXO C: Configuração [REDACTED].....	38
8. ANEXO D: Configuração [REDACTED] (IAM).....	38

DOCUMENTO USO INTERNO

3/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



1. Introdução

O presente relatório foi escrito no âmbito de um projeto da área de Compliance Corporativa e Monitorização (CCM), através do qual se pretende criar um processo único de Monitorização Contínua de Acessos Críticos que dê resposta a todas as necessidades das diferentes áreas.

A Monitorização Contínua de Acessos Críticos é atualmente constituída pelos seguintes controlos:

- Circularização de Acessos Críticos – Controlo responsável pela identificação e remoção de acessos, definidos como críticos pela área de Privacidade & Segurança, que não são necessários à execução das funções exercidas por cada um dos utilizadores. É também responsável pela validação dos acessos críticos a manter, havendo um registo da justificação utilizada (Finalidade) para a manutenção destes acessos. Este controlo é atualmente executado por CCM.
- Monitorização de Acessos Remotos – Controlo responsável pela monitorização da utilização diária e atribuição dos acessos remotos (com base na informação de IAM). Este controlo produz um conjunto de indicadores, através dos quais é possível identificar os acessos atribuídos sem utilização. Este controlo é atualmente executado por AS.

Estes dois controlos têm objetos de estudo, destinatários e bases de dados semelhantes. Assim, acredita-se ser possível explorar sinergias e melhorar o desempenho, agregando estes controlos numa ferramenta única.

1.1. Circularização de Acessos Críticos

1.1.1. Objetivos

De forma a garantir a privacidade dos clientes, a Circularização de Acessos tem como objetivos:

- Cumprir com o princípio *Need to Know*: apenas terão acesso aos dados pessoais os colaboradores cujas respetivas funções assim o exijam.
- Identificar os utilizadores que têm acesso a um conjunto de permissões identificadas como críticas e promover, junto dos Gestores de Acesso das respetivas áreas, a análise e correção das situações que necessitem de ajuste.
- Acompanhar e monitorizar o processo de correção.

1.1.2. Âmbito

A Circularização de Acessos tem como âmbito as seguintes informações sensíveis, obtidas através das respetivas aplicações:

- Tráfego detalhado não mascarado ([REDACTED])
- Apagamento a pedido de cliente ([REDACTED])
- Audição e download de chamadas gravadas ([REDACTED])

1.1.3. Responsabilidades

DOCUMENTO USO INTERNO

4/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



Compliance Corporativa e Monitorização (CCM):

- Criar e garantir a manutenção dos dashboards
- Obter e tratar os dados
- Importar os dados para o Power BI
- Assegurar o fluxo de informação com os gestores de acessos
- Atualizar os dashboards com as respostas dos gestores de acessos
- Analisar e validar os resultados

Owners da Informação: Fornecer acesso à informação das aplicações nas quais CCM não tem autonomia de acesso.

Diretores das Áreas: Decidir manter ou revogar os acessos.

Gestores de Acesso: Análise dos dashboards e correção dos acessos em IAM.

1.2. Monitorização de Acessos Remotos

A pandemia COVID-19 e a consequente remotização dos postos de trabalho, resultou no aumento do risco inerente dos controlos implementados e na necessidade de reforçar os atuais controlos MA. Em resposta, a equipa ARC/AS efetuou uma revisão profunda do processo de Monitorização de Acessos, da qual fez parte a construção de novos controlos de monitorização da capacidade, utilização e atribuição dos canais remotos disponíveis na empresa.

1.2.1. Objetivos

Este controlo tem como objetivos:

- Identificar padrões de utilização e atribuição de acessos
- Eliminar segregação de canais de atribuição de acessos
- Eliminar acessos não utilizadas
- Eliminar agregadores adicionais obsoletos

1.2.2. Âmbito

A Monitorização de Acessos Remotos tem como âmbito os registos de acessos obtidos nos seguintes sistemas:

- VPN Corporativa (██████████)
 - Plataforma que suporta o acesso remoto dos utilizadores corporativos e permite o acesso remoto aos servidores que suportam o negócio que se encontram no ██████████ e ██████████.
- VPN Tecnológica (██████████)
 - Plataforma semelhante à ██████████ que suporta o acesso remoto dos utilizadores corporativos. É de utilização exclusiva pelas equipas de suporte, de forma a garantir acesso permanente (acesso redundante) aos servidores

DOCUMENTO USO INTERNO

5/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



da empresa, ainda que um dos acessos possa estar temporariamente indisponível.

- VDI Checkpoint
 - Plataforma de acesso à rede interna quando em Call-Centers externalizados. A plataforma checkpoint de acesso remoto tem 2 clusters redundantes entre [REDACTED] e [REDACTED].

Nota-se que, do ponto de vista de risco, a VDI Checkpoint é um acesso mais restritivo e, por isso, que representa menor risco para a NOS.

Nota-se ainda que, dentro da VPN Corporativa, existe um canal que é mais restritivo que os restantes: a [REDACTED]; representando, por isso, menor risco para a empresa que os restantes canais, ainda que represente maior risco que a VDI Checkpoint.

Deste modo, como se pretende uma correta gestão de risco dos vários acessos remotos, é necessário tratar os diferentes graus de risco de forma diferenciada.

1.2.3. Responsabilidades

Auditoria de Sistemas (AS):

- Obter e tratar os dados
- Importar os dados em Power BI
- Desenvolver e manter os dashboards
- Analisar e validar os resultados

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2. Circularização de Acessos Críticos

2.1. Aspetos Gerais do Processo

2.1.1. Parâmetros do Processo

Periodicidade: Anual

Entradas:

- Evolução histórica de Circularizações de Acessos
 - Ficheiros Excel de circularizações anteriores
- Lista de Identidades em IAM
 - Extraída da Base de Dados por SAP BO
- Lista das permissões elegíveis para Circularização de Acessos
 - Definidas por CCM
- Lista de acessos (permissões por identidade) atribuídos por aplicação
 - Extraída da Base de Dados por SAP BO
- Registo de utilização de permissões críticas por utilizador para as aplicações [REDACTED]
 - Processado por AS através de [REDACTED]

Saídas:

- Acessos IAM atualizados
- Relatório de Circularização de Acessos

Subprocessos:

- Recolha e tratamento da informação
- Criação / Atualização dos dashboards
- Validação ou remoção de acessos
- Elaboração do relatório

Ferramentas e sistemas de suporte:

- IAM
- Excel
- Power BI
- SAP BO para extração de informação da Base de Dados

2.1.2. Indicadores Utilizados nos Dashboards

Nota-se que Acesso é a designação dada ao par do utilizador e de cada permissão de acesso a este atribuído.

DOCUMENTO USO INTERNO

7/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



Tipo de Indicadores	Indicadores	Exemplo
Gerais	Número de aplicações âmbito Número de direções âmbito Número de utilizadores Número de acessos Percentagem de acessos a manter e a remover	
Por Direção	Número de utilizadores Número de acessos Número de acessos a manter e a eliminar Top 5 finalidades dos acessos Número de acessos sem utilização por aplicação Número de acessos a manter e a eliminar por aplicação Número de acessos circularizados com e sem resposta Número de acessos por tipo	

DOCUMENTO USO INTERNO

8/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



Indicadores por direção relativos ao ano anterior	Número de acessos Número de acessos a manter e a eliminar Número de acessos a manter e a eliminar por aplicação Número de acessos por tipo	
Indicadores de estado	Percentagem de acessos com resposta, por aplicação Percentagem de acessos sem resposta, por aplicação Número de acessos com resposta, por direção Número de acessos sem resposta, por direção	
Filtros	Evento (ano da informação em análise) Direção Estado (ativo, suspenso ou suspenso por prova de vida) Aplicação Tipo de permissão Código da permissão Utilizador	

DOCUMENTO USO INTERNO

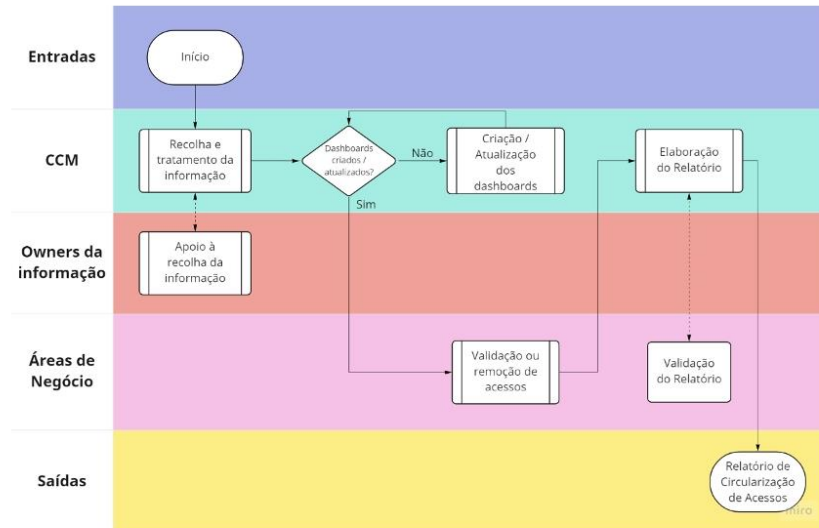
9/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

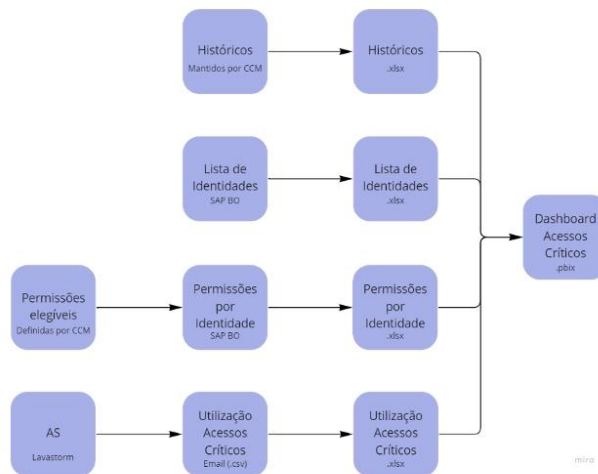
Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.1.3. Fluxograma



2.1.4. Fluxo de Informação



DOCUMENTO USO INTERNO

10/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.2. Recolha e tratamento da informação

Neste subprocesso ocorre a recolha e preparação da informação necessária ao desenvolvimento dos dashboards.

Podemos agrupar esta informação em duas categorias:

- Informação a que CCM tem acesso:
 - **Lista das permissões elegíveis para Circularização de Acessos**
 - Formato: Microsoft Excel
 - Detalhe: Lista com os nomes das permissões que serão âmbito da Circularização de acessos definida por CCM durante a definição dos requisitos de CCM.
 - Variáveis obtidas:
 - APP: Nome da aplicação a circularizar
 - TIPO_PERMISSAO: Categoria da permissão crítica. Pode ser de acesso a detalhe de comunicações, audição de chamada ou download de chamada, e apagamento de dados pessoais.
 - PERMISSAO: Nome da permissão
 - FUNC_PERMISSAO: Descrição da permissão
 - **Lista de Identidades em IAM**
 - Formato: SAP BO
 - Variáveis Obtidas:
 - TIPO_IDENTIDADE: Tipo de identidade registada em IAM. Pode ser interna, externa, aplicacional ou non worker
 - ESTADO_IDENTIDADE: A identidade pode estar ativa, inativa, suspensa ou suspensa por prova de vida
 - NUM_COLAB: Representa o ID da identidade
 - NOME_COLAB: Nome do colaborador, da aplicação ou do robot
 - USER_NT: Username utilizado pela identidade
 - DIRECAO: Direção a quem reporta a identidade
 - AREA: Área da identidade
 - EQUIPA: Equipa da identidade
 - LOC_TRAB: Local de operações da identidade
 - EMAIL: Email da identidade
 - EMAIL_SEC: Email secundário da identidade
 - MSISDN: Contacto da identidade
 - **Evolução histórica de Circularizações de Acessos**

DOCUMENTO USO INTERNO

11/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



- Formato: Microsoft Excel
 - Detalhe: Base de dados de Circularizações de acessos passadas, que compila e associa as identidades registadas em IAM às permissões críticas que lhes estão atribuídas e à justificação dada pelo gestor de acessos da área para a manutenção desse acesso, ou a respetiva indicação para remoção do mesmo. Contém ainda uma variável que indica se cada um dos acessos (associado a um utilizador) foi alvo de circularização nesse ano e, em caso afirmativo, se obteve resposta/justificação por parte da respetiva área.
- **Lista de permissões atribuídas por identidade**
 - Formato: SAP BO
 - Detalhe: Relaciona as identidades registadas em IAM com as permissões críticas que lhes estão atribuídos e que são âmbito da presente circularização de acessos, de acordo com as variáveis referidas anteriormente.
- Informação a que CCM não tem acesso diretamente, sendo necessário efetuar um pedido de recolha ao departamento responsável por esta informação, individualmente para cada aplicação:
 - **Registo de utilização de acessos críticos**
 - Formato: Microsoft Excel
 - Detalhe: É feito um pedido ao owner (AS) das bases de dados de [REDACTED] e [REDACTED] para a obtenção de uma base de dados que associe o utilizador a cada uma das permissões críticas a ele associadas e ao número de vezes que fez uso da mesma nos últimos 3 meses. O owner extrai os dados através de [REDACTED]. É enviado trimestralmente por email apesar de existir uma execução mensal de metadados e de ser possível a partilha direta pelas pastas partilhadas.

Em todas as bases de dados indicadas foi ainda acrescentada uma variável que indica o mês e o ano da circularização de acessos a que diz respeito.

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.2.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nfornado.

Atividades\ Funções→	CCM	Owners da Informação
1. Definição dos requisitos de CCM	A/R	
2. Pedido de acesso à informação	A/R	I
2.1. Cedência da informação	I	A/R
3. Extração da informação	A/R	
4. Tratamento da informação	A/R	

2.2.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Definição dos requisitos	Definição dos requisitos do controlo, nomeadamente do âmbito da monitorização e do plano de execução. Inclui requisitos CCM e das áreas.	Gestão (corrente) de Acessos lógicos	Requisitos de Plano de Execução	CCM
2.	Pedido de acesso à informação	CCM contacta os owners da informação para que estes lhe disponibilizem os dados necessários	Gestão (corrente) de Acessos lógicos	Emails para os owners	CCM
2.1.	Cedência da informação	Os owners da informação processam o pedido, enviando ficheiros no formato Microsoft Excel para CCM	Emails com os pedidos de informação	Ficheiros de dados	Owners da Informação
3.	Extração da informação	CCM extrai a informação que já lhe estava acessível e guarda numa pasta, à qual acrescenta os restantes dados, à medida que estes lhes são disponibilizados pelos owners	Gestão (corrente) de Acessos lógicos	Ficheiros de dados	CCM
4.	Tratamento da informação	Normalização das várias bases de dados de forma a que possam ser incorporados em Power BI	Ficheiros de dados	Base de dados normalizada	CCM

DOCUMENTO USO INTERNO

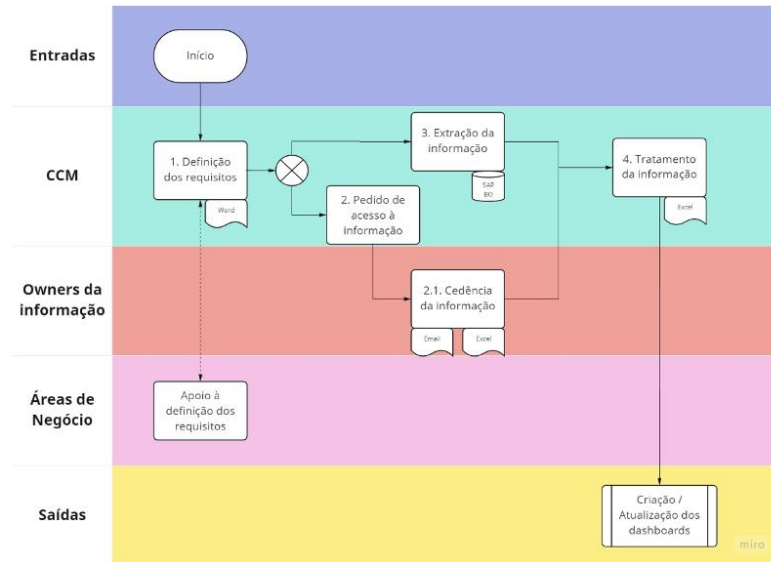
13/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.2.3. Fluxograma



DOCUMENTO USO INTERNO

14/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.3. Criação / Atualização dos Dashboards

Este subprocesso ocorre em dois momentos: no momento da primeira implementação da circularização de acessos, em que ainda não existiam dashboards e é, por isso, necessário criá-los; e sempre que CCM considere necessário atualizar/desenvolver os dashboards.

O objetivo é a criação de uma ferramenta que permita aos diretores e aos gestores de acesso das diversas áreas analisar os acessos sob a sua responsabilidade, bem como receber alertas de potenciais acessos obsoletos ou incorretamente atribuídos. É, por isso, de extrema importância a recolha, por parte de CCM, das necessidades e sugestões dos restantes stakeholders.

2.3.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nformado.

Funções→	CCM	Diretores	Gestores de Acesso
Atividades↓			
1. Definição dos requisitos das áreas	A/R	C	C
2. Desenho dos dashboards	A/R		
3. Validação dos dashboards	A	R	C
4. Melhoria dos dashboards	A/R		

2.3.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Desenho dos dashboards	CCM desenha os dashboards com base nos requisitos	Pasta com bases de dados normalizadas	Versão inicial dos dashboards	CCM
2.	Validação dos dashboards	CCM contacta algumas áreas para que estas validem os dashboards e indiquem melhorias ou correções a efetuar	Versão inicial dos dashboards	Lista de sugestões de melhoria das áreas	CCM e Áreas Negócio
3.	Melhoria dos dashboards	CCM melhora a versão inicial dos dashboards com base nas sugestões feitas pelas áreas	Versão inicial dos dashboards; Lista de sugestões de melhoria das áreas	Versão final dos dashboards	CCM

DOCUMENTO USO INTERNO

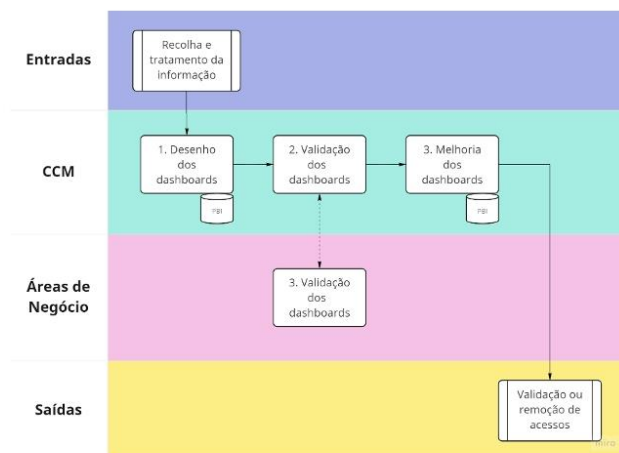
15/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.3.3. Fluxograma



DOCUMENTO USO INTERNO

16/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.4. Validação ou remoção de acessos

Neste subprocesso, os gestores de acesso analisam os dashboards de forma a validar a manutenção/remoção dos acessos atribuídos a cada um dos utilizadores da sua área. Este processo é desempenhado em contacto com o diretor da respetiva área.

2.4.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nfornado.

Funções→	CCM	Diretores	Gestores de Acesso
Atividades↓			
1. Envio da Circularização de Acessos	A/R	I	I
2. Análise dos dashboards		A	R
1.1. Remoção de Acessos Indesejados		A	R
1.2. Validação dos Acessos a Manter		A	R
2. Envio do ficheiro Excel preenchido	I	C	A/R

2.4.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Envio da Circularização de Acessos	CCM envia a versão final dos dashboards para os Diretores e Gestores de Acesso das áreas.	Versão final dos dashboards	Dashboards disponíveis na cloud Comunicação para os diretores e gestores de acesso	CCM
2.	Análise dos dashboards	O Diretor de cada área efetua a análise dos dashboards recebidas, com o apoio do gestor de acessos da área	Versão final dos dashboards	Conclusões da análise	Diretores
3.1.	Justificação dos Acessos a Manter	O Gestor de Acessos de cada área justifica os acessos a manter, no ficheiro Excel criado para esse efeito (Finalidade)	Conclusões da análise	Ficheiro Excel para a justificação das finalidades preenchido	Gestores de Acessos
3.2.	Remoção de Acessos Indesejados	O gestor de acessos de cada área remove os acessos indesejados diretamente na plataforma IAM	Conclusões da análise	Acessos indesejados removidos	Gestores de Acessos

DOCUMENTO USO INTERNO

17/38

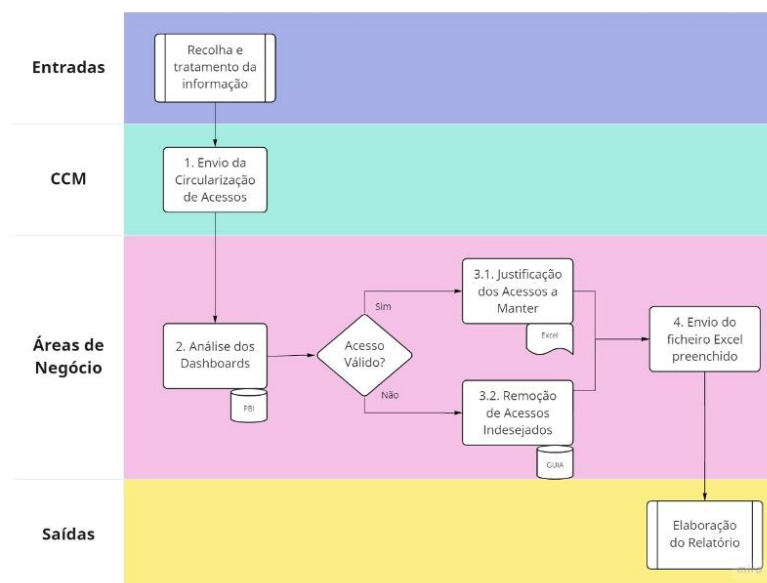
A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



4.	Envio do ficheiro Excel preenchido	O diretor de cada área valida as justificações registadas pelo gestor de acessos. Este envia o ficheiro Excel para CCM	Ficheiro Excel preenchido	Email com o ficheiro Excel preenchido	Gestores de Acesso
----	------------------------------------	--	---------------------------	---------------------------------------	--------------------

2.4.3. Fluxograma



DOCUMENTO USO INTERNO

18/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.5. Elaboração do Relatório

Por fim, o relatório é redigido, tirando conclusões acerca da monitorização efetuada e deixando algumas indicações para auxiliar futuras monitorizações, nomeadamente acerca das reincidências. Se aplicável, é definido um plano de ação (com responsabilidades e timings definidos).

2.5.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nformado.

Atividades↓	Funções→	CCM	Áreas de Negócio
1. Atualização dos dashboards		A/R	
2. Elaboração do Relatório		A/R	I
3. Validação do Relatório		I	A/R

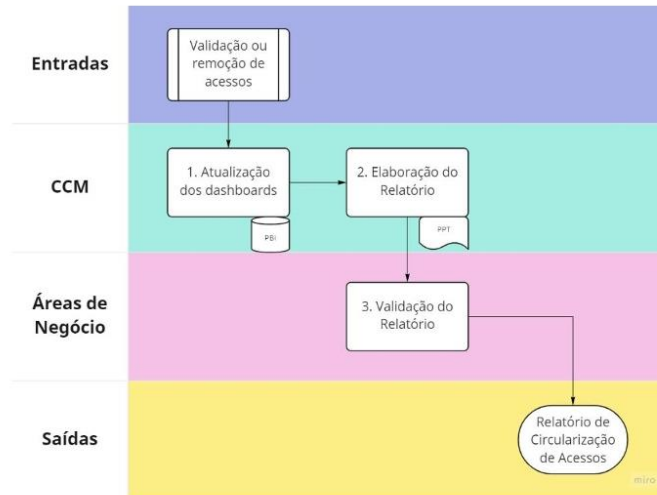
2.5.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Atualização dos dashboards	CCM atualiza os dashboards com base na informação enviada pelos diretores	Ficheiro Excel preenchido	Dashboard atualizada	CCM
2.	Elaboração do Relatório	CCM elabora o relatório de circularização de acessos, salientando quantos acessos foram mantidos e quantos foram sinalizados para remoção	Dashboard atualizada	Relatório	CCM
3.	Validação do Relatório	As áreas de negócio validam o relatório e informam CCM	Relatório	Relatório validado	Diretores das áreas

Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.5.3. Fluxograma



Monitorização Contínua de Acessos Críticos: Modelo AS IS



2.6. Conclusões e Ineficiências

Recolha e tratamento da informação

O processo de recolha de dados, o seu tratamento e a sua importação para Power BI é manual, moroso e repetitivo a cada repetição anual da Circularização de Acessos.

Assim, deve ser estudada a possibilidade de automatização total ou parcial deste processo, potenciando dessa forma a sua realização com maior frequência.

Se tal for possível, o acesso automatizado, em tempo real, às fontes de informação, permitirá a monitorização contínua dos acessos, com o mínimo esforço por parte de CCM.

Validação ou remoção de acessos

Os diretores e os gestores de acesso tomam a decisão de remover ou de manter, justificando, cada um dos acessos críticos da sua área. Após analisarem o seu dashboard, exportam um ficheiro Excel onde preenchem manualmente as justificações para a manutenção de acessos críticos.

As justificações deveriam ser dadas diretamente em IAM e, se possível, automaticamente incorporadas nos dashboards.

Elaboração do Relatório

Os acessos críticos indicados como não necessários têm que ser posteriormente removidos, em IAM, pelo gestor de acessos da área respetiva.

Esta remoção dos acessos nem sempre acontece e não existe qualquer monitorização da mesma.

Deste modo, as reincidências (acessos indicados para remoção que se encontram ativos) deveriam ser monitorizadas, emitindo um alerta periódico aos gestores de acesso que poderia ser na forma de um email automáticos, gerado após a deteção da ocorrência.

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3. Monitorização de Acessos Remotos

3.1. Aspetos Gerais do Processo

3.1.1. Parâmetros do Processo

Periodicidade do controlo: Mensal

Entradas:

- Listagem de identidades registadas na plataforma IAM
- Lista de permissões para cada um dos acessos remotos
- Lista das acessos remotos associados a cada uma das identidades (por restrições técnicas esta informação é delimitada a duas datas – primeiro dia do mês corrente e do mês anterior)
- Dados de utilização dos acessos remotos dos últimos 3 meses

Saídas:

- Dashboards de monitorização da utilização de acessos remotos face à capacidade
- Dashboards de monitorização dos acessos sem utilização
- Alterações na capacidade dos VPNs
- Acessos removidas
- Relatório

Subprocessos:

- Recolha e tratamento da informação
- Criação / Atualização dos dashboards
- Análise e Validação de resultados
- Elaboração do Relatório

Ferramentas e sistemas de suporte:

- IAM
- Excel
- Power BI
- SQL Developer (para recolha de informação na base de dados ██████████)
- DBeaver (para recolha de informação na base de dados ██████████)

3.1.2. Fontes de Informação

Os dados relativos aos registos de utilização dos acessos remotos é enviado diariamente, por email, para AS pela equipa ██████████, responsável pela administração dos sistemas SIEM (VPN Corporativa e VPN Tecnológica) e CLM(VDI Checkpoint).

Os dados relativos à atribuição de acessos são obtidos diretamente por AS, via SQL Developer para os dados relativos à plataforma IAM e via DBeaver para os dados relativos à VPN Corporativa.

DOCUMENTO USO INTERNO

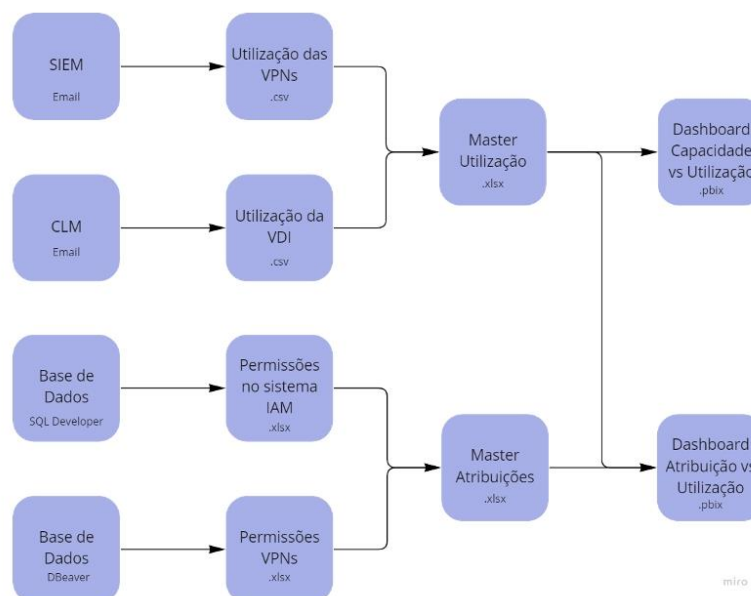
22/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.1.3. Fluxo de Informação



3.1.4. Detalhe das bases de dados

- **Master_AtribuiçõesIAM:** Associa as permissões aos utilizadores
 - DATA: Dia do controlo ou 1 mês antes
 - IAM_USER_NAME: Nome do utilizador
 - STATUS_DSC: Estado da identidade (Ativo ou Suspenso por Prova de Vida)
 - IDENTITY_TYPE_DSC: Tipo de identidade (Interna, Externa, Aplicacional, Non Worker)
 - CREATION_DAT: Data e hora de criação da permissão
 - APPLICATION_DSC: Tipo de acesso VPN permitido
 - AGGREGATOR_NAME: Nome do agregador adicional que confere a permissão
 - PERMISSION_NAME: Nome da permissão
 - AGGREGATOR_TYPE_ID: Indica se a atribuição foi feita por agregador adicional (1) ou por perfil funcional (2)
 - DIRECTION_DSC: Direção a que a identidade reporta
 - AREA_DSC: Área funcional da identidade
 - TEAM_DSC: Equipa da Identidade
 - FUNCTION_DSC: Função da Identidade
 - PARTNER_DSC LOCATION_DSC: Localização da identidade

DOCUMENTO USO INTERNO

23/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS

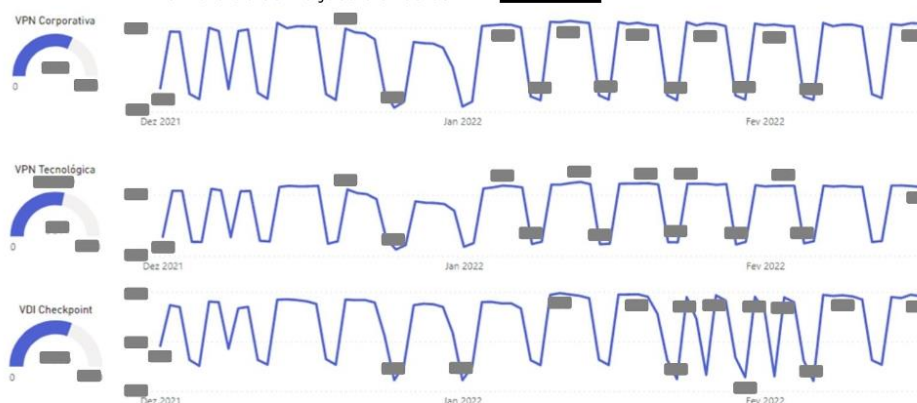


- **Master_PermissõesVPN:** Lista de todas as permissões existentes e descontinuadas
 - Data Inicio: Data de criação da permissão
 - Data Fim: Data de descontinuação da permissão (caso exista)
 - Elegibilidade: Sim se a permissão estiver ativa (Data Fim inexistente) ou Não se estiver descontinuada (Data Fim Existente)
 - Tipo VPN: Tipo de acesso VPN permitido
 - Permissão IAM: Nome da permissão
 - Aplicação
 - Descrição
 - Comentários
- **Master_UtilizaçãoVPN_VDI:** Lista de acessos utilizados pelas identidades
 - User: Nome da identidade
 - Network: Rede utilizada no acesso
 - VPN Type: Acesso utilizado (em todas as VPNs)
 - Date: Data e hora do acesso

3.1.5. Indicadores Utilizados

Capacidade vs Utilização

- Número de utilizações diárias da VPN Corporativa (██████████)
- Número de utilizações diárias da VPN Tecnológica (██████████)
- Número de utilizações diárias da VDI (██████████)



Atribuições vs Utilização VPN

- Número de acessos remoto com utilização nos últimos 3 meses por tipo de VPN
- Número de acessos remoto sem utilização nos últimos 3 meses por tipo de VPN
- Número de colaboradores com utilização nos últimos 30 dias
- Número de colaboradores cuja última utilização ocorreu há mais de 30, mas menos de 60 dias

DOCUMENTO USO INTERNO

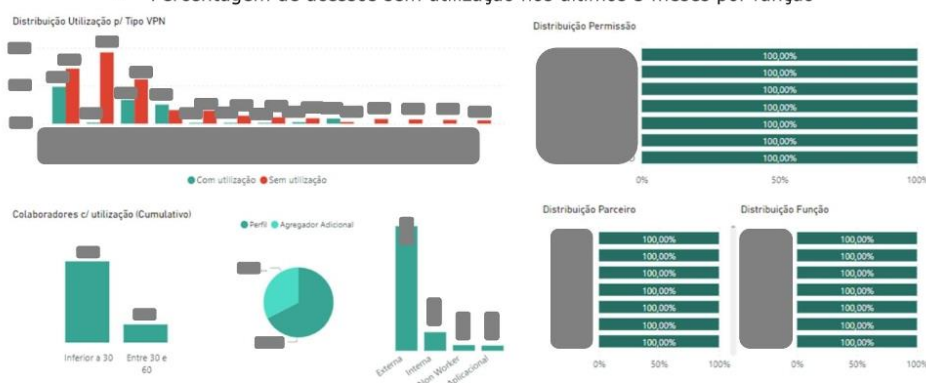
24/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



- Percentagem de acessos atribuídos através de perfil funcional
- Percentagem de acessos atribuídos através de agregador adicional
- Número de acessos atribuídos por tipo de VPN
- Percentagem de acessos com utilização nos últimos 3 meses por permissão
- Percentagem de acessos sem utilização nos últimos 3 meses por permissão
- Percentagem de acessos com utilização nos últimos 3 meses por parceiro
- Percentagem de acessos sem utilização nos últimos 3 meses por parceiro
- Percentagem de acessos com utilização nos últimos 3 meses por função
- Percentagem de acessos sem utilização nos últimos 3 meses por função



Arquitetura VPN TO BE

Neste dashboard foram utilizados indicadores de melhoria da arquitetura da gestão de acessos remotos, úteis no desenvolvimento da mesma num período de extremo aumento de utilizadores.

Arquitetura VPN AS IS

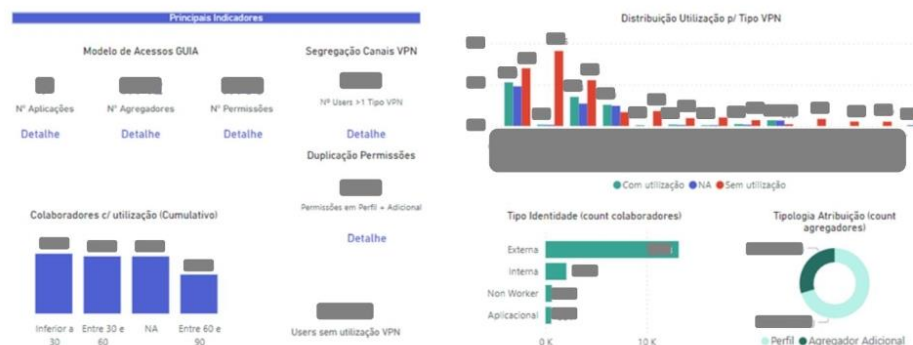
- Número de aplicações em IAM
- Número de agregadores em IAM
- Número de permissões em IAM
- Número de utilizadores com mais do que uma permissão de acesso remoto
- Número de permissões simultaneamente em perfil e em agregador adicional
- Número de acessos sem utilização
- Número de acessos com utilização por período temporal, em classes de 30 dias
- Distribuição de utilização por tipo de VPN
- Número de identidades por tipo (interna, externa, non worker, aplicacional)
- Percentagem de acessos atribuídos por perfil funcional
- Percentagem de acessos atribuídos por agregador adicional

DOCUMENTO USO INTERNO

25/38

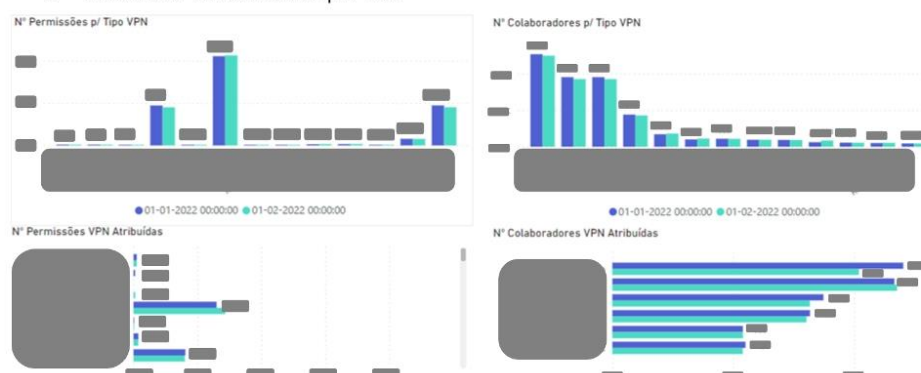
A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



Atribuições VPN – Geral

- Número de permissões por tipo de VPN
- Número de permissões por área
- Número de colaboradores por tipo de VPN
- Número de colaboradores por área



Atribuições VPN – Detalhe

- Número de permissões por tipo de VPN
- Número de aplicações por tipo de VPN por data
- Número de utilizadores por localização por data
- Número de agregadores adicionais por data
- Número de perfis funcionais por data
- Número de atribuições por tipo de identidade por data

DOCUMENTO USO INTERNO

26/38

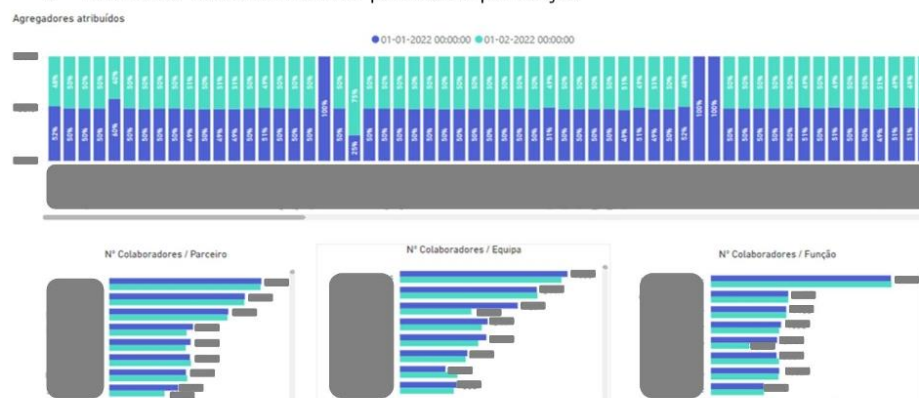
A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



Catálogo VPN – Need to Know

- Percentagem de agregadores atribuídos no mês anterior, por área
- Percentagem de agregadores atribuídos neste mês, por área
- Número de colaboradores com permissões por parceiro
- Número de colaboradores com permissões por equipa
- Número de colaboradores com permissões por função



Filtros

- Data
- Tipo de VPN
- Direção
- Área
- Username
- Aplicação
- Agregador

DOCUMENTO USO INTERNO

27/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

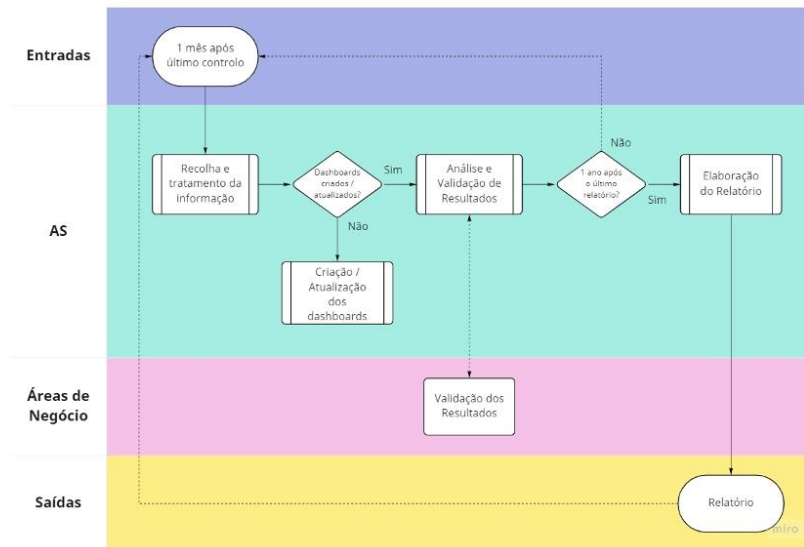
Monitorização Contínua de Acessos Críticos: Modelo AS IS



- Permissão

DATA	Tipo VPN	Direção	Área	Username	Aplicação	Agregador	Permissão
Tudo	Tudo	Tudo	Tudo	Search	Search	Search	Search

3.1.6. Fluxograma



DOCUMENTO USO INTERNO

28/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.2. Recolha e tratamento da informação

3.2.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nformado.

Atividades↓	Funções→	AS
1. Extração da Informação		A/R
2. Tratamento da Informação		A/R
3. Importação para Power BI		A/R

3.2.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Extração da informação	AS extrai a informação com recurso a SQL Developer e DBBeaver, e guarda os ficheiros. (Ver ANEXO A: Query ██████ e ANEXO B: Query ██████ (IAM)) São também recebidos dois documentos CSV enviados pela equipa ██████ (respeitantes aos registos de utilização)	1 mês após o último controlo	Ficheiros de dados	AS
2.	Tratamento da informação	Normalização das várias bases de dados de forma a que possam ser incorporados em Power BI	Ficheiros de dados	Base de dados normalizada	AS
3.	Importação para Power BI	AS importa as bases de dados em Power BI e efetua os ajustes necessários aos dashboards	Base de dados normalizada	Dashboards	AS

DOCUMENTO USO INTERNO

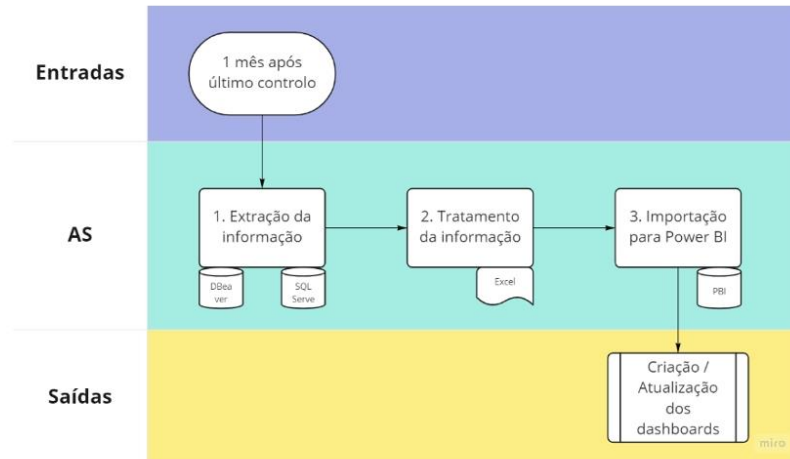
29/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.2.3. Fluxograma



DOCUMENTO USO INTERNO

30/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.3. Criação / Atualização dos Dashboards

Este subprocesso ocorre em dois momentos: no momento da primeira implementação da circularização de acessos, em que ainda não existiam dashboards e é, por isso, necessário criá-los; e sempre que CCM considere necessário atualizar/desenvolver os dashboards.

O objetivo é a criação de uma ferramenta que permita aos diretores e aos gestores de acesso das diversas áreas analisar os acessos sob a sua responsabilidade, bem como receber alertas de potenciais acessos obsoletos ou incorretamente atribuídos. É, por isso, de extrema importância a recolha, por parte de CCM, das necessidades e sugestões dos restantes stakeholders.

3.3.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nformado.

Funções→	AS	Diretores	Gestores de Acesso
Atividades↓			
1. Definição dos requisitos das áreas	A/R	C	C
2. Desenho dos dashboards	A/R		
3. Validação dos dashboards	A	R	C
4. Melhoria dos dashboards	A/R		

3.3.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Desenho dos dashboards	AS desenha os dashboards com base nos requisitos	Pasta com bases de dados normalizadas	Versão inicial dos dashboards	AS
2.	Validação dos dashboards	AS contacta algumas áreas para que estas validem os dashboards e indiquem melhorias ou correções a efetuar	Versão inicial dos dashboards	Lista de sugestões de melhoria das áreas	Áreas de Negócio
3.	Melhoria dos dashboards	AS melhora a versão inicial dos dashboards com base nas sugestões feitas pelas áreas	Versão inicial dos dashboards; Lista de sugestões de melhoria das áreas	Versão final dos dashboards	AS

DOCUMENTO USO INTERNO

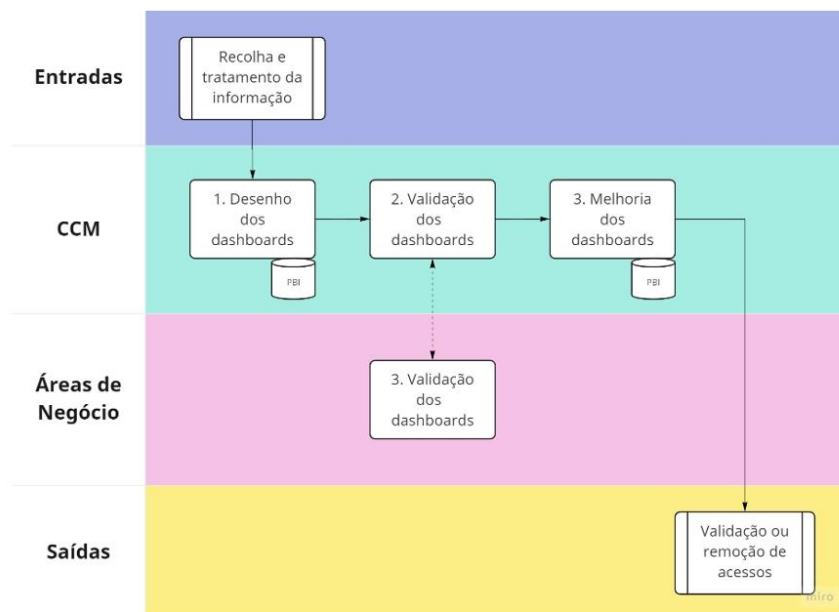
31/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.3.3. Fluxograma



DOCUMENTO USO INTERNO

32/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.4. Análise e Validação de Resultados

3.4.1. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nfornado.

Atividades↓	Funções→	AS	Áreas
1. Análise dos Dashboards de Capacidade		A/R	
2.1. Análise dos Dashboards de Atribuição / Utilização		A/R	
2.2. Identificação de situações anómalas		A/R	
3. Validação com as áreas		C	A/R

3.4.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Análise dos Dashboards de Capacidade	AS analisa as Dashboards referentes à capacidade dos VPNs	Dashboards	Análise	AS
2.1.	Análise dos Dashboards de Atribuição / Utilização	AS analisa as Dashboards referentes à utilização dos acessos atribuídos	Dashboards	Análise	AS
2.2.	Identificação de situações anómalas	AS regista as conclusões da análise efetuada num documento word, salientando as situações anómalas detetadas	Análise	Documento word com as conclusões da análise	AS
3.	Validação com as áreas	AS comunica aos diretores das áreas as situações anómalas detetadas. Nestas reuniões, os diretores decidem remover ou manter os acessos a seu cargo	Documento word com as conclusões da análise	Decisões das áreas	Áreas de negócio

DOCUMENTO USO INTERNO

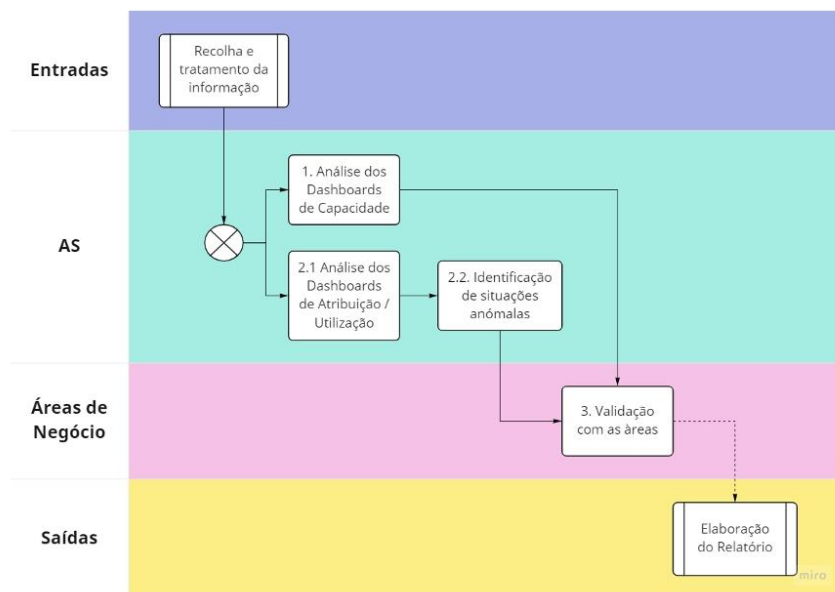
33/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.4.3. Fluxograma



DOCUMENTO USO INTERNO

34/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.5. Elaboração do Relatório

3.5.1. Tabela RACI

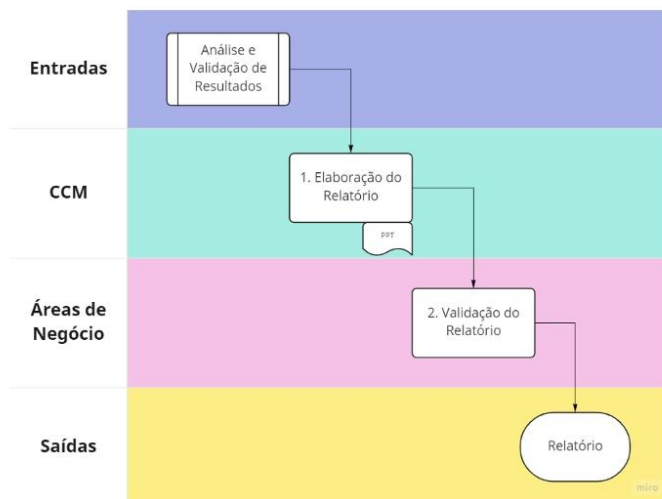
A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nformado.

Atividades↓	Funções→	CCM	AS
1. Elaboração do Relatório		A/R	I
2. Validação do Relatório		I	A/R

3.5.2. Narrativa

Nº	Atividade	Descrição	Entradas	Saídas	Responsável
1.	Elaboração do Relatório	AS elabora o relatório de circularização de acessos, salientando quantos acessos foram mantidos e quantos foram sinalizados para remoção	Dashboard atualizada	Relatório	AS
2.	Validação do Relatório	As áreas de negócio validam o relatório e informam AS	Relatório	Relatório validado	Diretores das áreas

3.5.3. Fluxograma



DOCUMENTO USO INTERNO

35/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



3.6. Conclusões e Ineficiências

No contexto atual de alívio das medidas de contenção da pandemia, com os colaboradores a regressar parcialmente aos escritórios e após o grande investimento da empresa nos servidores, a falta de capacidade destes deixou de ser um risco à continuidade do negócio. Deste modo, tornou-se irrelevante monitorizar a utilização dos acessos remotos face à sua capacidade.

Por outro lado, em reunião com o responsável pela área de Auditoria e Sistemas, este referiu que as principais ineficiências do processo se prendiam com a fraca automatização do mesmo, algo que poderia ser desenvolvido. Referiu ainda algumas ineficiências do sistema de gestão de acessos, entre as quais:

- O modelo IAM ser complexo e confuso, havendo, por isso, equipas com pouco conhecido do modelo, ainda que as áreas demonstrem boa adesão ao processo;
- A remoção de agregadores adicionais quando ocorre a alteração de funções por parte de um utilizador é manual. No entanto, a partir de Abril passará a ser automática;
- A gestão de acessos da VPN Corporativa não estar integrada em IAM, no que diz respeito à criação e modificação de agregadores adicionais;
- Não existir a possibilidade de automatizar a remoção de acessos não utilizados há mais de 90 dias caso as áreas demonstrem o queiram fazer;
- Ser frequente a duplicação de canais de acessos remotos, em especial no canais [REDACTED] e [REDACTED], onde uma grande parte dos utilizadores tem ambos os acessos;
- A atribuição de acessos remotos ser feita pelas áreas e não por IT, mais capaz de evitar a desnecessária duplicação de acessos que atualmente é comum.

4. Conclusões Gerais

Os vários processos de Monitorização Contínua de Acessos ocorrem de forma independente, implicando contactos regulares com as várias áreas da empresa. Estes contactos podem ser vistos como pouco produtivos para as áreas, no sentido em que exigem diversas respostas (algumas desnecessárias), consumindo um recurso escasso: tempo. Deveria, por isso, ser considerado o agrupamento destes processos num único, de resposta única por parte das áreas, o mais intuitivo e automatizado possível.

Monitorização Contínua de Acessos Críticos: Modelo AS IS



5. ANEXO A: Query

```
SELECT *, CURRENT_TIMESTAMP from
```

6. ANEXO B: Query (IAM)

```
SELECT
IAM_USER_NAME,
STATUS_DSC,
IDENTITY_TYPE_DSC,
CREATION_DAT,
,
AGGREGATOR_NAME,
PERMISSION_NAME,
AGGREGATOR_TYPE_ID,
DIRECTION_DSC,
AREA_DSC,
TEAM_DSC,
FUNCTION_DSC,
PARTNER_DSC,
LOCATION_DSC
from
INNER JOIN ON
=
INNER JOIN ON
=
where (STATUS_DSC = 'Ativo' OR STATUS_DSC = 'Suspenso por Prova de Vida')
and AGGREGATOR_ACTIVE_FLG = '1'
and PERMISSION_ACTIVE_FLG = '1'
and (APPLICATION_DSC like '%%'
or APPLICATION_DSC like '%%'
or APPLICATION_DSC like '%%'
or APPLICATION_DSC like '%%'
or APPLICATION_DSC like '%%'
or PERMISSION_NAME like '%%'
or PERMISSION_NAME like '%%'
or PERMISSION_NAME like '%%')
```

DOCUMENTO USO INTERNO

37/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo AS IS



```

or PERMISSION_NAME like ██████████%'
or PERMISSION_NAME like ██████████%'
or PERMISSION_NAME like ██████████%'
or PERMISSION_NAME like '%██████████%'
or PERMISSION_NAME like '%██████████%'
or PERMISSION_NAME like ██████████%')
and CAL_DAT = '22.02.01'
and VALID_TO >= '22.02.01'
    
```

7. ANEXO C: Configuração ██████████

8. ANEXO D: Configuração ██████████ (IAM)



DOCUMENTO USO INTERNO

38/38

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

8 ANEXO B: Processo TO BE



Monitorização Contínua de Acessos Críticos: Modelo TO BE

19 de Abril de 2022

Aviso: A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS SGPS, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".			
Data:	19 de Abril de 2022	Proprietário:	Nome da direção/área e/ou nome do autor
Versão:	V0.3	Aprovado por:	Nome da direção/área e/ou nome do aprovador
Classificação:	USO INTERNO	Lista de distribuição:	Nomes das direções/áreas e/ou funções e/ou pessoas destinatárias; idem; idem; idem

Monitorização Contínua de Acessos Críticos: Modelo TO BE



Índice

1.	Introdução.....	3
1.1.	Circularização de Acessos.....	3
1.1.1.	Objetivos.....	3
1.1.2.	Âmbito.....	3
1.1.3.	Responsabilidades.....	4
1.2.	Monitorização de Acessos Remotos.....	4
2.	Circularização de Acessos	5
2.1.	Parâmetros do Processo.....	5
2.2.	Fluxograma.....	6
2.3.	Tabela RACI.....	6
2.4.	Fluxo de Informação.....	7
2.5.	Detalhe das Fontes de Informação.....	8
2.6.	Dados a Importar em Power BI.....	9
2.7.	Indicadores a Analisar	9

Monitorização Contínua de Acessos Críticos: Modelo TO BE



1. Introdução

O presente relatório foi escrito no âmbito de um projeto da área de Compliance Corporativa e Monitorização (CCM), através do qual se pretende criar um processo único de Monitorização Contínua de Acessos Críticos que dê resposta a todas as necessidades das diferentes áreas.

A Circularização de Acessos Contínua será efetuada pelo seguinte conjunto de controlos:

- Circularização de Acessos – Controlo responsável pela identificação e remoção de acessos remotos e acessos definidos como críticos pela área de Privacidade & Segurança, que não são necessários à execução das funções exercidas por cada um dos utilizadores. É ainda responsável pela validação dos acessos críticos a manter, havendo um registo da justificação utilizada (Finalidade) para a manutenção destes acessos. Por fim, este controlo deteta problemas de conformidade, isto é, acessos atribuídos por perfil funcional que deveriam ser atribuídos por agregador adicional dada a sua criticidade, procurando corrigir estes problemas.
- Monitorização de Acesso a Dados – Controlo responsável por monitorizar os acessos a dados críticos, identificando e combatendo possíveis acessos fraudulentos e mal intencionados, que possam pôr em causa, entre outros, a continuidade do negócio.

Estes controlos têm objetos de estudo, destinatários e bases de dados semelhantes, pelo que estarão agregados numa ferramenta única, de forma a explorar sinergias e melhorar o desempenho deste processo.

1.1. Circularização de Acessos

1.1.1. Objetivos

De forma a garantir a privacidade dos clientes, a Circularização de Acessos tem como objetivos:

- Cumprir com o princípio *Need to Know*: apenas terão acesso aos dados pessoais os colaboradores cujas respetivas funções assim o exijam.
- Identificar os utilizadores que têm acesso a um conjunto de permissões identificadas como críticas e promover, junto dos Gestores de Acesso das respetivas áreas, a análise e correção das situações que necessitem de ajuste.
- Acompanhar e monitorizar o processo de correção.
- Eliminar acessos remotos não necessários. A deteção de erros na atribuição de acessos (acessos atribuídos por perfil funcional quando deveriam ser atribuídos por agregador adicional e viceversa).
- A deteção de agregadores adicionais que devem ser criados de forma a permitir uma melhor gestão da atribuição de acessos.

1.1.2. Âmbito

A Circularização de Acessos tem como âmbito as seguintes informações sensíveis, obtidas através das respetivas aplicações:

DOCUMENTO USO INTERNO

3/10

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo TO BE



- Tráfego detalhado não mascarado ([REDACTED])
- Apagamento a pedido de cliente ([REDACTED])
- Audição e download de chamadas gravadas ([REDACTED])
- Acessos remotos (VPN Corporativa, VPN Tecnológica, VDI Checkpoint)

1.1.3. Responsabilidades

Compliance Corporativa e Monitorização (CCM):

- Criar e garantir a manutenção dos dashboards
- Obter e tratar os dados
- Importar os dados em Power BI
- Preparar os dashboards
- Assegurar o fluxo de informação com os diretores
- Atualizar os dashboards com as respostas dos diretores
- Analisar e validar os resultados

Owners da Informação: Fornecer acesso à informação das aplicações nas quais CCM não tem autonomia de acesso.

Diretores das Áreas: Decidir manter ou revogar os acessos.

Gestores de Acesso: Análise dos dashboards e correção dos acessos em IAM.

1.2. Monitorização de Acessos Remotos

A Monitorização de Acesso a Dados consiste em identificar a utilização de acessos fora do âmbito para que estes foram atribuídos, prevenindo e corrigindo situações de acesso indevido a dados sensíveis de clientes, mitigando o risco de divulgação destas informações.

Enquanto os controlos anteriores são efetuados por CCM, este controlo é efetuado por AS, pelo que não será detalhado neste documento. É, no entanto, importante referir este controlo, pois será incorporado num repositório/dashboard único que enderece todas as monitorizações de acessos efetuadas pela Direção Auditoria, Risco e Compliance.

Monitorização Contínua de Acessos Críticos: Modelo TO BE



2. Circularização de Acessos

2.1. Parâmetros do Processo

Periodicidade: Mensal

Entradas:

- Resumo de canais VPN
- Histórico de Alertas
- Lista de utilizadores MFCC
- Lista de Identidades em IAM
 - IAM -> [REDACTED] -> SQL Developer -> Excel -> Power BI
- Lista de Permissões elegíveis pela CA (Acessos Críticos e Acessos Remotos)
- Lista de acessos atribuídos por aplicação (Acessos Críticos e Acessos Remotos)
 - IAM -> [REDACTED] -> SQL Developer -> Excel -> Power BI
- Lista de acessos atribuídos na [REDACTED] (VPN)
 - [REDACTED] -> [REDACTED] -> DBeaver -> Excel -> Power BI
- Registos de utilização de acessos para [REDACTED]
 - Aplicações -> [REDACTED] -> Excel -> Power BI
- Registos de utilização de acessos remotos
 - [REDACTED] -> Email -> Excel -> Power BI

Saídas:

- Acessos IAM atualizados
- Conformidade na Gestão de Acessos garantida
- Relatório de Circularização de Acessos

Ferramentas e sistemas de suporte:

- IAM
- Excel
- Power BI
- SQL Server
- DBeaver
- [REDACTED]

DOCUMENTO USO INTERNO

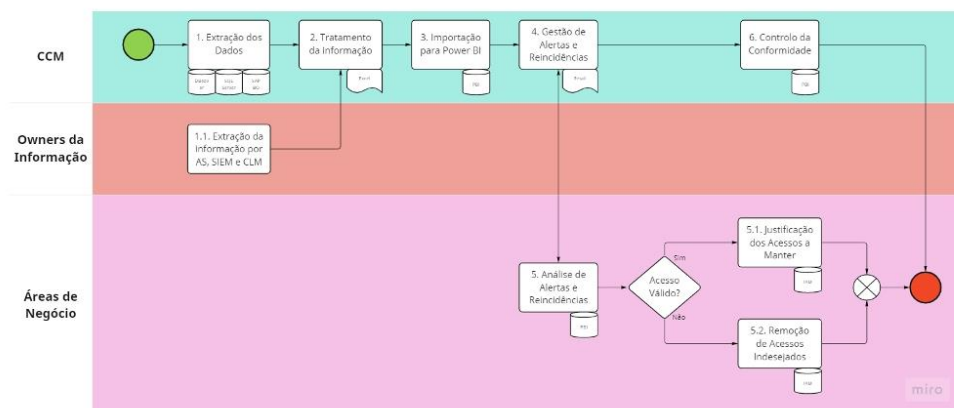
5/10

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo TO BE



2.2. Fluxograma



2.3. Tabela RACI

A tabela **RACI** identifica quem é **R**esponsável, detém **A**utoridade, quem é **C**onsultado e/ou **I**nfornado.

Funções→	CCM	Áreas de Negócio	Owners da Informação
Atividades↓			
1. Extração da informação	A/R		
1.1. Extração da informação por AS, SIEM e CLM	I		A/R
2. Tratamento da informação	A/R		
3. Importação para Power BI	A/R		
4. Gestão de Alertas e Reincidências	A/R	I	
5. Análise de Alertas e Reincidências	C	A/R	
5.1. Justificação dos Acessos a Manter	C	A/R	
5.2. Remoção de Acessos Indesejados	C	A/R	
6. Controlo da Conformidade	A/R	C	

DOCUMENTO USO INTERNO

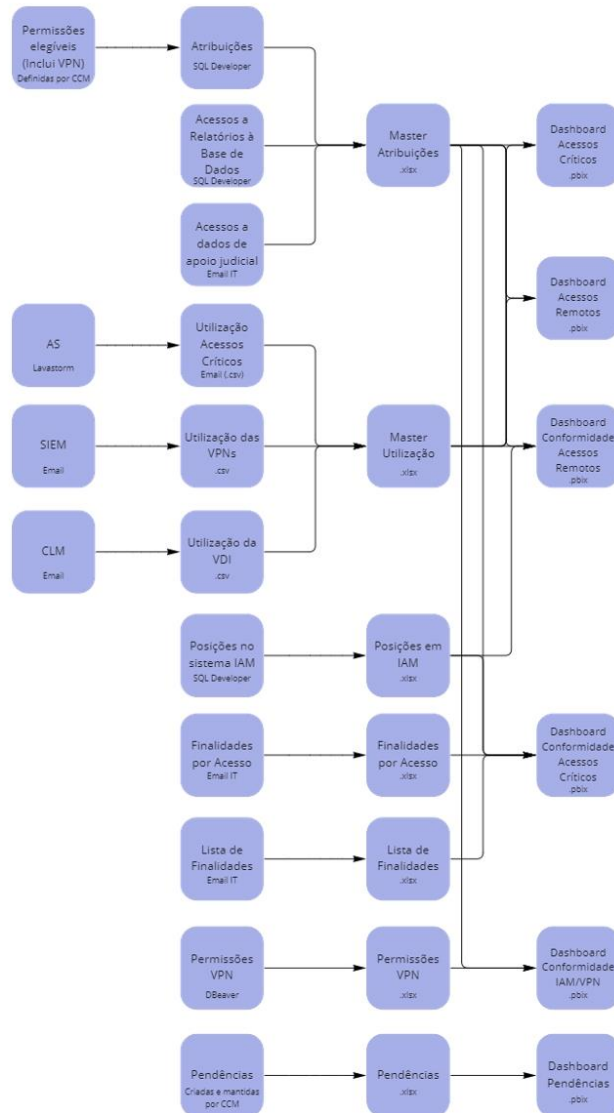
6/10

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo TO BE



2.4. Fluxo de Informação



DOCUMENTO USO INTERNO

7/10

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo TO BE



2.5. Detalhe das Fontes de Informação

O quê?	Quem?	Como?	Onde?	Período de Referência	Formato	Guardar em:
Resumo de Canais VPN	IT/Redes	Atualizado com base nos anteriores	Email	Último dia do mês anterior	.xlsx	Fontes\RefData
Histórico de Alertas	CCM	Recuperando alertas anteriores	Pastas Share	Meses anteriores	.xlsx	Fontes\Alertas
Lista MFCC (Utilizadores VDI)	DSI	Pedido à DSI	DSI	Último dia do mês anterior	.xlsx	Fontes\Users
Lista de Identidades em IAM	CCM	Query à base de dados	SQL Developer	Último dia do mês anterior	.csv	Fontes\Users
Permissões elegíveis (Inclui VPN)	CCM	Por definição dos requisitos	Excel	Último dia do mês anterior	.xlsx	Fontes\RefData
Permissões por Identidade	CCM	Query à base de dados	SQL Developer	Último dia do mês anterior	.csv	Fontes\Atribuições
Permissões VPN	AS	AS efetua query com o DBEaver	Pastas Share	Último dia do mês anterior	.csv	Fontes\Atribuições
Utilização Aplicações Críticas	AS	AS efetua query com o	Pastas Share	Mês anterior	.csv	Fontes\Utilização
Utilização das VPNs	SIEM	Equipa envia email mensal	Email	Diário	.msg	Fontes\Utilização
Utilização VDI	CLM	Equipa envia email mensal	Email	Diário	.msg	Fontes\Utilização

DOCUMENTO USO INTERNO

8/10

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo TO BE



2.6. Dados a Importar em Power BI

1. Resumo de Canais VPN (Ref Data)	2. Lista MFCC	3. Histórico de Alertas	4. Lista de Identidades em IAM	5. Master Atribuições	6. Master Utilizações
VPN Type	Username	ID	User_NT	User_NT	Data
Validado?		Direção	Estado	Aplicação	User_NT
Descrição		Estado	Tipo	Tipo de Agregador	Utilizações
		Tipo de Alerta	Empresa	Agregador	Permissão
		Aplicação	Localização	Permissão	
		Categoria da Permissão	Posição Principal?	Funcionalidade	
		Descrição do Problema	Número da Posição	Finalidade	
		Data de Abertura	Data de Início	Data da Query	
		Data de Resolução	Direção	Data de Criação	
		Reincidências	Área	Nível de Clearance	
		Prioridade	Equipa	Posição do User	
			Função		miro

2.7. Indicadores a Analisar

A	B	C	D	E
Indicador	Nome	Descrição	Formula	Operador
1	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
2	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
3	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
4	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
5	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
6	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
7	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
8	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
9	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
10	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
11	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
12	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
13	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
14	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
15	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
16	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
17	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
18	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
19	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
20	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
21	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
22	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
23	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
24	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
25	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
26	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
27	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
28	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
29	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
30	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
31	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
32	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
33	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
34	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
35	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
36	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
37	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
38	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
39	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
40	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
41	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
42	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
43	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
44	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
45	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
46	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
47	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
48	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
49	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso
50	Alertas_Acesso	Se Alertas_Acesso < 0, então com uma pontuação de 0, negativo, se > 0, positivo	Alertas_Acesso	Alertas_Acesso

DOCUMENTO USO INTERNO

9/10

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida no termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Monitorização Contínua de Acessos Críticos: Modelo TO BE

[illegible]

9 ANEXO C: Manual de Execução



Circularização Acessos Contínua | Manual Execução Dashboard

28 junho 2022

Aviso: A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS SGPS, S.A. , é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".			
Data:	dd mmmmm aaaa	Proprietário:	Auditoria, Risco e Compliance
Versão:	V0.1	Aprovado por:	Nome da direção/área e/ou nome do aprovador
Classificação:	USO INTERNO	Lista de distribuição:	Nomes das direções/áreas e/ou funções e/ou pessoas destinatárias; idem; idem; idem

Circularização Acessos Contínua | Manual
Execução Dashboard



Índice

1. Objetivo e metodologia do documento 4

1.1. Objetivo 4

1.2. Metodologia 4

2. Atividades 5

2.1. Configurar Ferramentas 5

2.2. Obter Dados 6

2.3. Tratar Dados 7

2.4. Validar dados 9

2.5. Resumo Esquema 10

Circularização Acessos Contínua | Manual Execução Dashboard



1. Objetivo e metodologia do documento

1.1. Objetivo

Descrever as atividades que são necessárias executar mensalmente para alimentar o dashboard Circularização Acessos Contínua, em PBI. Contempla ações manuais e ações automatizadas.

1.2. Metodologia

As atividades são apresentadas em 3 layers distintos, alinhados com a sequência em que são realizados:

1. Configurações necessárias nas ferramentas que vão ser usadas para automatizar atividades (Power Automate, Outlook, One Drive, VBA). [execução pontual]
2. Atividades necessárias para Obter Dados das respetivas fontes (diretamente ou através de pedidos a outras áreas) [execução mensal]
3. Atividades necessárias para Tratar Dados obtidos das fontes, por forma a assegurar um formato que possa ser importado para PBI. [execução mensal]
4. Atividades de validação de dados após execução da importação de dados e respetiva análise [execução mensal]

DOCUMENTO USO INTERNO

4/11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Circularização Acessos Contínua | Manual Execução Dashboard



2. Atividades

Atividades necessárias para proceder à obtenção de dados junto de cada uma das fontes, e posterior tratamento necessário para permitir o consumo pelo Dashboard desenvolvido no Power BI.

As atividades são segregadas em 3 blocos: i) Configurar de ferramentas (necessárias para executar as atividades dos blocos seguintes), ii) Obter Dados e iii) Tratar Dados.

2.1. Configurar Ferramentas

Power Automate (acesso através do Portal Office)

Necessário criar um fluxo para ir buscar dados ao outlook e entregar no OneDrive

1. Criar conectividades, uma por cada ponto do flow. Neste caso, será necessário criar um ponto de conectividade no Outlook (onde está a informação) e outro no One Drive (destino da informação).
2. Criar flows, um por cada processo de importação.
 - a. É permitido criar de raiz, ou importar flows já existentes.
 - b. Requer a criação de pastas específicas no Outlook e no One Drive, e respetiva configuração no flow
 - c. Especificar as ações pretendidas (entrega do email na pasta especificada, recolha do ficheiro anexo, cópia desse ficheiro para a pasta a indicar).
3. Ativar a execução do Flow, opção Turn On. O flow corre de forma contínua, sempre que surge um email na pasta identificada.

Outlook

Criar as pastas (de origem) referidas na criação dos flows em Power Automate

Criar regras que enviem os emails recebidos para as pastas adequadas

One Drive

Criar as pastas (de destino) referidas na criação dos flows em Power Automate. Deverá existir uma pasta por cada pasta de origem

1. Pastas: 01. Logs Utilização VDI e 02. Logs Utilização VPN
 - a. Dentro de cada uma destas pastas, criar uma "Pasta Temporaria_Não Elegíveis para Circularização". Esta pasta é auxiliar e deverá conter todos os ficheiros que não devem ser trabalhados na circularização corrente, nomeadamente aqueles que possuem dados fora dos limites do período alvo de análise (mês em estudo e mês anterior).
2. Pasta "03. Utilizações AppCríticas"
 - a. Criar duas pastas, uma para "Mês Anterior" e outra para "Mês Atual". Estas pastas deverão conter os ficheiros respetivos ao mês em causa.

VBA

São usados dois ficheiros com código VBA para realizar duas ações:

DOCUMENTO USO INTERNO

5/11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Circularização Acessos Contínua | Manual Execução Dashboard



1. Ficheiro “Agregar Ficheiros.xlsm”: tem por objetivo agregar conteúdo dos ficheiros de dados (de utilização) num único ficheiro, por forma a migrar esse conteúdo para o ficheiro “2. Master Utilizações.xlsx”.
 - a. A macro “Importar” pressupõe as seguintes configurações:
 - i. Localização dos dados Utilização da VDI
 - ii. Localização dos dados Utilização da VPN
 - iii. Regra de classificação da aplicação [REDACTED]
 - iv. Nome da folha onde estão os dados a importar
 - v. Localização dos dados Utilização de [REDACTED] (mês atual e mês anterior)
 - vi. Localização dos dados Utilização de [REDACTED] (mês atual e mês anterior)
 - vii. Localização dos dados Utilização de [REDACTED] (mês atual e mês anterior)
 - b. Se houver a necessidade de incorporar novas fontes de informação, é necessário atualizar o código para que sejam contempladas no processo de importação.
2. Transformar um ficheiro de formato .csv num ficheiro de formato .xlsx
 - a. Não requer configurações. A identificação da localização é parametrizada in live.

2.2. Obter Dados

Atividades	Aplicação	Tarefas
Obter Dados de Atribuições	Aplicações Críticas e Remotas	- Executar a query “<u>Atribuições.sql</u>” definindo a data à qual devem respeitar os dados. - Exportar para xlsx Nota: periodicamente deverá avaliar-se, junto do IT/IAM, se o universo de aplicações/permisões elegíveis para acessos remotos se mantém completo. Havendo necessidade de adicionar/corrigir aplicações/permisões deverá ser efetuado nesta query.
	[REDACTED]	Executar o relatório [REDACTED] (disponível no [REDACTED]).
	[REDACTED]	Efetuar (mensalmente) pedido de dados ao [REDACTED], via [REDACTED], tipificação [REDACTED]
	[REDACTED]	Efetuar (mensalmente) pedido à equipa do IAM de que nos indique a finalidade e SUB finalidade associada aos agregadores ou perfil de uma identidade, por cada uma das posições que esta possui.
	[REDACTED]	Executar o relatório [REDACTED]
Obter dados de utilização	[REDACTED]	Tarefa automatizada. Relatórios diários recebidos na mailbox [REDACTED] (um por cada fonte).

DOCUMENTO USO INTERNO

6/11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de “Cópia não controlada”.

Circularização Acessos Contínua | Manual
Execução Dashboard

		1. Mover os ficheiros da pasta "Mês Atual" para a pasta "Mês Anterior" 2. Copiar ficheiros (#5) dos emails recebido da Auditoria Sistemas (periodicidade mensal) para a pasta "Mês Atual" 3. Alterar formato do ficheiro (csv → xlsx) fazendo uso do ficheiro "csv to xlsx.xlsm". Requer a identificação da pasta onde residem os ficheiros csv, e onde serão armazenados os ficheiros output.
Obter Ref Data "4.1. Lista Finalidades" "5. Permissões VPN"	(Finalidades)	1. Obter em [redacted] a lista de finalidades/subfinalidades em vigor à data. 2. Copiar e colar em "4.1 Lista Finalidades".
	[redacted]	1. Via DBeaver, aceder à BD [redacted], e executar a query SELECT *, CURRENT_TIMESTAMP from [redacted] 2. Exportar e tratar (text to columns). 3. Apagar conteúdo existente em "5. Permissões VPN" e colar novo conteúdo (values e s/ formatação).

2.3. Tratar Dados

Atividades	Aplicação	Tarefas
Preparar dados de atribuição (Fontes → Share) (Ver Anexo A: Tratamento de Dados)	[redacted]	1. Copiar "1.2. Acessos a relatórios da Base de Dados", sheet "Dados Extraídos" para as respetivas colunas (a azul) dos "Dados Trabalhados", como texto, sendo o username copiado após ser processado pela fórmula aplicada na última coluna <code>=IF(C5="";"";IF(OR(LEFT(C5;1)="";LEFT(C5;1)=";";MID(C5;2;10000000);C5)))</code>. A fórmula aplicada ao utilizador (colunaC) permite remover qualquer delimitador que exista antes do texto. a. A coluna Objetos Acesso separa-se em colunas pelo sinal ">" b. Agregador e Permissão vêm de Objetos Acesso, por fórmula c. Username acesso separa-se em colunas por vírgula ",", e ponto e vírgula ";;" 2. Na sheet "Dados Finais" carregar no botão "Tratar Dados". O código VBA processa os dados e cria uma linha única por utilizador/agregador/permissão. 3. Na sheet "Master" (prepara-se os dados para integrar no ficheiro "1. Master Atribuições.xlsx"): a. Na data, colocar manualmente o último dia do mês da circularização b. Verificar o número de linhas em "Dados Finais" e arrastar as fórmulas e valores todos até ao número de linhas correspondente ao da página anterior c. É expectável a existência de #N/A em alguns campos, para certos non workers e aplicacionais d. Não é expectável que o user esteja #N/A, 0 ou vazio e. Para a página Master executar algumas das fórmulas, é necessário ter o documento das posições em IAM ("3. Posições IAM.xlsx") aberto f. Em username, a fórmula =IF(LEFT('Dados Finais'!A2;4)="USR_";MID('Dados Finais'!A2;5;1000000);'Dados Finais'!A2) permite remover "USR_" de alguns utilizadores que aparecem com esta nomenclatura em [redacted] mas que não a têm em IAM Nota: necessário ter o cuidado de colar apenas valores (sem formatação), por forma a preservar o formato e a configuração da tabela de destino.
	[redacted]	1. Apagar os dados que possam estar presentes no ficheiro "1.1. Acesso a dados de apoio judicial.xlsx" do mês N-2. Manter N-1

DOCUMENTO USO INTERNO

7/11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Circularização Acessos Contínua | Manual Execução Dashboard



		- Efetuar cópia do conteúdo do ficheiro recebido por email (do IT) para o ficheiro "1.1. Acesso a dados de apoio judicial.xlsx", sheet 1. - Atualizar o ficheiro "1.1. Acesso a dados de apoio judicial.xlsx", sheet Master - Para a página Master executar algumas das fórmulas, é necessário ter o documento das posições em IAM ("3. Posições IAM.xlsx") aberto - Na data, colocar manualmente o último dia do mês da circularização - Assumir o pressuposto que Nome Agregador/Permissão/ Cod. Permissão é "Search"
Construir "1. Master Atribuições.xlsx"		- Abrir "1. Master Atribuições.xlsx". Apagar dados - Copiar manualmente dados de ficheiro xls extraído da base de dados, importado, para o ficheiro "2. Master Atribuições.xlsx" (link)
		- Abrir "1. Master Atribuições.xlsx". Apagar dados do mês N-2. Manter N-1 - Copiar manualmente dados de ficheiro "1.2. Acessos a relatórios da Base de Dados", sheet Master, para o ficheiro "2. Master Utilizações.xlsx" (link)
		- Abrir "1. Master Atribuições.xlsx". Apagar dados do mês N-2. Manter N-1 - Copiar manualmente dados de ficheiro "1.1. Acesso a dados de apoio judicial.xlsx", sheet Master, para o ficheiro "2. Master Utilizações.xlsx" (link)
Transferir dados de utilização (Fontes → One Drive)		Processo automatizado com recurso ao Power Automate. O flow corre de forma contínua, sempre que surge um email na pasta origem configurada
		- Mover os ficheiros da pasta "Mês Atual" para a pasta "Mês Anterior" - Copiar ficheiros (#5) dos emails recebido da Auditoria Sistemas (periodicidade mensal) para a pasta "Mês Atual" - Alterar formato do ficheiro (csv → xls) fazendo uso do ficheiro "csv to xls.xlsm". Requer a identificação da pasta onde residem os ficheiros csv, e onde serão armazenados os ficheiros output.
		...
Construir Ficheiro "2. Master Utilizações.xlsx"		- Movimentar ficheiros nas pastas 01. Logs Utilização VDI e 02. Logs Utilização VPN - Mover da "Pasta Temporária_Não Elegíveis para Circularização" para a pasta "02. Logs Utilização VPN" todos os ficheiros que no mês anterior aí foram colocados. - Mover da pasta "02. Logs Utilização VPN" para a "Pasta Temporária_Não Elegíveis para Circularização" todos os ficheiros que não devem ser trabalhados na circularização corrente, por possuírem dados mais recentes que o período em análise (mês em estudo e mês anterior). - Apagar dados anteriores ao mês anterior. - Executar a Importação de Dados, fazendo uso da macro presente no Ficheiro "Agregar Ficheiros.xlsm", com o objetivo de agregar dados dos ficheiros presentes no One Drive (Acessos Remotos, Acessos Críticos). - Deverá ser apagado o conteúdo da tabela, caso esteja presente. - No final do processo de importação é requerido a introdução do último dia do mês que se pretende circularizar. - Esta ação requer libertação de recursos de máquina, pelo que deve ser executada com a maior capacidade de processamento disponível. - Copiar o resultado da importação para o ficheiro "2. Master Utilizações.xlsx" (link) - Deverá ser apagado o conteúdo da tabela, caso esteja presente, mantendo as aplicações Search (Mês N-1). - Colar dados provenientes do ficheiro de importação, tendo o cuidado e colar apenas valores (sem formatação), por forma a preservar o formato e a configuração da tabela de destino. - Assegurar que não existem linhas em branco no final da tabela. - Copiar manualmente dados de ficheiro "1.1. Acesso a dados de apoio judicial.xlsx", sheet1, para o ficheiro "2. Master Utilizações.xlsx" (link). Apenas dados de utilização mês N.

DOCUMENTO USO INTERNO

8/11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S., S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".

Circularização Acessos Contínua | Manual Execução Dashboard



		a. A data a preencher é a data do último dia do mês.
Construir "3.Posições IAM.xlsx"		1. Apagar conteúdo do ficheiro "3.Posições IAM.xlsx" 2. Copiar conteúdo do ficheiro "[REDACTED]" (values) 3. Validar o correto preenchimento do campo "Ligação DW (User+Posição)" (preenchido com recurso a fórmula).
Construir "4. Finalidades Declaradas"		4. Apagar conteúdo do ficheiro "4. Finalidades Declaradas" 5. Copiar conteúdo ficheiro recebido da equipa IAM, para o ficheiro "4. Finalidades Declaradas"
Atualizar ficheiro "7. Pendências.xlsx"		1. Ficheiro deve ser alimentado diretamente e manualmente pela ARC ao longo do mês. 2. Validar que se encontra atualizado.

Nota. O ficheiro "8. Resumo de Canais VPN.xlsx" não está a entrar no PBI. É informação complementar.

2.4. Validar dados

Atividades	Aplicação	Tarefas
Validar Dados "6. Tipos de Permissão.xlsx"	All	1. Após execução do PBI verificar se existem Permissões não classificadas numa Tipologia (novas permissões) Se existirem, é necessário aceder ao ficheiro e atualizar.

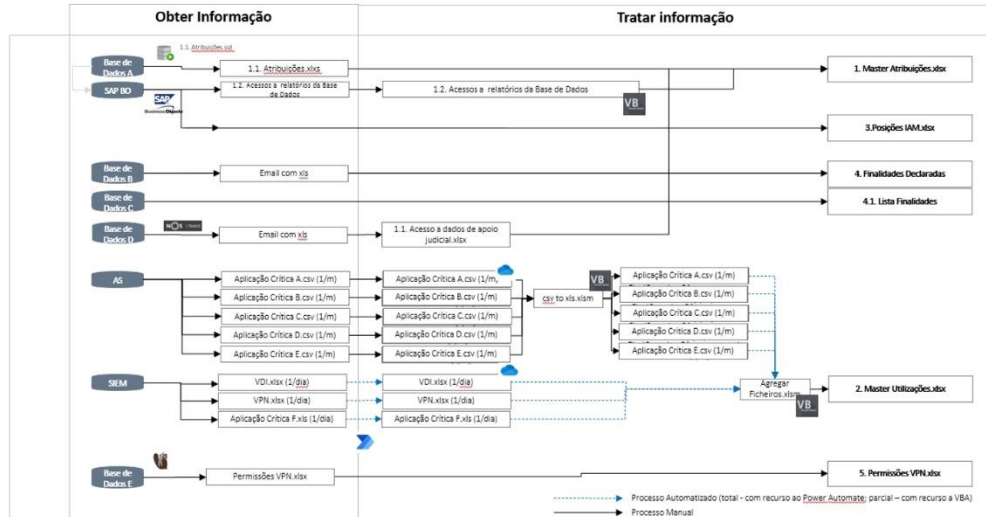
DOCUMENTO USO INTERNO

9/11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da NOS, S.G.P.S, S.A. é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da NOS. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".



2.5. Resumo Esquema



Circularização Acessos Contínua | Manual Execução Dashboard



3. Anexo A: Tratamento de Dados de acessos a relatórios da Base de Dados

	A	B	C	D	E	F	G	H	I	J	K	L
1	"Dados Extraídos" para "Dados Trabalhados"											
2	Copia-se os "Dados Extraídos" para as respetivas colunas (a azul) dos "Dados Trabalhados", como texto,											
3	sendo o username copiado após ser processado pela fórmula aplicada na última coluna											
4	A fórmula =IF(C5="";"";IF(OR(LEFT(C5,1)=""",LEFT(C5,1)=""");MID(C5,2,10000000),C5)),											
5	aplicada ao utilizador (colunaC) permite remover qualquer delimitador que exista antes do texto											
6												
7	"Dados Trabalhados"											
8	Objetos Acesso separa-se em colunas pelo sinal ">"											
9	Agregador e Permissão vêm de Objetos Acesso, por fórmula											
10	Username acesso separa-se em colunas por vírgula "," e ponto e vírgula ";"											
11												
12	"Dados Finais"											
13	Carregar no botão -> O código VBA processa os dados e cria uma linha única por utilizador											
14												
15	"Master"											
16	Na data, colocar manualmente o último dia do mês da circularização											
17	Verificar o número de linhas em "Dados Finais" e arrastar as fórmulas e valores todos											
18	até ao número de linhas correspondente ao da página anterior											
19	É expectável a existência de #N/A em alguns campos, para certos non workers e aplicacionais											
20	Não é expectável que o user esteja #N/A, 0 ou vazio											
21	Para a página Master executar algumas das fórmulas, é necessário ter o documento das posições no sistema IAM aberto											
22	Em username, a fórmula =IF(LEFT(Dados Finais!A2:4)=""USR ""MID(Dados Finais!A2:5,100000),Dados Finais!A2)											
23	permite remover "USR " de alguns utilizadores que aparecem com esta nomenclatura mas que não a têm no sistema IAM											
24												
25	"Importação para o "Master Atribuições"											
26	Copiar a tabela da folha Master e colar no final do ficheiro Master Atribuições											
27												

10 ANEXO D: Programa em VBA para agregação de dados de utilização

```

Sub Importar()
    'Localização dos dados
    Dim WbDest As Workbook
    Set WbDest = ThisWorkbook
    Dim WbSource As Workbook
    Dim strPath As String
    Dim strExtension As String
    Dim NomeFolha As String
    'Contadores de linhas
    Dim LastRow As Long
    Dim NumTotalLinhasVDI As Long
    Dim NumTotalLinhasVPN As Long
    'Data da circularização
    Dim MêsAtual As Date
    Dim MêsAnterior As Date

    'Ao longo do programa abre-se diversos ficheiros .xlsx - Esta linha evita que o ecrã esteja constantemente a mostrar os ficheiros a abrir e a fechar
    Application.ScreenUpdating = False

    'Programa
    'Importar dados da VDI
    'Reset de Contadores e Localização
    NumTotalLinhasVDI = 1
    strPath = "C:\Users\jlopes\OneDrive - NOS SGPS, S.A\Circularização de Acessos\VDI\"
    ChrDir strPath

    'Identifica os ficheiros excel na pasta Path e regista o caminho do primeiro ficheiro encontrado
    strExtension = Dir("**.xlsx")
    Do While strExtension <> ""
        Set WbSource = Workbooks.Open(strPath & strExtension)
        With WbSource
            'Definir o nome da folha a copiar, neste caso "Sheet1"
            'O seguinte código assume que o nome da folha é igual ao nome do livro
            'NomeFolha = Left(strExtension, Application.WorksheetFunction.MinLen(strExtension) - 5, 31))
            NomeFolha = "Sheet1"
            LastRow = .Sheets(NomeFolha).Cells.Find("**", SearchOrder:=xlByRow, SearchDirection:=xlPrevious).Row
            .Sheets(NomeFolha).Range("A2:A" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "D").End(xlUp).Offset(1, 0)
            .Sheets(NomeFolha).Range("B2:B" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "E").End(xlUp).Offset(1, -4)
            'Como existem users em branco, far-se a identificação da linha na coluna E e far-se offset para a A
            .Sheets(NomeFolha).Range("D2:D" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "E").End(xlUp).Offset(1, 0)
            .Close savechanges:=False
        End With
        NumTotalLinhasVDI = NumTotalLinhasVDI + LastRow - 1
    End With
    'Avança para o próximo .xlsx identificado
    strExtension = Dir
    Loop
    WbDest.Sheets("Master").Range("B2:C" & NumTotalLinhasVDI).Value = "VDI"
    'Identifica o início do contador de linhas para VPN para depois ser possível identificar o range onde se encontram os dados VPN
    NumTotalLinhasVPN = NumTotalLinhasVDI

    'Importar dados da VPN e da [Redacted]
    'Definir a localização dos ficheiros a agregar
    strPath = "C:\Users\jlopes\OneDrive - NOS SGPS, S.A\Circularização de Acessos\VPN\"
    ChrDir strPath

    'Identifica os ficheiros excel na pasta Path e regista o caminho do primeiro ficheiro encontrado
    strExtension = Dir("**.xlsx")
    Do While strExtension <> ""
        Set WbSource = Workbooks.Open(strPath & strExtension)
        With WbSource
            'Definir o nome da folha a copiar excelFolha

```

miro

Figura 42 - VBA para Agregar Dados de Utilização (1/5)

```

'Identifica os ficheiros excel na pasta Path e regista o caminho do primeiro ficheiro encontrado
strExtension = Dir("**.xlsx")
Do While strExtension <> ""
    Set WbSource = Workbooks.Open(strPath & strExtension)
    With WbSource
        'Definir o nome da folha a copiar excelFolha
        'O código atual assume que o nome da folha é igual ao nome do livro
        'NomeFolha = Left(strExtension, Application.WorksheetFunction.MinLen(strExtension) - 5, 31))
        NomeFolha = "Sheet1"
        LastRow = .Sheets(NomeFolha).Cells.Find("**", SearchOrder:=xlByRow, SearchDirection:=xlPrevious).Row
        .Sheets(NomeFolha).Range("A2:A" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "B").End(xlUp).Offset(1, -1)
        'Como existem users em branco, far-se a identificação da linha na coluna B e far-se offset para a A
        .Sheets(NomeFolha).Range("C2:C" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "B").End(xlUp).Offset(1, 0)
        .Sheets(NomeFolha).Range("D2:D" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "D").End(xlUp).Offset(1, 0)
        .Sheets(NomeFolha).Range("E2:E" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "E").End(xlUp).Offset(1, 0)
        .Close savechanges:=False
    End With
    NumTotalLinhasVPN = NumTotalLinhasVPN + LastRow - 1
End With
strExtension = Dir
Loop
WbDest.Sheets("Master").Range("C" & NumTotalLinhasVDI + 1 & "I" & NumTotalLinhasVPN).Value = "VPN"

'Quando o canal é [Redacted] ou [Redacted] a aplicação define-se com [Redacted]
LastRow = WbDest.Sheets("Master").Cells.Find("**", SearchOrder:=xlByRow, SearchDirection:=xlPrevious).Row
For i = 1 To LastRow
    If Cells(i, 2).Value = [Redacted] Or Cells(i, 2).Value = [Redacted] Then
        Cells(i, 3).Value = [Redacted]
    End If
    If Cells(i, 2).Value = [Redacted] Then
        Cells(i, 3).Value = [Redacted]
    End If
Next

'Importar dados de acessos críticos
'Recibe a data da última circularização de acessos
MêsAtual = InputBox("Intira o último dia do mês que pretende circularizar" & vbCrLf & "Utilize o formato dd/mm/aaaa", "Circularização de Acessos", Format(Now(), "dd/mm/yyyy"))
While IsDate(MêsAtual) = False
    MsgBox "Wrong date format"
    MêsAtual = InputBox("Intira o último dia do mês que pretende circularizar" & vbCrLf & "Utilize o formato dd/mm/aaaa", "Circularização de Acessos", Format(Now(), "dd/mm/yyyy"))
Wend
MêsAtual = Format(Date(MêsAtual), "dd/mm/yyyy")
MêsAnterior = DateAdd("m", -1, MêsAtual)

'Identificar o nome da onde estão os dados em cada ficheiro de acessos críticos
NomeFolha = "Sheet1"

'Identificar a localização dos ficheiros
strPath = "C:\Users\jlopes\OneDrive - NOS SGPS, S.A\Circularização de Acessos\Utilizações Críticas\"

'No código seguinte, é criada uma regra para cada tipo de ficheiro para cada mês
'Como cada tipo de ficheiro tem um formato específico, existe a necessidade deste código ser escrito individualmente
'Embora possa parecer repetitivo por ter muitas semelhanças, não me pareceu viável aplicar qualquer tipo de loop devido

'Opção [Redacted] Mês Atual
Set WbSource = Workbooks.Open(strPath & "Mês Atual [Redacted].xlsx")
With WbSource
    LastRow = .Sheets(NomeFolha).Cells.Find("**", SearchOrder:=xlByRow, SearchDirection:=xlPrevious).Row
    .Sheets(NomeFolha).Range("A2:A" & LastRow).Copy WbDest.Sheets("Master").Cells(1048576, "B").End(xlUp).Offset(1, -1)

```

miro

Figura 43 - VBA para Agregar Dados de Utilização (2/5)

miro

miro

miro

miro

miro

miro