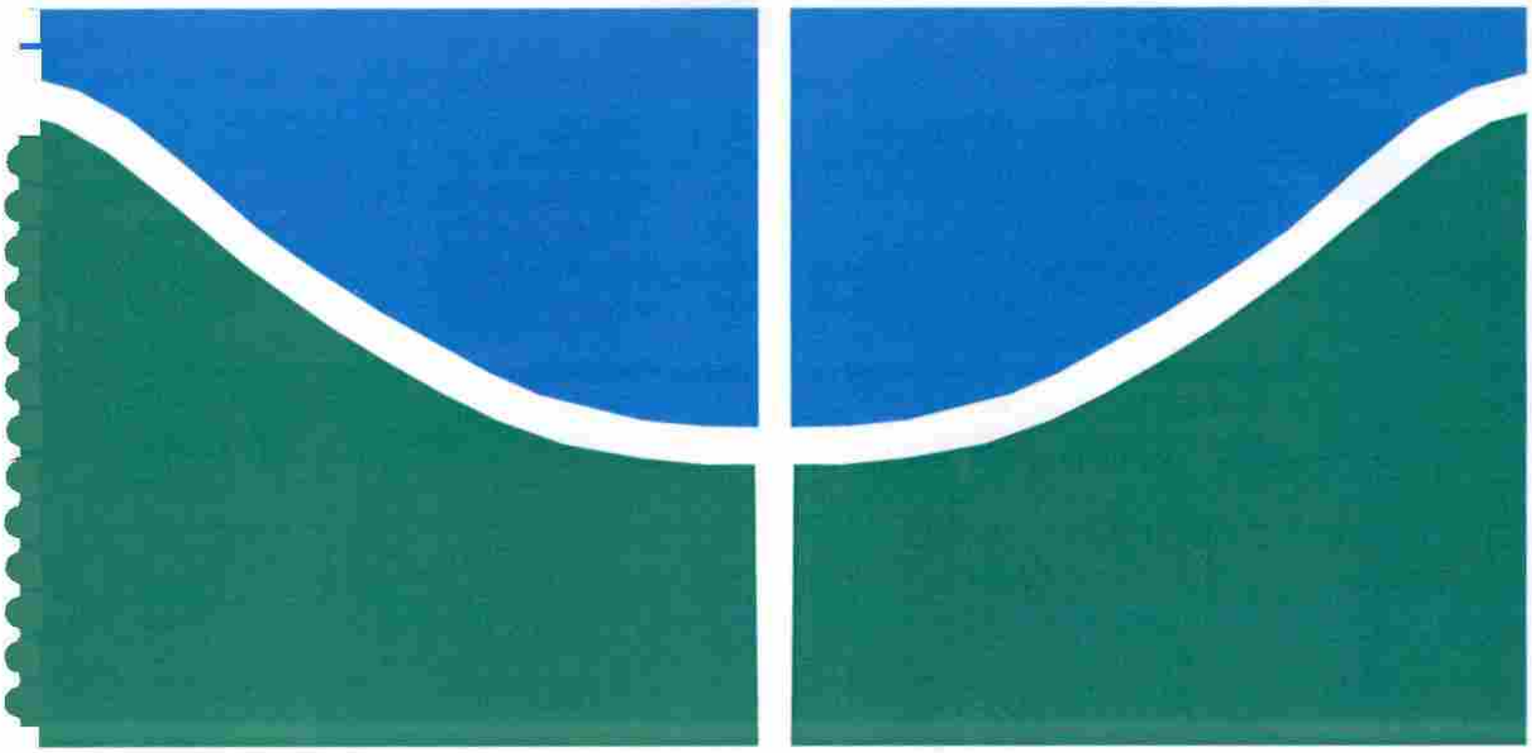

UM ESTUDO DAS CONDIÇÕES DA UTILIZAÇÃO DE NUVEM HÍBRIDA NA ADMINISTRAÇÃO PÚBLICA FEDERAL

FERNANDO ALVES DE ALMEIDA

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM ESTUDO DAS CONDIÇÕES DA UTILIZAÇÃO DE NUVEM HÍBRIDA NA ADMINISTRAÇÃO PÚBLICA FEDERAL

FERNANDO ALVES DE ALMEIDA

ORIENTADOR: CÉSAR AUGUSTO BORGES ANDRADE

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.TD – XX / 2017

BRASÍLIA, DF: SETEMBRO / 2017.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM ESTUDO DAS CONDIÇÕES DA UTILIZAÇÃO DE NUVEM HÍBRIDA NA ADMINISTRAÇÃO PÚBLICA FEDERAL

FERNANDO ALVES DE ALMEIDA

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

CÉSAR AUGUSTO BORGES ANDRADE
MESTRE, UNB/ENE (ORIENTADOR)

_____

RAFAEL TIMÓTEO DE SOUSA JÚNIOR
DOUTOR, UNB/ENE (EXAMINADOR INTERNO)

_____

ROBSON DE OLIVEIRA ALBUQUERQUE
DOUTOR, UNB/ENE (EXAMINADOR EXTERNO)

BRASÍLIA, DF, 11 DE SETEMBRO DE 2017.

FICHA CATALOGRÁFICA

Almeida, Fernando Alves de.

Um Estudo das Condições da Utilização de Nuvem Híbrida na Administração Pública Federal [Distrito Federal], 2017.

Xiii, 65p., 210 x 297mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2017).

Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Nuvem Híbrida
2. Exchange Online
3. Administração Pública Federal
4. Exchange Online Protection
5. Legislação e Orientações

I. ENE/FT/UnB

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Almeida, Fernando Alves de. (2017). Um Estudo das Condições da Utilização de Nuvem Híbrida na Administração Pública Federal. Monografia de Especialização, Publicação PPGENE.TD-XXA/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 65p.

CESSÃO DE DIREITOS

AUTOR: Fernando Alves de Almeida

TITULO DA MONOGRAFIA: Um Estudo das Condições da Utilização de Nuvem Híbrida na Administração Pública Federal.

GRAU / ANO: Especialização / 2017

Fernando Alves de Almeida
SHVP Rua 4 A Chácara 192/1 Casa 01 - Vicente Pires
CEP: 72.006-227 - Brasília - DF
Tel. 55 – 61 – 981392436 / fernando.web@gmail.com

AGRADECIMENTOS

Agradeço a Deus por ter me concedido a oportunidade de realizar este curso de especialização e a minha família, principalmente mãe e irmãos, pelo completo apoio e compreensão em toda a minha jornada. Toda força necessária me foi dada durante o período em que me dediquei a este curso e nos momentos em que as dificuldades se apresentaram.

Agradeço ao professor César Augusto Borges Andrade pela disponibilidade e compromisso de poder me orientar no desenvolvimento desse trabalho.

Agradeço também a todos os professores e profissionais que tornaram possível a realização desse curso.

RESUMO

UM ESTUDO DAS CONDIÇÕES DA UTILIZAÇÃO DE NUVEM HÍBRIDA NA ADMINISTRAÇÃO PÚBLICA FEDERAL

Autor: Fernando Alves de Almeida
Orientador: Professor MSc. César Augusto Borges Andrade
Especialização em Gestão de Segurança da Informação
Brasília, 11 de Setembro de 2017.

Dimensionar os recursos de computação na Administração Pública Federal representa um grande desafio para os gestores, diante da crescente demanda de entrega de serviço que um órgão público precisa suportar com o uso da TI. A aquisição de recursos de TI não é uma tarefa fácil quando tem que se preocupar com a redução de gastos, principalmente na aquisição de *hardware* para aumentar os recursos de seus próprios *data centers*. Nesse sentido, esse trabalho apresenta um estudo das condições da utilização de nuvem híbrida na Administração Pública Federal. A computação em nuvem se tornou uma tendência para empresas e órgãos do governo por oferecer benefícios como redução de custos, elasticidade, melhor aproveitamento dos recursos e agilidade na implantação de novos serviços com foco no negócio e no uso inteligente da equipe de TI. O presente trabalho apresenta um estudo de caso da implantação do modelo de nuvem híbrida no Ministério da Integração Nacional, que aborda também as orientações e recomendações do Governo Federal para adoção deste modelo através de decretos e normas. Para validar a proposta de nuvem híbrida no modelo de infraestrutura de *software* como serviço (*SaaS*), foi utilizado o cenário de implementação dos produtos *Office 365 Exchange Online* e *Exchange Online Protection* em que a organização ganhou a flexibilidade e escalabilidade ao poder mover carga de trabalho para Nuvem, desonerando o uso de recursos computacionais da infraestrutura de TI local.

ABSTRACT

A STUDY OF THE CONDITIONS OF THE USE OF HYBRID CLOUD IN THE FEDERAL PUBLIC ADMINISTRATION

Author: Fernando Alves de Almeida
Supervisor: Professor MSc. César Augusto Borges Andrade
Especialização em Gestão de Segurança da Informação
Brasília, 11 September 2017.

Scaling the computing resources in the Federal Public Administration represents a great challenge for managers, faced with the growing demand for service delivery that a public agency needs to support with the use of IT. The acquisition of IT resources is not an easy task when you have to worry about cost cutting, mainly in hardware acquisition to increase the resources of their own data centers. In this sense, this work presents a study of the conditions of the use of hybrid cloud in the Federal Public Administration. Cloud computing has become a tendency for companies and government agencies to offer benefits such as cost savings, elasticity, better utilization of resources and agility in deploying new services focusing on business and intelligent use of IT staff. The present work presents a case study of the implementation of the hybrid cloud model in the Ministry of National Integration, which also addresses the guidelines and recommendations of the Federal Government for adoption of this model through decrees and regulations. To validate the hybrid cloud proposal, the products Office 365 Exchange Online and Exchange Online Protection deployment scenario in which the organization has gained the flexibility and scalability by being able to move workload to the use of the computing resources of the local IT infrastructure.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

Lista de ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnicas
ADFS	*Active Directory Federation Services*
APF	Administração Pública Federal
DSIC	Departamento de Segurança da Informação e Comunicação
EOP	*Exchange Online Protection*
FISMA	*Federal Information Security Modernization Act*
GB	*Gigabyte*
GSIPR	Gabinete de Segurança Institucional da Presidência da República
HIPAA	*Health Insurance Portability and Accountability*
IaaS	*Infrastructure as a Service*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
MX	*Mail Exchanger*
NC	Norma Complementar
NIST	*National Institute of Standards and Technology*
PaaS	*Platform as a Service*
PBX	*Private Branch Exchange*
SaaS	*Software as a Service*
SIC	Segurança da Informação e Comunicação
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SMTP	*Simple Mail Transfer Protocol*
SSO	*Single Sign-On*
TI	Tecnologia da Informação
TIA	*Telecommunications Industry Association*
TIC	Tecnologia da Informação e Comunicação

1 – INTRODUÇÃO

A Computação em nuvem representa uma alternativa para a redução do custo da infraestrutura de TI nas organizações, por ser uma maneira eficiente de maximizar e flexibilizar os recursos computacionais, sendo um ambiente redundante e resiliente. Seus benefícios são poder simplificar o ambiente, diminuir encargos na administração do ambiente de TI, facilitar a alocação de recursos ou serviços, melhorando as condições de atender as demandas da organização. Um ambiente de nuvem híbrido é a combinação do ambiente público (como *Amazon*, *Google*, *Azure* e etc.) com o ambiente privado, que normalmente é configurado e desenvolvido sob demanda em um *data center*. Os ambientes públicos e privados funcionam de maneira independentes e conectam entre si quando necessários.

A ideia por trás da estratégia de TI híbrida é otimizar as suas cargas de trabalho com base nos componentes e requisitos específicos delas. Em comparação aos proveitos da computação em nuvem, o uso de salas-cofre e salas seguras torna-se dispendioso, com perda de escala e eficiência, além de apresentar maior complexidade na operação e manutenção de equipamentos (DSIC, 2012). No entanto, não há regulamentação específica para o uso da computação em nuvem na Administração Pública Federal, sendo a legislação que trata desse assunto ainda baseada em normas e decretos, embora haja uma forte recomendação e orientações quanto a sua adoção.

1.1 – OBJETIVO

O modelo de nuvem híbrida é uma opção de computação em nuvem que atende aos órgãos públicos da Administração Pública Federal, podendo os serviços de Nuvem mais usuais ser contratado como *SaaS* (*Software* como Serviço), *PaaS* (Plataforma como Serviço) e *IaaS* (Infraestrutura como Serviço), ou seja, contratação de serviço.

O objetivo desse trabalho é descrever como a implementação de nuvem híbrida no Ministério da Integração Nacional proveu escalabilidade e flexibilidade em transferir cargas de trabalho para Nuvem com o modelo baseado na arquitetura de *software* como serviço *(SaaS)* para atender a demanda de correio eletrônico e serviço de *AntiSpam*.

1.2 – JUSTIFICATIVA

O serviço de correio eletrônico estava desatualizado e sem recursos computacionais para crescimento, apresentando dificuldades em atender as demandas da organização. Passou por um longo período sem um projeto de atualização ou melhoria devido a possibilidade de migração para o serviço de correio eletrônico Expresso do Serpro, em decorrência do Decreto 8.135/2013.

Não tendo mais essa preocupação, os projetos de atualização e melhorias voltaram a ser considerados pelos gestores, onde se definiu a implementação do modelo de nuvem híbrida baseado na arquitetura de *software* como serviço *(SaaS)* oferecida pela *Microsoft*, fornecedora com o qual o Ministério da Integração Nacional possuía contrato.

1.3 – METODOLOGIA UTILIZADA

Nesta monografia será apresentado um Estudo de Caso em que descreve sobre as condições de implementação do modelo de nuvem híbrida com arquitetura de *software* como serviço *(SaaS)* para prover maior disponibilidade, confiança e desempenho do serviço específico de correio eletrônico. Foi realizado uma revisão literária para definir os conceitos básicos necessários a um bom entendimento da monografia e pesquisa de trabalhos acadêmicos relacionados sobre os modelos de computação em nuvem e sua utilização.

1.4 – ESTRUTURA DA MONOGRAFIA

Para um melhor entendimento deste trabalho, a sua organização é descrita a seguir:

O Capítulo 2 apresenta as características sobre computação em nuvem e seus conceitos básicos, normas, legislações, recomendações e orientações do Governo Brasileiro quanto ao seu uso em órgãos públicos e trabalhos acadêmicos relacionados.

No Capítulo 3 será apresentado o Ministério da Integração Nacional, onde foi realizado o estudo de caso;

No Capítulo 4 é apresentado o estudo de caso, demonstrando a implementação dos produtos *Exchange Online e Exchange Online Protection* numa infraestrutura de *software* como serviço no Ministério da Integração Nacional;

No Capítulo 5 são realizadas as considerações finais e na seção seguinte apresenta as Referências Bibliográficas.

2 – CONCEITOS BÁSICOS E REVISÃO BIBLIOGRÁFICA

Neste capítulo serão abordados os principais conceitos da computação em nuvem para um melhor entendimento do modelo de nuvem híbrida e do estudo de caso apresentado. Será abordado os tipos de contratações mais usuais, as legislações, recomendações e orientações quanto ao seu uso em órgãos públicos. Os conceitos estão divididos em seções e apresentados em tópicos específicos. Na seção 2.1 é apresentado os conceitos de computação em nuvem. Na seção 2.2 é apresentado as normas e legislações do governo brasileiro. Na seção 2.3 é apresentado as recomendações e orientações para órgãos públicos. Na seção 2.4 é apresentado os trabalhos relacionados.

2.1 – A COMPUTAÇÃO EM NUVEM

Segundo Veras (2012), a computação em nuvem introduz a ideia de elasticidade na utilização de infraestrutura de TI, onde os recursos podem ser utilizados em períodos de alta demanda e devolvidos em períodos de baixa demanda, permitindo flexibilizar a alocação de custos para empresas mudando de um modelo baseado em custo de capital para um modelo baseado em despesas operacionais.

2.1.1 – Características da Computação em Nuvem

Conforme Taurion (2009), a computação em nuvem possui características próprias que definem o seu conjunto de tecnologias, como:

- A abstração da infraestrutura e a distribuição geográfica dos sistemas, que permitem autonomia de gestão e operação entre diversos sites;
- A heterogeneidade dos sistemas;
- Escalabilidade e adaptabilidade, sendo o fundamento básico da computação em nuvem a virtualização dos recursos computacionais.

Segundo Diógenes e Veras (2015), a computação em Nuvem exige um modelo de segurança da informação que reconcilie a capacidade de expansão de recursos computacionais com a necessidade de confiança. É necessário a confiança nos sistemas e nos provedores de nuvem quanto ao controle de acesso, segurança dos dados, gerenciamento e monitoramento contínuo de eventos e informações.

O modelo de computação em nuvem possui cinco características genéricas e essenciais que são consideradas pela maior parte da literatura sobre o assunto. Estas características essenciais estão divididas em três modelos de serviço e quatro modelos de implementação, conforme apresentado na figura 2.1:

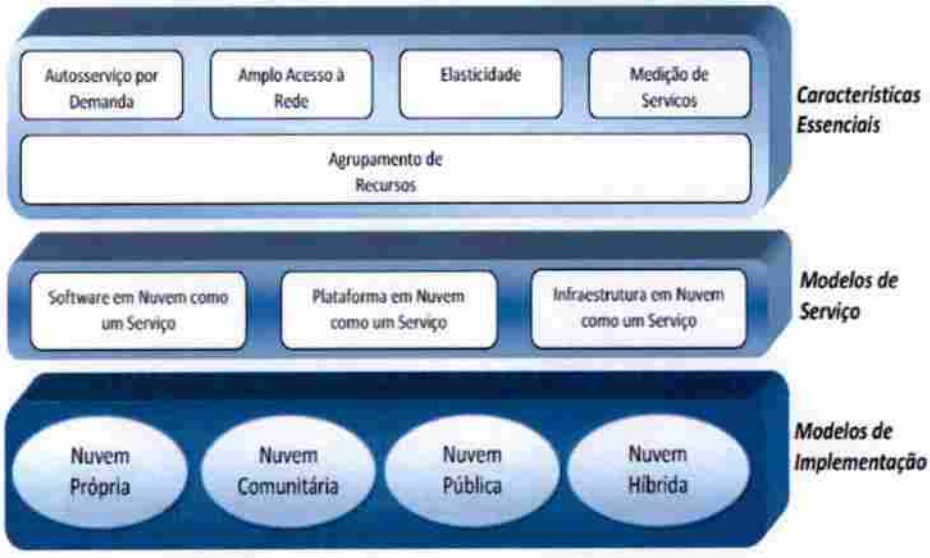

Figura 2.1 – Características do Modelo de Computação em Nuvem. (*CSA – Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, adaptado por DSIC, p.5).

Há muitas definições sugeridas para computação em nuvem na literatura sobre o assunto, a mais aceita é a definição do NIST que também trata das características essenciais da Nuvem. A computação em nuvem habilita de forma simplificada o acesso conforme a demanda a uma rede, a qual possui um *pool* de recursos computacionais configuráveis, como servidores, armazenamento, aplicações e serviços. Esses recursos podem ser rapidamente provisionados, configurados e liberados com um esforço de gerenciamento mínimo e automatizado, promovendo a melhoria da disponibilidade e do desempenho do ambiente de TI. Para certas tarefas de infraestrutura o usuário pode, ele mesmo, configurar a sua necessidade e liberar o recurso (DIÓGENES; VERAS, 2015). A Tabela 2.1 apresenta a descrição das características essenciais de uma solução de computação em nuvem.

Tabela 2-1 – Descrição das Características Essenciais da Computação em Nuvem.

Características Essenciais	Descrição
Autosserviço por demanda	Pode ser provisionado conforme a necessidade e capacidades computacionais de maneira automática.

Características Essenciais	Descrição
Amplo acesso à rede	Os recursos computacionais estão disponíveis através da rede, possibilitando o uso de plataformas heterogêneas.
Agrupamento de recursos	Os data centers dos provedores de serviço são organizados como *multi-tenant*, podendo ser dinamicamente configurados pelos clientes conforme suas demandas.
Elasticidade	Os recursos podem ser provisionados de forma rápida e automática, conforme a demanda.
Medição de Serviços	Os recursos são medidos apropriadamente para cada tipo de serviço, de modo a trazer transparência para o cliente.

A computação em nuvem possui diferentes modelos de serviços. A Tabela 2.2 apresenta a descrição dos modelos de serviços oferecidos em uma solução de computação em nuvem.

Tabela 2-2 – Descrição dos Modelos de Serviços da Computação em Nuvem.

Modelos de Serviços	Descrição
Software como um Serviço	A aplicação é oferecida como serviço, sem a necessidade de se adquirir licenças de uso ou infraestrutura para utilizá-la. O cliente gerencia apenas as configurações específicas do usuário.
Plataforma como um Serviço	O cliente tem a possibilidade de ter sua capacidade computacional atendida por uma infraestrutura customizada na nuvem.
Infraestrutura como um Serviço	O cliente pode implementar e executar arbitrariamente suas aplicações, o que inclui o sistema operacional e seus recursos.

O NIST descreve os três principais modelos de serviços para computação em nuvem:

- **Infraestrutura como um serviço (*Infrastructure as a Service – IaaS*)**: o provedor oferece uma infraestrutura de processamento e armazenamento de forma transparente e representa uma abstração da infraestrutura propriamente dita. O usuário não tem o controle da infraestrutura física, mas possui o controle sobre as máquinas virtuais, o armazenamento, os aplicativos instalados e algum controle limitado sobre os recursos de rede;
- **Plataforma como um serviço (*Platform as a Service – PaaS*)**: é uma plataforma oferecida pelo provedor para o desenvolvimento de aplicativos que serão executados e disponibilizados na nuvem;

- **Software como um serviço (*Software as a Service – SaaS*)**: é um tipo de aplicativo de interesse para uma grande quantidade de usuários que passam a ser hospedados na Nuvem como uma alternativa ao processamento local. Eles são oferecidos como serviços por provedores e acessados pelos clientes através de aplicações como o *browser*. Todo o controle e gerenciamento da rede, sistemas operacionais, servidores e armazenamento é feito pelo provedor de serviço.

2.1.2 – Características do Modelo de Nuvem Híbrida

Um aspecto importante da computação em nuvem é que ela padroniza o acesso e a comunicação entre aplicações utilizando como tecnologia de base os *browsers* e os *web services*. As formas de implementar a nuvem são também descritas pelo NIST, que embora sejam conceitos que têm se aperfeiçoado, estes ainda são os mais utilizados. A Tabela 2.3 apresenta a descrição dos modelos de implementação de uma solução de computação em nuvem.

Tabela 2-3 – Descrição dos Modelos de Implementação da Computação em Nuvem.

Modelos de Implementação	Descrição
Nuvem Própria	A infraestrutura pertence apenas a organização.
Nuvem Comunitária	A infraestrutura é compartilhada entre organizações que tem necessidades comuns.
Nuvem Pública	A infraestrutura está disponível a sociedade e para organizações, sendo administrada por um provedor de serviços.
Nuvem Híbrida	É a composição da nuvem própria com a nuvem pública.

Na nuvem híbrida a infraestrutura é uma composição de duas ou mais nuvens (privadas, públicas ou comunitárias) que continuam a ser entidades únicas, porém conectadas através de tecnologias proprietárias ou padronizadas que propiciam a portabilidade de dados e aplicações. A nuvem híbrida impõe uma coordenação adicional a ser realizada para uso das nuvens privadas e públicas com impactos na governança.

As ofertas de nuvem pública são diversas. Algumas tendências nesta área apontam que grandes provedores de soluções para computação em nuvem pública como a *Microsoft* e a

Amazon estão integrando suas ofertas de modelos de serviços *IaaS* e *PaaS* (DIÓGENES; VERAS, 2015).

No modelo *IaaS* o usuário não tem o controle da infraestrutura física, é basicamente uma infraestrutura virtual baseada na Internet, adquirida e paga na forma de serviço (VERAS, 2012).

2.2 – NORMAS E LEGISLAÇÕES DO GOVERNO BRASILEIRO

Nesta seção será apresentada as principais normas e legislações que recomendam e orientam a contratação da computação em nuvem na administração pública federal.

- O Comitê de Governança Digital, criado pelo Decreto nº 8.638 de 15 de Janeiro de 2016, institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Gera benefícios para a sociedade mediante o uso da informação e dos recursos de tecnologia da informação e comunicação na prestação de serviços públicos (BRASIL, 2016).
- SISP - Sistema de Administração dos Recursos de Tecnologia da Informação, que foi instituído pelo Decreto nº 1.048 de 21 de janeiro de 1994 e atualizado pelo Decreto nº 7.579 de 11 de outubro de 2011, com o objetivo de organizar a operação, controle, supervisão e coordenação dos recursos de tecnologia da informação da administração direta, autárquica e fundacional do Poder Executivo Federal (BRASIL, 2011).
- A Norma Complementar número 14, NC 14/IN01/DSIC/GSIPR, estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta (DSIC, 2012).
- A Lei nº 12.527, que regula o acesso a informações previsto no inciso XXXII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal (BRASIL, 2016).
- A norma ABNT NBR ISO/IEC 17788:2015 fornece uma visão geral sobre a computação em nuvem e um conjunto de termos e definições sobre o tema. É basicamente uma versão em português feita pela Associação Brasileira de Normas Técnicas (ABNT), Serpro e Anatel, de um trabalho realizado em cooperação entre a *International Telecommunication Union* (ITU), que coordena padrões internacionais

para telecomunicações e a *International Organization for Standardization* (ISO), uma organização internacional para padronização. Esta norma permitirá a compreensão dos diversos elementos que compõem a computação em nuvem, dando mais clareza ao mercado quanto a sua adoção (ABNT, 2015).

2.3 – RECOMENDAÇÕES E ORIENTAÇÕES PARA ÓRGÃOS PÚBLICOS

A computação em nuvem despontou com a grande promessa de reduzir os custos das organizações em tecnologia da informação – seja pela simplificação dos ambientes, pela diminuição dos encargos de administração das infraestruturas ou pela facilidade de alocação de recursos ou serviços. A nova tecnologia está sendo cada vez mais adotada por empresas e órgãos públicos. Em comparação aos benefícios da computação em nuvem, como redução de custos, elasticidade e agilidade na implantação de novos serviços, o uso de salas-cofre e aquisição de *hardware* torna-se mais dispendioso, com perda de escalabilidade e eficiência, além de apresentar maior complexidade de operação e manutenção de equipamentos (DSIC, 2012).

Com o objetivo de estabelecer diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta, o DSIC (2012) e o MPOG (2016) recomendam aos órgãos contratarem preferencialmente Nuvem Híbrida como modelo de implantação, de fornecedor público ou privado, beneficiando-se da elasticidade e agilidade do modelo de nuvem pública e do desempenho garantido dos recursos dedicados no modelo privado e ao mesmo tempo minimizando os riscos e otimizando os custos com cada modelo.

No momento da contratação, os órgãos deverão exigir conformidade com a norma ABNT NBR ISO/IEC 27001:2013, objetivando mitigar os riscos relativos à segurança da informação e conformidade com o disposto na Norma NC 14/IN01/DSIC/GSIPR, obedecendo princípios e diretrizes como os que seguem:

> 5.2. Ao contratar ou implementar um serviço de computação em nuvem, o órgão ou entidade da APF deve garantir que:
>
> 5.2.1. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes e normas de SIC, estabelecidas pelo GSIPR, e às legislações vigentes;

> 5.2.2. A legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem;
>
> 5.2.3 O contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;
>
> 5.3. Os órgãos ou entidades da APF devem avaliar quais informações serão hospedadas na nuvem, considerando:
>
> 5.3.4. O modelo de serviço e de implementação de computação em nuvem a serem adotados;
>
> 5.3.5. A localização geográfica onde as informações estarão fisicamente armazenadas (DSIC, 2012).

A disponibilidade deve ser de no mínimo 99,749% para os data centers onde os serviços estarão hospedados, aceita a comprovação por meio de certificação TIA 942 TIER II.

Tabela 2-4 – Classificação de *Data Centers* – Norma TIA 942 (adaptado de DSIC, 2012).

Categoria	Disponibilidade	Característica
Tier I	99,671%	Componentes internos não redundantes e uma rota de alimentação externa não redundante servindo ao ambiente crítico. Sua infraestrutura inclui um espaço dedicado para os sistemas de TI, um sistema UPS, um equipamento de refrigeração e um gerador para proteção de falhas no fornecimento de energia
Tier II	99,741%	Componentes internos redundantes e uma rota de alimentação externa não redundante servindo ao ambiente crítico. Os componentes redundantes são: geradores, sistemas UPS, sistemas de refrigeração e tanques de combustível
Tier III	99,982%	Datacenter paralelamente sustentável que possui componentes de capacidade redundantes e múltiplas rotas independentes de distribuição, sendo que apenas uma rota é necessária para servir o ambiente crítico, que pode ter qualquer componente nas rotas de distribuição interrompido sem causar impacto no ambiente crítico

Tier IV	99,99%	Datacenter tolerante a falhas composto por vários sistemas fisicamente independentes de alimentação ativas simultaneamente, servindo o ambiente crítico. Sistemas complementares e rotas de distribuição devem estar compartimentalizados para prevenir qualquer tipo de incidente impactar simultaneamente os sistemas ou rotas de distribuição.

2.4 – TRABALHOS RELACIONADOS

A computação em nuvem é um assunto de relevância no meio acadêmico. Nesta seção são apresentados alguns trabalhos relacionados com a computação em nuvem e sua implantação numa perspectiva de empresas e instituições brasileiras.

Segundo Medeiros (2015) em seu artigo sobre análise da implantação de computação em nuvem, são apresentados fatores importantes para implantar ou não a computação em nuvem, avaliando o fornecimento de infraestrutura e armazenamento de dados por terceiros, escalabilidade, disponibilidade e segurança dos dados que trafega pela rede. Partindo do princípio que esse modelo computacional surgiu a partir da necessidade de diminuir os custos de compra de equipamentos para as empresas e de ter um grande poder para armazenamento de informação de forma escalável. Com isso, o artigo objetiva analisar os possíveis impactos da adoção da computação em nuvem, identificando os fatores de riscos e benefícios e investigando as soluções disponíveis no mercado, principalmente em relação à viabilidade desse modelo computacional para micro e pequenas empresas. Em seu estudo de caso realizado na empresa Alfa Informática .NET, é relatado que a empresa obteve mais confiabilidade em seus serviços, mais escalabilidade de armazenamento e segurança em guardar informações de seus clientes e também mais acessibilidade de suas informações. A percepção da gestão da empresa sobre a adoção da computação em nuvem é que se trata de um modelo computacional inovador que está funcionando perfeitamente para empresas reconhecidas mundialmente e que trará inúmeros benefícios para a forma de operação da empresa.

Júnior e Heinzelmann (2016) argumentam que a falta de recursos em instituições públicas dificulta a implantação de novas tecnologias e manutenção dos recursos existentes, aumentando assim os gastos e a quantidade de trabalho pela equipe responsável por manter o sistema. Tiveram a ideia de realizar um experimento, a partir da implantação de uma

plataforma de computação em nuvem, com serviços orquestrados, através do uso do *CloudStack* e serviços de monitoramento, para analisar e propor uma alternativa à uma infraestrutura de computação extremamente heterogênea e pouco interligada. Existem algumas ferramentas que possibilitam a criação de uma Nuvem, as quais são conhecidas como orquestradores. Algumas delas são de *software* livre, como o *CloudStack*. O ponto principal da computação em nuvem é entregar todas as funcionalidades de serviços de TI existentes e, ao mesmo tempo, reduzir os custos que uma organização teria para implantação de seus serviços. Em seu trabalho, Júnior e Heinzelmann apresenta um experimento, detalhando a estrutura existente e uma análise entre os dados da estrutura legado com os novos dados obtidos do experimento. O *CloudStack*, utilizado para realização do experimento, é um *software* livre desenvolvido para implantar e gerenciar projetos de nuvens privadas, públicas ou híbridas, entregando uma infraestrutura como serviço (*IaaS*) confiável e escalável em uma plataforma de computação em nuvem. É um orquestrador completo de recursos e seu gerenciamento é um processo prático e integrado, seja por uma interface *web* ou através de linha de comando, podendo gerenciar uma quantidade imensa de servidores físicos que podem estar distribuídos em *data centers* ao redor do mundo, possui uma infraestrutura hierárquica, a fim de permitir a gestão de vários nós físicos por uma única interface. O experimento tem como objetivo verificar a viabilidade da utilização de uma infraestrutura de Nuvem como solução para alguns dos problemas encontrados e tornar o trabalho da equipe responsável pela manutenção mais ágil e automatizado. A plataforma de computação em nuvem desenvolvida nesse projeto mostrou ser uma boa alternativa para se obter melhor desempenho, gerenciamento de recursos de forma escalável e com maior disponibilidade, um maior nível de resiliência e confiabilidade, com uma redução nos custos, de forma indireta, para a Instituição.

Ramalho (2012) apresenta, em sua tese de mestrado, um estudo sobre a adoção da computação em nuvem no Brasil. A maneira como as empresas brasileiras estão adotando a computação em nuvem, em que caracteriza um forte apelo econômico e o seu uso como uma utilidade que podem ser consumidos e pagos com a mesma conveniência que a energia elétrica. Seu estudo mostra como a computação em nuvem são oferecidos no mercado, quais motivações das organizações na escolha de um provedor e os diferentes perfis de organizações em função dos serviços adotados. As características organizacionais e as características dos serviços de computação em nuvem, em que uma empresa não necessita mais investir antecipadamente um alto capital em equipamento de TI ao iniciar suas

atividades. Os recursos computacionais podem ser adquiridos sob demanda de um provedor de Nuvem e a empresa pagará apenas pelo que for consumido. Concluindo que há uma predominância de serviços de computação em nuvem genéricos, adotados no mercado brasileiro, seu estudo mostra uma tendência do mercado de uso da TI como uma utilidade, ou seja, o que não é específico é terceirizado sob forma de computação em nuvem.

Dias (2013), faz uma exposição da norma que regulamenta o uso dos serviços da computação em nuvem, como os Estados Unidos está trabalhando com Nuvem e como o governo brasileiro tem se posicionado em relação a essa tecnologia. Seu uso exige esforços e atenção por parte dos órgãos e entidades da Administração Pública Federal (APF) em viabilizar e assegurar a Segurança da Informação e Comunicação (SIC). Um cenário novo que gera lacunas e dúvidas a respeito de que medidas devem ser tomadas para que a computação em nuvem seja melhor aproveitada para atender, com segurança, aos objetivos estratégicos institucionais. Para isso foi criada pelo Departamento de Segurança da Informação e Comunicação (DSIC) a Norma Complementar número 14 que estabelece diretrizes para a utilização de tecnologias de computação em nuvem nos órgãos e entidades da Administração Pública Federal direta e indireta, garantindo que a legislação brasileira prevalece sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações em Nuvem, e também garantias contratuais de disponibilidade, confidencialidade e integridade das informações. Empresas de tecnologia do Governo, como o Serpro e a Dataprev, estão empenhados nos estudos e estruturação da Nuvem Privada, que proporcionará uma interoperabilidade entre o cidadão e o Governo, para ofertar *software* como serviço. Já o governo norte-americano exporta toda a tecnologia usada no mundo e tem recomendado o uso da computação em nuvem ao invés de adquirir infraestrutura própria. Essa decisão se baseia no fato de que o gasto com infraestrutura não tem efeito direto para o cidadão. Segundo o governo norte-americano, o estado atual da TI na gestão pública é ineficiente, com inúmeras redundâncias de infraestrutura, sistemas, dados e informações, com aquisições morosas, com prazos de instalação incertos e com o risco de que a compra por menor preço geralmente não garanta a melhor qualidade tecnológica. O trabalho conclui que as leis brasileiras ainda não abrangem todas as questões legais nos negócios da *Internet*, mas mesmo assim o judiciário consegue usar as leis existentes para tentar preencher essa lacuna. Mas isso é só o início, pois como muitas vezes acontece, será a prática que impulsionará a criação de novas legislações.

Ferreira e Andrade (2016), explicita de maneira simples e concisa as principais leis, normas e orientações no Brasil que envolvam a computação em nuvem, os principais documentos elaborados pelo governo brasileiro e seus parceiros nos últimos anos que envolvam de alguma forma a computação em nuvem. Em seu artigo, descreve que a computação em nuvem tem sido adotada por empresas e órgãos de governo do mundo todo. Leis, normas, decretos, portarias, orientações do governo, entre outros regulamentos foram criados no Brasil abordando temas relacionados à Tecnologia da Informação. Contudo, há dificuldades envolvendo o tema de computação em nuvem devido à quantidade de variáveis envolvidas e à sua complexidade. Legislar sobre o assunto tornou-se algo complexo, mas de fundamental importância visto que essa tecnologia está sendo cada vez mais utilizada por governos e empresas. A norma ABNT NBR ISO/IEC 17788:2015 apresenta uma visão geral sobre computação em nuvem, além de estabelecer um conjunto de termos e definições sobre o tema, que trouxe muitos benefícios. O fato da norma ter sido escrita baseada em uma norma internacional facilita a exportação dos serviços por empresas brasileiras, de como as legislações brasileiras tratam o assunto e como é o entendimento do Governo Federal com relação a computação em nuvem.

Diferentemente dos trabalhos acima citados, nesta monografia será apresentado um estudo de caso em que a implantação de nuvem híbrida foi realizada e bem-sucedida com a utilização dos produtos *Exchange Online* e *Exchange Online Protection* em um órgão da Administração Pública Federal, observada as normas, recomendações e orientações fornecidas pelo Governo.

3 – O MINISTÉRIO DA INTEGRAÇÃO NACIONAL

O Ministério da Integração Nacional é uma das mais importantes instituições do Governo Federal devido ao seu papel social. Sua origem é antiga e data do período do Império, criada por D. João V como Secretaria de Estado dos Negócios Interiores do Reino. O Ministério passou por várias modificações em sua trajetória ao absorver outras Secretarias e Superintendências, como:

- Superintendência do Desenvolvimento do Nordeste (SUDENE);
- Superintendência do Desenvolvimento da Amazônia (SUDAM);
- Superintendência do Desenvolvimento do Centro-Oeste (SUDECO);
- Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba (CODEVASF).

As autarquias SUDENE e SUDAM foram extintas para a criação das Agências de Desenvolvimento do Nordeste e da Amazônia, respectivamente. O Ministério da Integração Nacional sempre esteve vinculado há outros órgãos existentes por meio de leis e decretos, consequentes de reformas políticas e organizacionais da administração pública nos governos que sucederam da sua criação, às vezes, de forma independente. A tabela 3.1 apresenta algumas de suas denominações das mudanças ocorridas no decorrer do tempo, até ganhar sua própria identidade como instituição.

Tabela 3-1 – Denominações do Ministério da Integração Nacional.

Denominação	Ano de Criação
Secretaria de Estado dos Negócios Interiores do Reino	1736
Ministério da Justiça e Negócios Interiores	1891
Ministério do Interior	1967
Secretaria de Desenvolvimento Regional	1990
Ministério da Integração Regional	1992
Secretaria Especial de Políticas Regionais	1998
Ministério da Integração Nacional	2003

Em 2006, o Ministério da Integração Nacional teve aprovada sua estrutura regimental por decreto, tendo seu próprio regimento interno no ano seguinte. É uma instituição que teve sua estrutura readequada a cada governo. Sua atuação é na proteção e defesa civil, tendo como referência o Centro Nacional de Gerenciamento de Riscos e Desastres (CENAD), no

desenvolvimento regional, na infraestrutura hídrica e em projetos de grande projeção nacional, como o Projeto Rio São Francisco e Programa Água para Todos.

Os objetivos estratégicos do Ministério são:

- Superar desigualdades regionais e erradicar a miséria;
- Ampliar e garantir a eficiência da irrigação;
- Garantir segurança hídrica;
- Assegurar proteção civil;
- Implementar gestão eficiente, eficaz e efetiva;

Em seu planejamento estratégico, o Ministério da Integração Nacional tem como visão de futuro ser uma instituição reconhecida na articulação e indução do desenvolvimento regional equilibrado e da proteção civil, atuando em todo o território nacional. Sua missão é promover a integração nacional, o desenvolvimento sustentável e a superação das desigualdades regionais do país, assegurando inclusão socioeconômica, melhoria de qualidade de vida, proteção civil reduzindo a vulnerabilidade a desastres por meio de políticas de prevenção e ampliando e qualificando a capacidade de resposta a desastres, alertas de problemas meteorológicos, aviso de desastres e também segurança hídrica da população.

4 – ESTUDO DE CASO

Este trabalho apresenta o modelo de nuvem híbrida e sua utilização no Ministério da Integração Nacional, descrevendo um estudo de caso de uma implementação de nuvem híbrida no Ministério da Integração Nacional, em que foi implementado a utilização híbrida do produto de correio eletrônico *Microsoft Exchange* e *Exchange Online Protection*.

4.1 – DESCRIÇÃO DO PROBLEMA

O Ministério da Integração Nacional dispõe de uma infraestrutura de TI robusta, com três *data centers*, sendo dois destes em salas-segura, com ativos de *hardware* e soluções de TI que são referências de mercado. Seus recursos tecnológicos são determinantes para o fornecimento de informações e para tomada de decisões estratégicas nas atividades em que atua. Embora tenha o seu parque tecnológico bem estruturado, não é o suficiente para atender a demanda de atividades em que precisa prestar contas para os cidadãos. Sua infraestrutura de TI é cara e seu crescimento muito dispendioso, fazendo com que a utilização de seus ativos seja inadequada.

Os dois *data centers* em salas-seguras não são utilizados com redundância e nem alta-disponibilidade entre eles, mas apenas como uma extensão um do outro para suportar toda a demanda existente. A falta de recursos de *hardware* fez com que os *data centers* em salas-segura fossem utilizados independentes dentro de uma mesma infraestrutura. Estas limitações de recursos de *hardware* foram determinantes para que se buscasse alternativas que pudesse garantir o crescimento e a melhoria de serviços críticos. A alternativa encontrada foi o modelo de serviço de nuvem híbrida, que mais se adequava como solução para a realidade dos problemas que se apresentavam no momento.

O serviço de correio eletrônico do Ministério da Integração Nacional é um dos ativos mais críticos de toda sua infraestrutura de TI. É através dos serviços de correio eletrônico, por exemplo, que é realizado todos os alertas de desastres naturais e calamidades públicas para as prefeituras de todo o território nacional. O serviço de correio eletrônico é fundamental para garantir a atuação de proteção e defesa civil, através do Sistema Integrado de Informações sobre Desastres (S2ID) do Centro Nacional de Gerenciamento de Riscos e Desastres (CENAD). É através desses alertas, realizados por *e-mail*, que o Governo toma todas as medidas cabíveis de prevenção de desastres e também de liberação de verbas para as prefeituras de territórios que sofrem alguma calamidade.

O serviço de correio eletrônico, que é o *Microsoft Exchange*, apresentava limitação de crescimento e risco de indisponibilidade devido à falta de recursos de *hardware*. Os tamanhos das caixas postais não permitiam mais crescimento e causava impacto nos processos de trabalho e no atendimento das demandas de várias áreas da instituição. Recursos como armazenar mensagens dos usuários em arquivos no computador local, ou *deletar* mensagens para liberar espaço da caixa postal do usuário eram ineficazes e comprometiam a disponibilidade da informação, como em casos que os usuários apagavam mensagens que não deviam por engano e não tinha disponível um *backup* da mensagem, por estar armazenada no computador do usuário. O volume de fluxo de mensagens gerados pelos sistemas do Ministério também era um problema crítico, porque o Ministério não possuía um serviço próprio de *AntiSpam,* todo o tratamento das mensagens era realizado pelo Serpro e a equipe de TI não possuía administração da solução. Era comum casos de enfileiramento e bloqueio de falsos positivos.

Uma melhoria no serviço de correio eletrônico e o seu crescimento era uma necessidade urgente, por ser um serviço crítico e que precisa ter sua disponibilidade garantida.

4.2 – MODELO PROPOSTO DE NUVEM HÍBRIDA

Esta seção descreve a proposta de implementação de Nuvem Híbrida para o Ministério da Integração Nacional, que apresenta o modelo de infraestrutura *software* como serviço da *Microsoft*. Na seção 4.2.1 é apresentado o *SaaS Microsoft Office 365*. Na seção 4.2.2 é apresentado a adequação da infraestrutura e do ambiente para a integração com o serviço de Nuvem Híbrida no Ministério. Na seção 4.2.3 é apresentado o produto *Exchange Online*. Na seção 4.2.4 é apresentado o produto *Exchange Online Protection*.

4.2.1 – *Microsoft Office* 365

A implementação de Nuvem Híbrida no Ministério da Integração Nacional foi realizada com a integração do *Office* 365 à sua infraestrutura local, que consiste na criação do *tenant* do Ministério. O *tenant* de seu serviço *online* da *Microsoft* será criado e os usuários licenciados poderão acessar os serviços *online* da *Microsoft,* usando contas na Nuvem exclusivas ou contas sincronizadas do *Active Directory* local e, opcionalmente, federadas com o ADFS. A organização estará ciente e usando os serviços integrados.

Algumas organizações podem planejar mover toda a infraestrutura local para o *Microsoft Azure* e o *Office* 365, outras podem escolher uma solução híbrida hospedando alguns produtos no local e outros, como o *Exchange*, na Nuvem.

Integração de serviços são as tarefas necessárias para configurar os serviços *online* da *Microsoft* qualificados no escopo. O processo de integração é definido em quatro fases principais: iniciar, avaliar, corrigir e habilitar. Com um conjunto definido de tarefas e responsabilidades da *Microsoft* e do cliente para cada fase. As tarefas de migração de dados, se necessárias, serão integradas no decorrer de outras fases.

Tabela 4-1 – Fases do Processo de Integração do *Office* 365.

Iniciar	Primeiro contato com o Cliente (Planejamento)
Avaliar	Verificar se o ambiente do cliente está preparado e desenvolver um Plano de Habilitação e Implantação.
Corrigir	Corrigir problemas identificados na Avaliação. Concluir atividades de preparação para a habilitação de serviços.
Habilitar	Configurar e habilitar a infraestrutura central para o uso do serviço e provisionar os serviços online adquiridos da *Microsoft*.
Migração de Dados	Migrar as caixas de correio dos ambientes originais para o *Office* 365 *Exchange Online*.

O *Office* 365 é o pacote de produtividade baseado em nuvem da *Microsoft*, que oferecem *software* como um serviço (*SaaS*) aos usuários de todo mundo, seus produtos concentram-se em quatro áreas principais:

- Dispositivos: oferece suporte a uma grande variedade de dispositivos nos quais a interface do usuário suporta diferentes métodos de interação, incluindo toque, caneta, mouse e teclado.
- Nuvem: foi projetado para a nuvem como um serviço de demanda que está sempre atualizado. É uma solução de produtividade de Nuvem de nível empresarial com segurança robusta, confiabilidade garantida e conformidade com padrões do setor, como ISO-27001, lei de responsabilização (HIPAA) e a lei federal americana de gerenciamento de segurança da informação (FISMA).
- Mídia Social: integra redes sociais na organização, fornecendo *feeds* de notícias e serviços de *microblogging* que podem ser estendidos com o produto *Yammer*.
- Controle: fornece uma maneira segura para que as organizações controlem seus dados de negócios, com recursos como a prevenção de perda de dados (DLP), *eDiscovery* e arquivamento e de dados.

Os principais serviços do *Office* 365 consistem em equivalentes baseados em nuvem de três produtos da *Microsoft*, juntamente com um serviço de diretório integrado e uma versão de instalação *on-demand* do *Office* 2016. Esses aplicativos de produtividade populares permitem que organizações de todos os tamanhos movam sua infraestrutura de TI inteira para a nuvem ou implementem uma variedade de opções híbridas, dependendo de suas necessidades. A figura 4.1 apresenta os componentes centrais do *Office* 365.

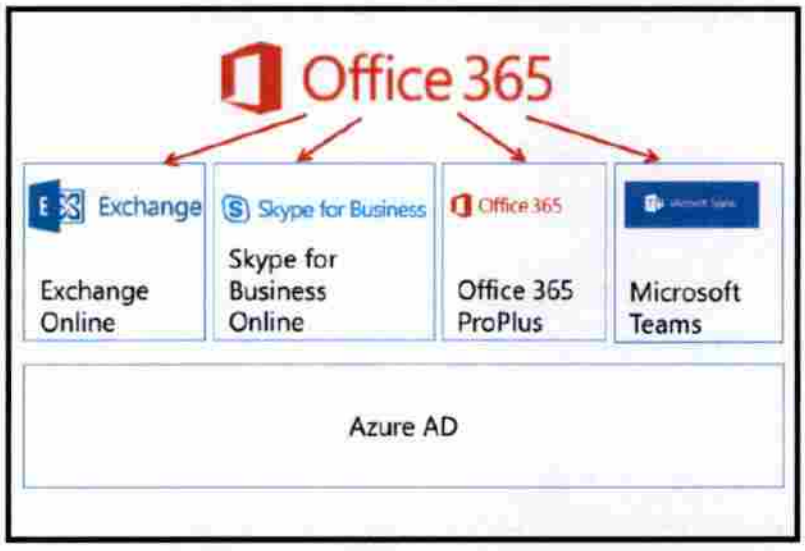

Figura 4.1 – Componentes Centrais do *Office* 365 (Microsoft, 2017).

Microsoft Azure Active Directory (*Azure AD*) sustenta todos os serviços do *Office* 365. O *Azure AD* é uma instância *online* do *Active Directory* que também fornece serviços de autenticação e autorização para outras ofertas da *Microsoft Cloud*, incluindo o *Microsoft Azure* e o *Microsoft Intune*. A autenticação através do Azure *AD* pode estar em uma base somente em nuvem, através da sincronização de diretórios ou incluir integração completa com os serviços de diretório no local por meio do suporte a serviços de Federação do *Microsoft Active Directory* (AD FS) ou outros provedores de SSO.

O *Exchange Online* no *Office* 365 é a versão mais recente desta plataforma de mensagens e colaboração, que fornece um local para escrever, ler e armazenar *e-mails*, calendário, contatos e informações sobre tarefas no *Microsoft Outlook*, *Outlook Web Access* ou *Outlook Mobile*. O *Exchange Online* inclui uma caixa de correio de 100 *Gigabyte* (GB) sem restrição e oferece suporte ao acesso da maioria dos dispositivos móveis, incluindo dispositivos *Android*, *iPhone* e *Windows Mobile*.

O *Skype for Business Online* fornece informações de presença e mensagens instantâneas, para que os outros usuários possam identificar se as pessoas estão disponíveis para conversas, chamadas e videoconferências uns com os outros. É possível criar reuniões *online* com áudio, vídeo e *web* conferência para até 250 pessoas, incluindo usuários anônimos de fora da organização. Para melhorar a produtividade, o *Skype for Business Online* fornece integração com os calendários dos usuários do *Microsoft Exchange* e também habilita o recurso "*Click-to-comunique*" no *Outlook*, no *SharePoint* e em outros aplicativos do *Office*. Além disso, introduz a integração com sistemas de PBX e videoconferência no local.

O *Office 365 ProPlus* é uma suíte de produtividade que oferece suporte à implantação de *streaming*, permitindo aos usuários clicar no ícone de instalação do aplicativo e começar a usar o próprio aplicativo enquanto o programa é instalado em segundo plano, e também oferece versões do aplicativo via *web*.

Usando a plataforma *Microsoft Teams*, que é baseada no *SharePoint Online*, é possível implementar um espaço de trabalho baseado em bate-papo e compartilhar documentos importantes, informações e atualizações de status com os colegas, manter equipes em sincronia e gerenciar projetos importantes.

Uma parte importante do processo de provisionamento do *Office* 365 é a criação da conta do *tenant*. Os procedimentos para a criação de uma conta *tenant* é descrito abaixo:

1. Decidir plano do *Office* 365 que melhor atende as necessidades da organização;

2. Verifique se tem uma conta de *e-mail* válida (a conta organizacional ou *Microsoft* funcionará bem);

3. Executar a avaliação no site do *Office* 365, inserindo as informações corretas para sua organização;

5. Concluir o processo de *logon* validando a mensagem de texto ou a chamada telefônica.

As contas de avaliação estão disponíveis para os seguintes planos do *Office* 365:

- *Business e Business Premium*
- *Enterprise* (E3 e E5)
- Educação
- Governo
- Sem fins lucrativos (*Business Premium* e E3)

Ao inscrever uma nova conta de *tenant*, é necessário fornecer informações sobre a pessoa e a empresa que está sendo inscrita. A localização do *tenant* determina onde os dados serão armazenados. Por exemplo, se o local for Alemanha, os dados serão armazenados na Europa *data centers*. O nome do administrador do *tenant* deve ser um nome real e não "administrador do sistema". O *e-mail* usado para inscrição deve estar disponível.

Será gerado um nome de domínio padrão com base no nome da empresa que foi fornecido na inscrição. Esse nome de domínio não pode ser alterado após a criação, portanto, é importante que seja verificado se esse domínio é aceitável, em seguida é solicitado a digitar uma senha e indicar um mecanismo para validar o *Sign-up*, que é feito a partir de uma mensagem de texto enviada ou de uma chamada telefônica

4.2.2 – Adequação da Infraestrutura e do Ambiente do Ministério

Nas fases de integração do *Exchange Online* e do *Exchange Online Protection* no Ministério da Integração Nacional, descobriu-se que a infraestrutura não estava adequada para suportar o serviço de Nuvem oferecido pela *Microsoft*. Foi necessário um projeto de adequação da infraestrutura para realizar uma integração eficaz com os produtos *Exchange Online* e *Exchange Online Protection*. O serviço de correio eletrônico existente teve que ser atualizado para uma versão que suportasse a integração com a Nuvem.

A topologia da infraestrutura do Ministério não permitia uma comunicação adequada com os serviços de correio eletrônico da nuvem. A topologia anterior é mostrada na figura 4.2.

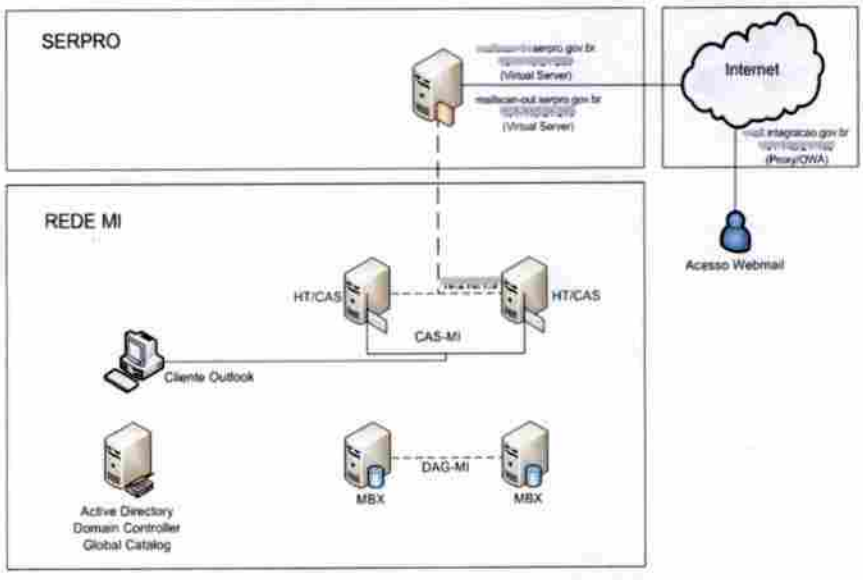

Figura 4.2 – Topologia Anterior da Infraestrutura Local do Ministério.

Para estabelecer uma comunicação eficaz com o serviço de correio eletrônico *Exchange Online*, foi necessário a implementação do serviço *Edge Transport* para realizar roteamento de mensagens entre o *Exchange* local e o *Exchange Online*, garantido o correto funcionamento de envio e recebimento de mensagens. A figura 4.3 mostra a topologia que permitiu esta integração.

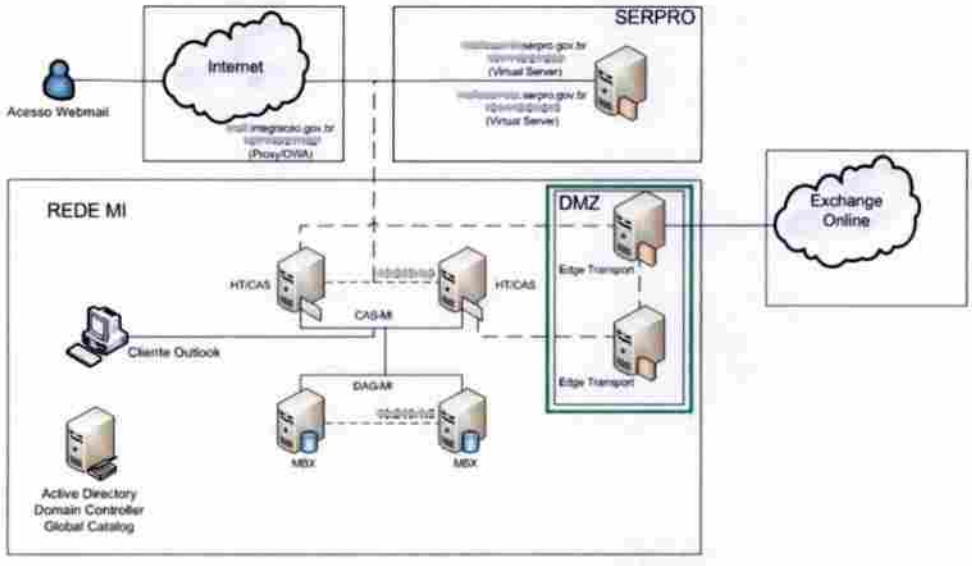

Figura 4.3 – Implementação do Edge Transport na Infraestrutura Local do Ministério.

Após a implementação do *Edge Transport*, a topologia da infraestrutura ficou adequada para a integração do *Exchange Online*. A figura 4.4 mostra a topologia atual com o *Exchange Online* e *Exchange Online Protection* corretamente integrados na infraestrutura local do Ministério.

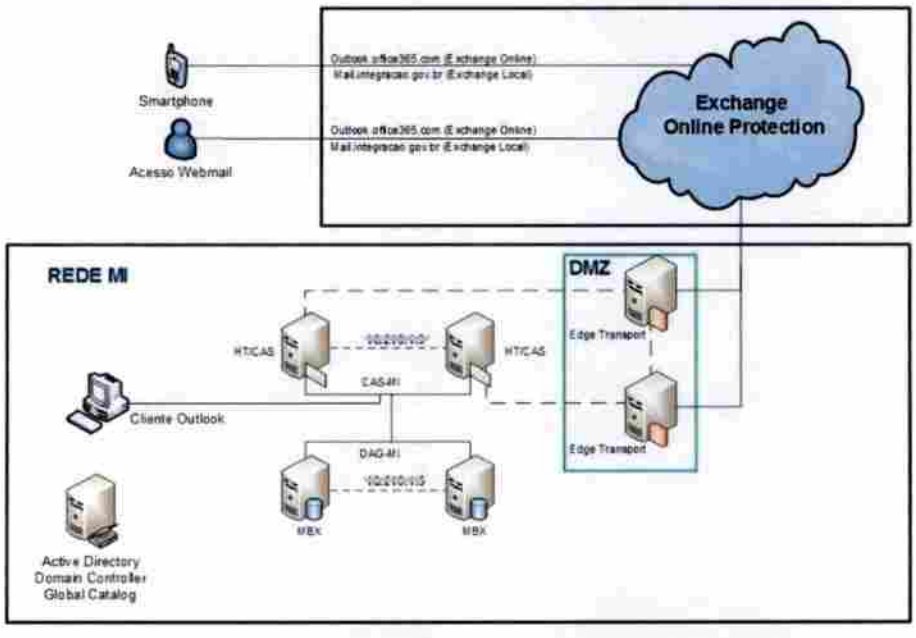

Figura 4.4 – Topologia Adequada da Infraestrutura Local do Ministério

4.2.3 – *Exchange Online*

O *Exchange Online* faz parte do pacote de produtos do *Office* 365. A sua implantação híbrida oferece às organizações a experiência e o controle administrativo com os recursos que já possuem do *Exchange* em sua infraestrutura local, com a aparência perfeita de uma única organização do *Exchange Online*. A implantação híbrida habilita recursos, como:

- Roteamento de *e-mail* seguro entre organizações locais e do *Exchange online*;
- Um catálogo global de endereços unificado, também chamado de catálogo de endereços compartilhado;
- Controle centralizado do fluxo de *e-mail* de entrada e saída;
- Movimentação de caixas de correio da infraestrutura local para a organização do *Exchange Online* e também do *Exchange Online* para a infraestrutura local;
- Gerenciamento centralizado de caixa de correio usando o Centro de Administração do *Exchange*, conforme a figura 4.2.
- Arquivamento de mensagens em nuvem para caixas de correio do *Exchange* local. O arquivamento *online* do *Exchange* pode ser usado com uma implantação híbrida.

O gerenciamento do *Exchange Online* é feito usando uma interface *Web* ou o *Windows PowerShell*. A interface *Web* inclui vários portais administrativos do *Office* 365, para poder gerenciar com o *PowerShell*, é preciso importar o módulo do *Active Directory* do *Azure* para o *Windows PowerShell*.

Os portais administrativos baseados na *Web* do *Office* 365 incluem:

- *Office* 365 *Admin Center*: um console de gerenciamento que pode usada para implantar o *Office* 365 para sua organização na nuvem, criar usuários, gerenciar domínios e licenças e administrar todos os aspectos do *Office* 365.
- Centro de Administração do *Exchange:* O centro de administração do *Exchange* (EAC) é o console de gerenciamento usada para gerenciar as configurações do *Exchange Online*. Essas configurações incluem destinatários, proteção, fluxo de mensagens, pastas públicas e etc.
- Centro de Segurança e *Compliance*: usado para gerenciar recursos de conformidade em todo o *Office* 365 para a organização. Esses recursos incluem arquivamento, prevenção de perda de dados (DLP), *eDiscovery*, relatórios, retenção e pesquisa.

- *Azure AD Admin Center*: o *Azure AD Admin Center* é usado para gerenciar a instância do *Azure Active Directory* que o *Office* 365 está usando. No centro de administração do *AD Azure*, você pode gerenciar usuários, domínios e configurações do diretório. Usando o módulo *Azure Active Directory* pelo *PowerShell*, pode-se executar tarefas administrativas que não são possíveis com o portal do *Office* 365 *Admin Center Web*. Por exemplo, automatizar tarefas repetitivas, como a criação de um grande número de contas de usuário, adicionando usuários a grupos e atualizando várias propriedades de usuário.

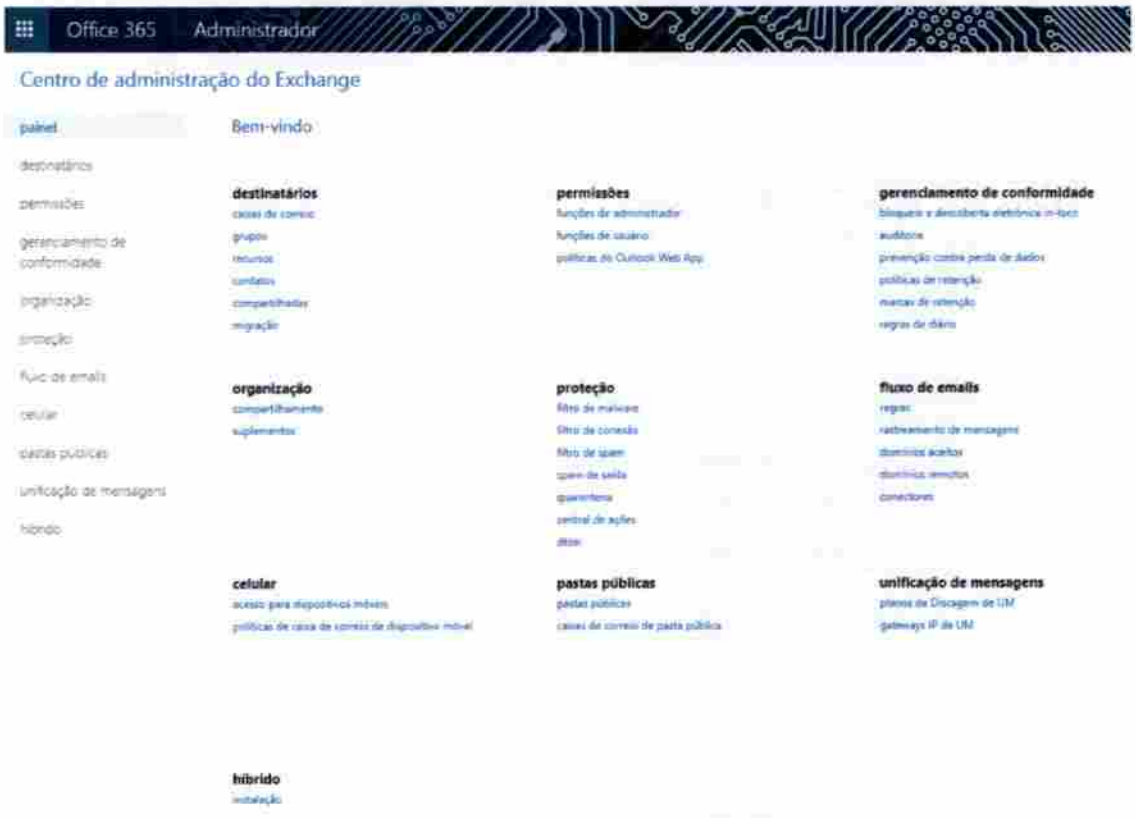

Figura 4.5 – Centro de Administração do *Exchange* (Microsoft, 2017).

Para a implantação do *Exchange Online* em uma organização, é necessário o planejamento de uma assinatura do *Office* 365, considerando:

- As necessidades que conduzirá o negócio da organização: melhor disponibilidade, segurança padrão do setor, menor custo para manutenção de *hardware* e *software* e suporte para vários dispositivos e plataformas.
- A atual infraestrutura de TI da organização: durante a transição de infraestrutura e aplicativos para a nuvem, as organizações podem optar por implantar uma solução

híbrida, na qual eles movem caixas de correio do *Exchange* para o *Office* 365 e continuam a hospedar aplicativos personalizados no local.

As organizações devem garantir a melhor maneira de gerenciar contas de usuário e serviços, que devem existir na nuvem e potencialmente no local. Deve ser feito as seguintes considerações antes de realizar uma implantação híbrida do *Exchange*:

- Requisitos de implantação híbrida: verificar se a organização local atende a todos os pré-requisitos necessários para uma implantação bem-sucedida.
- Clientes do *Exchange ActiveSync:* quando uma caixa de correio local é migrada para o *Exchange Online*, todos os clientes que acessam a caixa de correio precisam ser atualizados para usar o *Exchange Online*. Isso inclui dispositivos do *Exchange ActiveSync*. A maioria dos clientes do *Exchange ActiveSync* é automaticamente reconfigurada quando a caixa de correio é movida para o *Exchange Online*.
- Migração de permissões de caixa de correio local: permissões de: **Enviar como**, **Receber como** e **Acesso Total**, que são explicitamente aplicadas na caixa de correio são migradas para o *Exchange Online*. As permissões de caixa de correio herdadas (não explícitas) e qualquer permissão em objetos que não sejam da caixa de correio – como listas de distribuição ou usuário habilitado por *e-mail*, não são migrados.
- Suporte para permissões de caixa de correio entre instalações *Exchange*, as implantações híbridas do *Exchange* oferecem suporte ao uso da permissão de caixa de correio Acesso Total entre caixas de correio localizadas em uma organização do *Exchange* local e caixas de correio localizadas no *Exchange Online*. Uma caixa de correio em um servidor do *Exchange* local pode receber a permissão **Acesso Total** para uma caixa de correio do *Office* 365 e vice-versa. No entanto, não há suporte para o uso das permissões de caixa de correio **Enviar como** e **Receber como** em implantações híbridas entre organizações do *Exchange* local e *Exchange Online*. Também não tem suporte delegação de permissões para uma caixa de correio ou pastas individuais usando o cliente *Outlook*. Essas permissões só ficam disponíveis quando a caixa de correio que está concedendo as permissões e a caixa de correio que está recebendo as permissões estão na mesma organização. As caixas de correio que recebem essas permissões de outra caixa de correio precisam ser movidas ao mesmo tempo que ela. Se uma caixa de correio recebe permissões de várias caixas de correio, essa caixa de correio e todas as caixas de correio que concedem permissões a ela devem ser movidas ao mesmo tempo.

- Exclusão Como parte do gerenciamento contínuo de destinatários, você pode precisar mover caixas de correio do *Exchange Online* de volta para o seu ambiente local.

O *Exchange Online* oferece muitos relatórios diferentes que podem ajudar a determinar o status geral e a integridade da organização. Há também ferramentas para auxiliar na solução de problemas específicos, como mensagem que não é entregue a destinatários específicos, e relatórios de auditoria com requisitos de conformidade. A figura 4.6 mostra um exemplo de relatório gerado no *Exchange Online*.

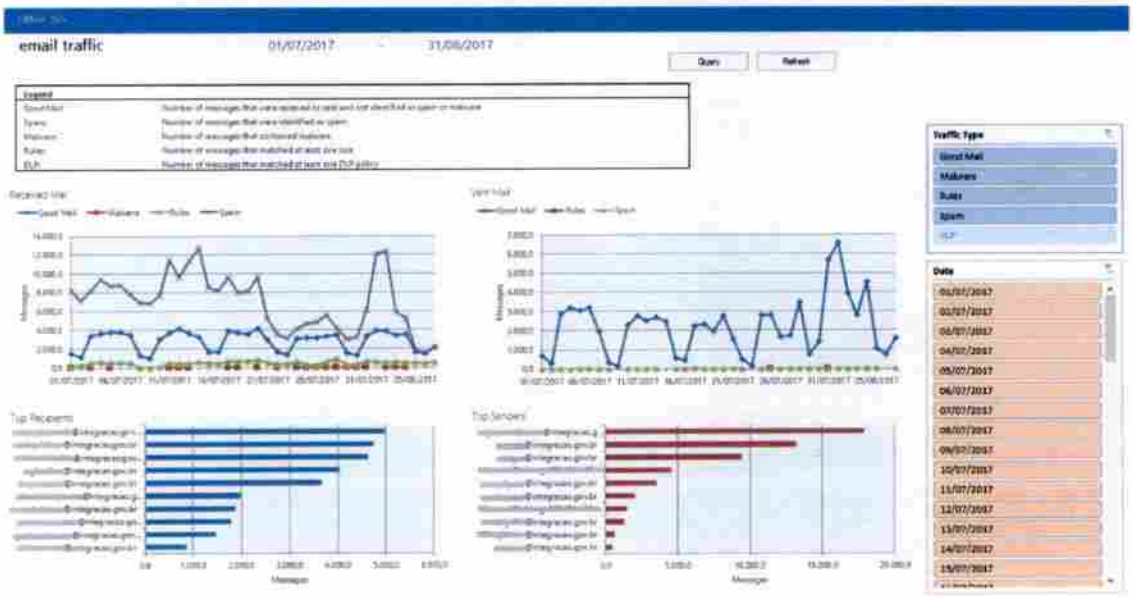

Figura 4.6 – Relatório de Tráfego de *E-mail* do *Exchange Online* (Microsoft, 2017).

4.2.4 – *Exchange Online Protection*

O *Exchange Online Protection* (EOP) é um serviço de *AntiSpam* e Antivírus em nuvem que processa toda comunicação de *e-mail* antes que seja recebido pelas caixas de correio do *Office* 365 ou servidores locais. O EOP é projetado para fornecer a melhor disponibilidade, sendo executado em uma rede de *data centers*, automaticamente roteadas entre si e balanceadas por região, assegurando a entrega de mensagens sem atraso. As configurações do EOP são customizadas com regras de conformidade de acordo com as características e necessidades da organização.

As principais maneiras de usar o EOP para proteção de mensagens podem ser divididas em: um cenário autônomo, em que fornece proteção de *e-mail* com base na nuvem para o ambiente local do *Exchange* ou qualquer outra solução de *e-mail* SMTP local; como parte do *Exchange Online*, que é a proteção padrão de *e-mail* para as contas hospedadas na nuvem e em uma implantação híbrida, em que pode ser configurado para proteger o *e-mail* local e controlar o roteamento de mensagens combinado com as contas que estão em nuvem.

Na figura 4.7 é mostrado o fluxo de funcionamento da filtragem de *e-mail* pelo EOP, em que uma mensagem passa pela filtragem de conexão, verifica a reputação do remetente e inspeciona a mensagem em busca de *malware*. Grande parte do *spam* é interceptada nesse ponto e excluída pelo EOP.

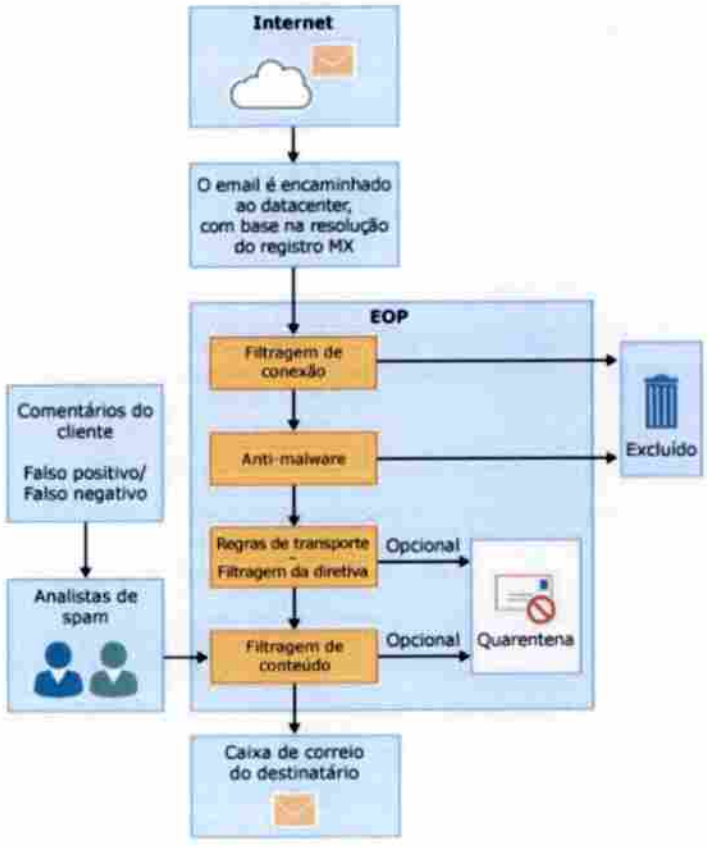

Figura 4.7 – Fluxo do *Exchange Online Protection* (Microsoft, 2017).

Uma mensagem de entrada passa inicialmente pela filtragem de conexão, que verifica a reputação do remetente e inspeciona a mensagem em busca de *malware*. Grande parte do spam é interceptada nesse ponto e excluída pelo EOP. As mensagens continuam pela filtragem da política e são avaliadas com base em regras de transporte personalizadas que

você crie ou impõe a partir de um modelo. Por exemplo, você pode ter uma regra que envia uma notificação a um gerente quando o *e-mail* chega de um remetente específico. Em seguida, as mensagens passam pela filtragem de conteúdo, na qual o conteúdo é verificado com relação à terminologia ou propriedades comuns ao *spam*. Uma mensagem considerada *spam* pelo filtro de conteúdo pode ser enviada a uma pasta de Lixo Eletrônico do usuário ou para a quarentena, entre outras opções, com base em suas configurações. Depois que uma mensagem passa com êxito por todas essas camadas de proteção, ela é entregue ao destinatário (Microsoft, 2015).

A implementação do EOP basicamente segue o seguinte processo:

- Verificar os pré-requisitos, como credenciais, nomes de domínio a serem protegidos pelo EOP, endereços IP, regras de *firewall* e et;
- Validar o domínio DNS no EOP, provando a propriedade sobre o mesmo;
- Estabelecer o fluxo de mensagens entre o EOP e o ambiente *on-premisses* por meio de conectores;
- Configurar e personalizar as configurações de acordo com as necessidades da organização e requisitos de negócio;
- Ativar o fluxo de mensagens para a filtragem no EOP, alterando os respectivos registros MX. Após esta etapa é recomendável configurar o ambiente *on-premisses* para aceitar mensagens somente originadas;
- Por último é essencial monitorar o ambiente para efetuar ajustes finos e correções conforme necessários. Geralmente alguns ajustes são demandados durante esta fase. É altamente recomendável documentar cada configuração do EOP.

O EOP permite gerar relatório interativos e fornece ferramentas para gerar relatórios customizados, para melhor monitoração e acompanhamento da quantidade de *spam* e *malware* que está sendo detectada. Para que administradores do *Exchange Online* possam gerar e visualizar relatórios é preciso que tenham a função de "administrador global". A figura 4.8 mostra um exemplo de relatório de *Spam*.

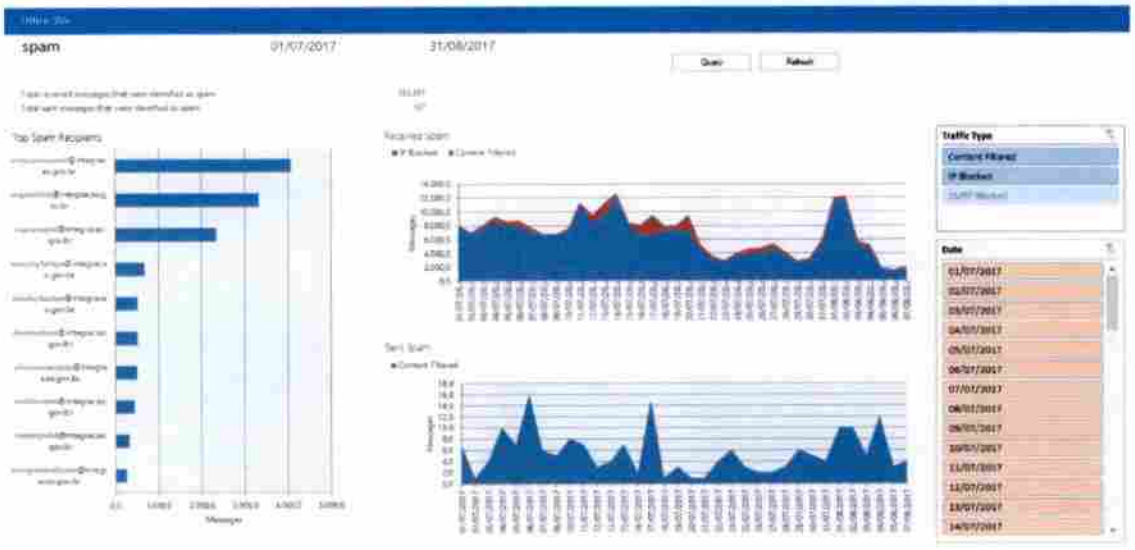

Figura 4.8 – Relatório de *Spam* do *Exchange Online Protection* (Microsoft, 2017).

Com os relatórios interativos de proteção de *e-mail*, pode-se obter rapidamente um relatório visual de dados resumidos e fazer uma busca detalhada por período. A figura 4.9 mostra um exemplo de relatório de *malware* gerada no EOP.

Figura 4.9 – Relatório de *Malware* do *Exchange Online Protection* (Microsoft, 2017).

O *Exchange Online Protection* permite gerar relatórios para verificar com que frequência as regras de fluxo de *e-mail* estão sendo correspondidas. A figura 4.10 mostra um relatório de regras do EOP.

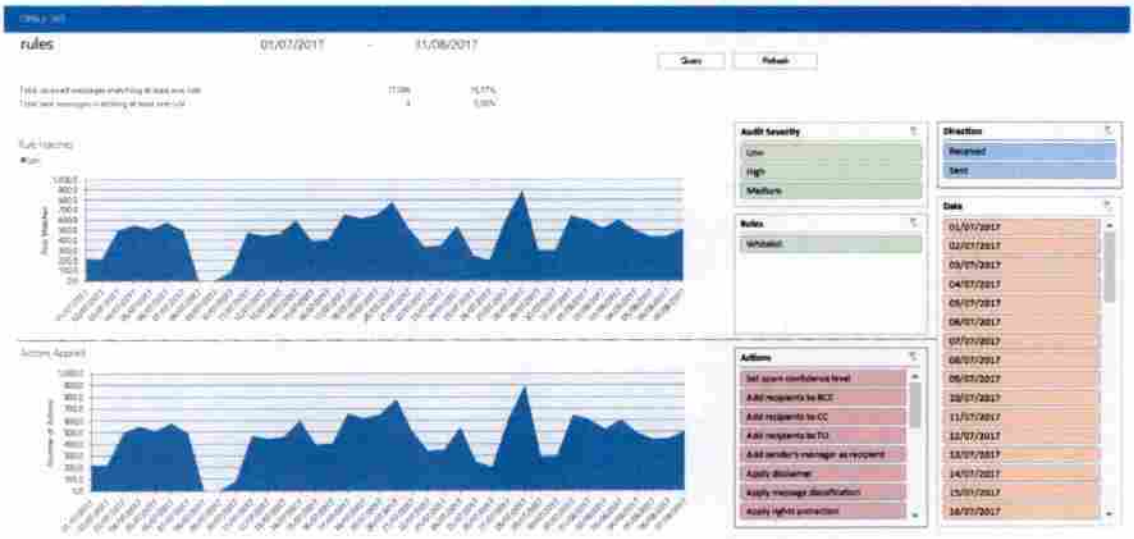

Figura 4.10 – Relatório de Regras do *Exchange Online Protection* (Microsoft, 2017).

Relatórios de proteção de *e-mail* do *Exchange* também estão disponíveis pelo *PowerShell* remoto.

4.3 – RESULTADO E ANÁLISE DO AMBIENTE ATUAL

Esta seção tem como objetivo demonstrar o uso da computação em nuvem em seu aspecto prático, voltado para o cenário corporativo e seus detalhes de implantação, através do modelo de nuvem híbrida com *SaaS Exchange Online* do *Office* 365. Apresenta um projeto realizado que consiste na configuração da infraestrutura de TI do Ministério da Integração Nacional para a implementação do *Exchange* Híbrido, em que seu sistema de correio eletrônico trabalha de forma coexistente do ambiente local e Nuvem. A implantação do *Exchange* Híbrido se justifica por prover escalabilidade e elasticidade para garantir o crescimento e mais segurança e disponibilidade no serviço de correio eletrônico de uma maneira mais otimizada, utilizando todos os recursos de serviço em nuvem oferecido pela *Microsoft* em serviços de mensageria.

A adoção do *Exchange Online* no Ministério da Integração Nacional foi bem-sucedida e está implementada para trabalhar em modo híbrido, podendo migrar caixas de correio dos usuários para nuvem de acordo com as demandas que são solicitadas.

O *Exchange Online* trouxe diversas melhorias para o Ministério da Integração Nacional, dentre as quais podem ser citadas:

- Redução significativa na utilização dos recursos de *hardware* na infraestrutura de TI local;
- Maior segurança e disponibilidade do serviço de *e-mail*;

- Maior facilidade de acesso para o usuário final;
- Facilidade de gerenciamento e administração do *Exchange*, podendo as caixas de *e-mail* ser movidas da infraestrutura local para nuvem e vice-versa;
- Caixas de correio com maior capacidade de armazenamento, aumentando de um *gigabyte* anterior para cem *gigabytes* atual, no *Exchange Online*, sem restrição de crescimento;
- Aumento no tamanho de anexos, de dez *megabyte* para cinquenta *megabyte*;
- Administração do serviço de *AntiSpam*;

O serviço de correio eletrônico do Ministério da Integração Nacional se tornou mais estável e confiável com a implementação do *Exchange Online* em modo híbrido. Os incidentes e requisições de correio eletrônico gerados pela instituição, diminuíram consideravelmente, desonerando o atendimento do suporte técnico.

5 – CONSIDERAÇÕES FINAIS

O trabalho apresentado pode demonstrar a sua utilização em um cenário corporativo e, também, da administração pública federal, através do modelo de nuvem híbrida com *SaaS Exchange Online* do *Office* 365.

A metodologia de estudo de caso, utilizada neste trabalho, permitiu ter uma visão ampla e detalhada das necessidades que ocorrem na TI do ambiente corporativo.

O estudo de caso realizado no Ministério da Integração Nacional, apresenta a adoção do produto *Exchange Online* e *Exchange Online Protection*, que foi bem-sucedida e trouxe melhorias significativas para a TI, das quais podemos citar:

- Maior confiabilidade para os processos críticos da instituição que dependem do serviço de correio eletrônico (que são quase todos);
- Maior flexibilidade e elasticidade para o crescimento das demandas de correio eletrônico que são gerados pelo Ministério da Integração Nacional;
- Maior disponibilidade e facilidade de acesso ao serviço de correio eletrônico.

5.1 – TRABALHOS FUTUROS

A base de uma nuvem computacional é a capacidade de interoperabilidade entre seus componentes e o modelo de nuvem híbrida é um processo intermediário para que a instituição possa explorar com mais segurança e confiança a tecnologia de computação em nuvem. É recomendável como trabalho futuro um estudo sobre nuvem privada, em que pode ser melhor explorado tecnologias como orquestração e automação de processos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 17788:2016. (2016). Tecnologia da Informação – Computação em Nuvem – Visão Geral e Vocabulário.

ABNT NBR ISO/IEC 27001:2006. (2006) – Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos.

ABNT NBR ISO/IEC 27002:2005. (2005). Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação. ISBN 978-85-07-00668-0.

BRASIL. Decreto nº 1.048 de 21 de Janeiro de 1994.

BRASIL. Decreto nº 7.579 de 11 de Outubro de 2011.

BRASIL. Decreto nº 8.135 de 04 de Novembro de 2013.

BRASIL. Decreto nº 8.638 de 15 de Janeiro de 2016.

BRASIL. Lei nº 12.527 de 18 de Novembro de 2011.

DIAS, Carlos Luís Soares. Computação em nuvem – Brasília. 2016. 37f. Trabalho de Conclusão de Curso (Especialização em Rede de Computadores), UniCEUB - Centro Universitário de Brasília - DF. Disponível em: http://repositorio.uniceub.br/bitstream/235/8146/1/51106265.pdf. Acessado em 27 JUL. 2017.

DIÓGENES, Yuri. VERAS, Manoel. Certificação cloud essentials: guia preparatório para o exame CLO-001. Rio de Janeiro: Novaterra, 2015. ISBN 978-85-61893-26-2

DSIC Departamento de Segurança da Informação e Comunicação / GSI / PR Gabinete de Segurança Institucional da Presidência da República. Norma complementar 14/IN01/DSIC/GSI/PR de 30 de janeiro de 2012. Diretrizes Relacionadas À Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos Órgãos e Entidades da Administração Pública Federal. Disponível em: http://dsic.planalto.gov.br/documentos/nc_14_nuvem.pdf. Acessado em: 12 JUN. 2017.

FERREIRA, Marina Alves. ANDRADE, César Augusto Borges. Cloud computing – normas, leis e orientações do governo brasileiro – Brasília. 2016. 24f. Trabalho de Conclusão de Curso (Especialização em Infraestrutura e Gestão de Serviços de TI), Faculdade JK - DF.

JÚNIOR, Nelson de Melo Guimarães. HEINZELMANN, Ricardo Luiz de Oliveira.

Plataforma de computação em nuvem com serviços orquestrados: um experimento em uma IES. Rio de Janeiro. 2016. 61f. Tese de Doutorado (Engenharia de Computação e Informação). Universidade Federal do Rio de Janeiro. Escola Politécnica. Disponível em: http://monografias.poli.ufrj.br/monografias/monopoli10019408.pdf. Acessado em 27 JUL. 2017.

KATZER, Matt. (2015). Moving to Office 365: Planning and Migration Guide. Apress (ISBN-13: 978-1-4842-1198-4 or ISBN-13: 978-4842-1197-7).

MEDEIROS, Monnalisa Christina Pereira de. Análise da implantação de computação em nuvem: estudo de caso na Alfa Informática .Net – Currais Novos. 2015. 76f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação), Departamento de Computação e Tecnologia, Universidade Federal do Rio Grande do Norte. Caicó - RN. Disponível em: https://monografias.ufrn.br/jspui/handle/123456789/2110. Acessado em 27 JUL. 2017.

MICROSOFT. Fluxo do *Exchange Online Protection*. 2017. Disponível em: https://technet.microsoft.com/pt-br/library/jj723119(v=exchg.150).aspx. Acessado em: 09 AGO. 2017.

MPOG. Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem. 2016. Disponível em: https://www.governoeletronico.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf/view. Acessado em: 17 JUL 2017.

RAMALHO, Neilson Carlos Leite. Um estudo sobre a adoção da computação em nuvem no Brasil – São Paulo. 2012. 157f. Dissertação (Mestrado em Ciências), Escola de Artes, Ciências e Humanidades da US - SP. Disponível em: www.teses.usp.br/teses/disponiveis/100/100131/.../Dissertacao_Neilson_Ramalho.pdf. Acessado em 27 JUL. 2017.

TAURION, Cezar. Cloud computing: computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009. ISBN 978-85-7452-423-8

VERAS, Manoel. Cloud Computing: nova arquitetura da TI. Rio de Janeiro: Brasport, 2012. ISBN 978-85-7452-489-4

APÊNDICES

APÊNDICE A – IMPLANTAÇÃO DO *EXCHANGE ONLINE*

Neste apêndice é descrito todos os processos necessários para adequação da infraestrutura de TI local para suportar a implantação do *Exchange Online.*

a. Execução do **IdFix DirSync**: o IdFix varre os atributos dos objetos do *Active Directory* local e caso alguma inconsistência/valor não adequado ao *Office* 365 seja encontrado uma correção será sugerida.

Ferramenta: **IdFix DirSync Error Remediation Tool**
Download em: https://www.microsoft.com/en-us/download/details.aspx?id=36832.
Requisitos para execução: *Windows Server* 2008 R2 e *Windows* 7 65 *bits*. O servidor ou estação de trabalho deve ser membro do domínio.
Usuário: Administrativo

b. Execução do **HRC** – Ferramenta de validação do ambiente: esta ferramenta verifica alguns pré-requisitos da infraestrutura local como conectividade entre outras configurações.

Ferramenta: **HRC**
Acesso da ferramenta: https://configure.office.com/Scenario.aspx?sid=11
Requisitos para execução: *Internet Explorer* 9 ou posterior, *Windows* 7 ou posterior e *Microsoft* .net *Framework* 3.5). O servidor ou estação de trabalho deve ser membro do domínio.
Usuário: Administrativo
Instruções:

1. Vá para **HRC**;
2. Faça o *login* usando suas credenciais de administrador para o *tenant* da organização;
3. Selecione a opção "*Advanced*", e então *next*
4. *Click* em *run checks*

Importante: Para execução desta ferramenta, deve estar em uma estação de trabalho autenticada no domínio e com acesso administrativo.
Nota: O relatório do **HRC** será automaticamente salvo nos servidores da *Microsoft*.

c. **Verificações de integridade, disponibilidade e conectividade**: esta ferramenta executa diversos testes para determinar a capacidade da infraestrutura de TI local para o uso dos serviços do *Office* 365. Os resultados da execução desta ferramenta são enviados automaticamente para a *Microsoft* para que possam ser revistos. Você pode executar esta ferramenta múltiplas vezes sem perder os resultados anteriores. Esta ferramenta deve ser executada em três diferentes máquinas de sua rede, pois os testes executados variam em função do tipo de computador em que são executados e das funções que este computador desempenha:

- Uma estação de trabalho da rede local, com um usuário padrão sem direitos administrativos.
- Um servidor *Exchange* publicado para a *Internet* (*Exchange* 2007 CAS ou superior)
- Um controlador de domínio

Ferramenta: **Verificações de integridade, disponibilidade e conectividade**
Acesso da ferramenta: https://configure.office.com/Scenario.aspx?sid=11.
Importante: O *login* deve ser com as credenciais do *Office* 365. Uma vez autenticado, escolha fazer os testes **Rápido** e **Avançado**, marcando as duas opções, para obter o quadro mais completo possível. Os testes devem durar em torno de dez a quinze minutos, mas em ambientes complexos, o tempo pode ser maior.

d. ***On-Premises Inventory Check***: Esta ferramenta executa diversos testes para determinar a capacidade de seu ambiente para o uso dos serviços do *Office* 365 e ajudará a entender a arquitetura técnica do *Active Directory* na infraestrutura de TI local e do correio eletrônico *Exchange Server*. Os resultados da execução desta ferramenta são enviados automaticamente para a *Microsoft* para que possam ser revistos. Você pode executar esta ferramenta múltiplas vezes sem perder os resultados anteriores. Esta ferramenta deve ser executada a partir de um servidor *Exchange Server* CAS, autenticado com um usuário membro do grupo de segurança *Exchange Organization Management*.

Ferramenta: ***On-Premises Inventory Check***
Acesso da ferramenta: https://configure.office.com/Scenario.aspx?sid=28.
Importante: O login deve ser com as credenciais do *Office* 365 e escolha a opção "Eu preciso de um inventário do meu ambiente local".

e. Implementar as atualizações de compatibilidade do *Exchange* Híbrido:

Atualização: **Update Rollup 11 for Exchange Server 2010 Service Pack 3**

Download em: https://support.microsoft.com/en-us/kb/3078674

Atualização: **Microsoft Exchange Server 2010 Service Pack 3 (SP3)**

Download em: https://www.microsoft.com/en-us/download/details.aspx?id=36768

Atualização: **Office 2016 Deployment Tool**

Download em: https://www.microsoft.com/en-us/download/details.aspx?id=49117

Atualização: **Prepare to upgrade Office 365 ProPlus to the Office 2016 version**

Download em: https://technet.microsoft.com/en-us/library/mt422981.aspx

f. Criação de registros DNS:

- ~~*autodiscover*~~.integracao.gov.br (NLB do CAS/*Hub Transport*)
- ~~*mail*~~.integracao.gov.br (NLB do CAS/*Hub Transport*)
- TXT de validação do domínio (a ser definido durante a configuração do *Exchange* híbrido)

g. Alteração de registro DNS:

- Redução do TTL dos domínios mi.gov.br, cenad.gov.br e integração.gov.br
- Alteração dos registros SPF dos domínios mi.gov.br, cenad.gov.br e integração.gov.br
- Criação dos registros TXT nos domínios mi.gov.br e integração.gov.br
- Permitir que o *Exchange Online* e a solução atual enviem *email* em nome dos domínios mi.gov.br, cenad.gov.br e integração.gov.br

h. Publicação no *Firewall*: é imperativo que a comunicação entre EOP e *Edge* e entre *Edge* e *Hub* esteja funcionando perfeitamente.

- Endereços do EOP estão disponíveis em: https://technet.microsoft.com/library/dn163583(v=exchg.150).aspx.
    - Importante: Os intervalos de endereços IP fornecidos pela Microsoft são usados apenas para retransmissão por meio de conectores de clientes. As

alterações na lista de endereços IP são raras e são comunicadas com antecedência.

- *Internet* -> NLB do CAS/*Hub Transport* (TCP25, TCP80, TCP443)
  - EOP para *Edge*: TCP 25
  - *Edge* para EOP: TCP 25
  - *Edge* para *Hub*: TCP 25
  - *Hub* para *Edge*: TCP 25 e TCP 50636
- Os relógios dos servidores *Exchange Edge* e *Hub* devem estar sincronizados
- Os servidores *Edge* devem ter instalado o certificado digital *.integracao.gov.br
- O certificado digital *.integracao.gov.br deve estar associado ao serviço SMTP, mas não deve ser o certificado padrão para SMTP
- O certificado SMTP padrão deve ser o próprio certificado auto assinado, criado durante a instalação do *Edge*
- Os servidores *Edge* devem estar corretamente licenciados antes de configurar o **EdgeSync**
- Na hora de configurar o **EdgeSync**, não criar o conector de saída para Internet

i. Configurar o **EdgeSync**:

- Em cada um dos *Edge*:

New-EdgeSubscription -FileName "c:\<nome-do-servidor-edge>.xml"

- No *Hub*:

New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\<nome-do-servidor-edge>.xml" -Encoding Byte -ReadCount 0)) -Site "<nome-do-site-AD>" -CreateInternetSendConnector $false

j. Configurar o fluxo de *e-mails* para o *Office* 365:

- Executar o ***Hybrid Configuration Wizard*** levando em consideração as informações dos servidores *Edge*
- Criar conectores de entrada no *Edge*
- Alterar o conector de envio na organização *Exchange*

k. Testar o fluxo de *e-mails*:

- Do Ministério da Integração para *Internet*

- Da *Internet* para o Ministério da Integração
- Do Ministério da Integração para o *Exchange Online*
- Do *Exchange Online* para o Ministério da Integração
- Da Internet para o *Exchange Online*
- Do *Exchange Online* para a *Internet*

1. Criação do site *SharePoint* para troca de dados com a *Microsoft*

- Obter um computador executando Sistema operacional *Windows* 64 *bit*
  - *Windows* 10, 8.1, 8 ou 7
  - *Windows Server* 2012 R2, 2012, 2008 R2
- Instalar o ***Microsoft Online Services Sign-In Assistant for IT Professionals RTW***
  Download em: https://www.microsoft.com/en-us/download/details.aspx?id=41950.
- Instalar o ***Azure Active Directory Module for Windows PowerShell (64-bit version)***
  Download em: http://go.microsoft.com/fwlink/p/?linkid=236297.
- Instalar o ***SharePoint Online Management Shell*** numa estação *Windows* 10/8.1/8/7 SP1 64-bit ou num servidor *Windows Server* 2012 R2/2012/2008 R2 SP1
  Download em: https://www.microsoft.com/en-us/download/details.aspx?id=35588.
  - Executar ***sharepointonlinemanagementshell_4915-1200_x64_en-us.msi***
  - Reiniciar o computador
- Criar uma conta para acesso ao site SharePoint
- Criar pasta *Solutions* na área de trabalho
- Copiar o arquivo gerado **FTC-ProvisionMigrationSite.ps1.txt** para o computador
- Renomear o arquivo **FTC-ProvisionMigrationSite.ps1.txt** para **FTC-ProvisionMigrationSite.ps1**
- Abir uma sessão de *PowerShell* evevada (como administrador)
- Conceder permissão para execução de *scripts* sem assinatura digital

  Set-ExecutionPolicy Unrestricted -Scope Process
- Navegar para a pasta onde o *script* foi gravado
- Executar o *script*

  .\FTC-ProvisionMigrationSite.ps1
- Informar uma credencial administrativa do *Office* 365 quando questionado pelo *script*
- Acessar o site https://integracao.sharepoint.com/sites/migracao
- Clicar no link *Solution Gallery*
- Clicar no botão *Activate*

- Acessar o site https://integracao.sharepoint.com/sites/migracao
- Selecionar a guia *Custom* e Clicar no botão OK
- Depois de algum tempo na tela "*Working on it*", será aberta a página "*Set Up Groups for this Site*"
- Clicar no botão OK

m. Criação das contas administrativas para migração

- **GlobalAdmin**

  integracaoCloudAdmin1@integracao.onmicrosoft.com

  integracaoCloudAdmin2@integracao.onmicrosoft.com

  integracaoCloudAdmin3@integracao.onmicrosoft.com

- **AD Local com permissão de *recipiente admin***

  integracao\OnPremMigAdmin1

  integracao\OnPremMigAdmin2

  integracao\OnPremMigAdmin3

  integracaoTestMbx01@integracao.gov.br

  integracaoTestMbx02@integracao.gov.br

  integracaoTestMbx03@integracao.gov.br

  integracaoTestMbx04@integracao.gov.br

  integracaoTestMbx05@integracao.gov.br

  integracaoTestMbx06@integracao.gov.br

  integracaoTestMbx07@integracao.gov.br

  integracaoTestMbx08@integracao.gov.br

  integracaoTestMbx09@integracao.gov.br

  integracaoTestMbx10@integracao.gov.br

APÊNDICE B – IMPLANTAÇÃO DO *EXCHANGE ONLINE PROTECTION*

Neste apêndice é descrito a implantação do *Exchange Online Protection* (EOP). Primeiramente foi implementado um ambiente piloto para que a equipe de TI pudesse explorar mais a solução do EOP. Como sugestão, o domínio com menos uso **"mi.gov.br"** foi utilizado nesta fase, assim possibilitou a equipe ter uma familiarização com o EOP, efetuando as configurações necessárias, eventuais ajustes finos, monitorando, documentando as configurações, garantindo confiança para operar a solução e implantar em produção o domínio principal **"integração.gov.br".**

a. Realizar os devidos processos internos para as alterações necessárias nos respectivos registros DNS em suas zonas;

b. O acesso as configurações do *AntiSpam* atual (hospedado e suportado pelo SERPRO), ajudara a assegurar que regras de negócio, especificações de segurança e conformidade, bloqueios (*blacklists*), *whitelists* sejam migradas. Com as informações em mãos, normalmente, é investido um tempo para analisa-las e traduzi-las para serem portadas para o EOP, já que as configurações variam muito de fabricante para fabricante.

c. Efetuar testes com o recurso para mover spam para a pasta Lixo Eletrônico (*Junk Email*) do *Outlook*. Para usar a funcionalidade é necessário criar duas regras específicas de transporte no ambiente *On-Premisses*. É importante também lembrar que antes de implementar o recurso é recomendável instruir os usuários sobre a nova funcionalidade. As regras a serem criadas são:

```
Set-OrganizationConfig –SCLJunkThreshold 4

New-TransportRule "NameForRule" -HeaderContainsMessageHeader "X-
Forefront-Antispam-Report" -HeaderContainsWords "SFV:SPM" -SetSCL 6
```

New-TransportRule "NameForRule" -HeaderContainsMessageHeader "X-Forefront-Antispam-Report" -HeaderContainsWords "SFV:SKS" -SetSCL 6

- Efetuar testes com base nas configurações realizadas, medindo se tudo que foi configurado está efetivo no ambiente;
- Monitorar a solução de perto, acompanhando o fluxo de mensagens, *logs* e rastreamentos de mensagens. Isso ajudará a efetuar ajustes finos finais. Validar se todas as regras de negócio estão sendo atingidas;
- Após conclusão dos itens entra a migração do MX do domínio principal **"integracao.gov.br"** para o EOP;
- É recomendável notificar os usuários quanto a utilização e monitoração da pasta Lixo Eletrônico, de forma que verifiquem periodicamente a pasta em busca de falsos-positivos;
- É recomendável ainda eleger alguns usuários para coletar o *feedback* quanto a utilização, como está a filtragem de mensagens, monitorar pasta lixo eletrônico e etc;
- Avaliar e acompanhar para configurar as mensagens de entrada com a opção de *"Hard Fail"* de SPF em caso de falha, isso ajudará a reduzir a quantidade de *Spam* entrando na organização.

d. Acompanhar o comportamento do ambiente híbrido *Exchange Server* durante e após a virada da entrada de mensagens provenientes da *Internet* do *AntiSpam* de terceiros (*Proofpoint* no SERPRO) para o *Exchange Online Protection*, através do ajuste/apontamento de registros MX e SPF do domínio SMTP principal @integracao.gov.br.

- ***Enabled Directory-based Edge Blocking (DBEB)*** – todos domínios foram marcados como autoritativos.
- ***Fine tune anti-malware and anti-spam settings in Exchange Online Protection* (EOP)**:

  Create or adapt an SPF TXT record for your SMTP domains (@integracao.gov.br and others, if any)

- Pendente alteração de sintaxe de registro SPF para inclusão de *-all* no final, pois configuração atual encontra-se menos restritiva: v=spf1 ip4:~~200.198.213.91~~ ip4:~~200.198.213.92~~ *include:spf.protection.outlook.com ~all*

- ***Change your MX record to point to*** integracao-gov-br.*mail.protection.outlook*.com – virada da entrada de e-mails para o *Exchange Online Protection* realizada.
    - *Test if the mail is flowing correctly, from and to different directions*:
        - *Exchange Online Protection* > *Internet*;
        - *Internet* > *Exchange Online Protection*.
    - Testes de envio e recebimento de mensagens de e para a Internet foram executados.

e. Principais configurações do EOP: para iniciar o processo de configuração é necessário conectar-se ao *Tenant* do *Office* 365 utilizando o Remote *PowerShell*:

```
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://ps.protection.outlook.com/powershell-liveid/ -Credential
$UserCredential -Authentication Basic -AllowRedirection
Import-PSSession $Session
```

f. Importando dados de *Whitelist*:

- O Office 365 trabalha com três tipos de *whitelist*: *Domain Lists*, IP *Address Lists* e *Email Address Lists*. É necessário criar uma regra de transporte para cada tipo de lista.
- É possível importar dados para as configurações do EOP. Para importar os dados da *Whitelist* é necessário tratar o arquivo, deixando conforme alguns exemplos abaixo:
    - **IP Address List:**
        - **Formato do arquivo CSV:**

          WhiteListIPAddressList

          100.100.100.22-100.100.100.25

          100.100.100.221

          10.10.10.1-10.10.10.22

          100.100.100.0/24

        - **Cmdlet:**

```
$csv = import-csv "C:\CSV\WhiteListIPAddressList.csv"
```

New-TransportRule "WhiteList – IP Address List" -SenderIpRanges $csv.WhiteListIPAddressList -setscl -1 -Comments "Listagem de endereços IP em Whitelist" -Setscl -1

- **Domain List**
  - **Formato do arquivo CSV:**

    WhiteListDomainList

    hotmail.com

    outlook.com

    google.com

    microsoft.com
  - **Cmdlet:**

$csv = import-csv "C:\CSV\WhiteListDomainList.csv"

New-transportrule "WhiteList – Domain List" -senderdomainIs $csv.WhiteListDomainList -setscl -1

- **Email Address List**
  - **Formato do arquivo CSV:**

    WhiteListEmailAddressList

    xxx@*hotmail*.com

    mh197@*microsoft*.com

    c11@*home.net*

    wsws@nfl.com
  - **Cmdlet:**

$csv = import-csv "C:\CSV\WhiteListEmailAddressList.csv"

New-TransportRule "WhiteList – Email Address List" -AnyOfRecipientAddressContainsWords $csv.WhiteListEmailAddressList -setscl -1

g. Importando dados de *Blacklist*:

- As *Transport Rules* do EOP possuem algumas limitações quanto ao tamanho e número de caracteres para as respectivas listagens

- Ao importar os dados da *blacklist* ou para qualquer outra regra é importante validar a ação que está sendo configurada para cada regra (Quarentena, deletar sem notificar, rejeitar e etc.).

    - **Para importar os endereços IP bloqueados:**
        - **Formato do arquivo CSV:**

          BlackListIPAddressList

          100.100.100.22-100.100.100.25

          100.100.100.221

          10.10.10.1-10.10.10.22

          100.100.100.0/24
        - **Cmdlet:**

$csv = import-csv "C:\CSV\BlackListIPAddressList.csv"

New-TransportRule "BlackList – IP Address List" -SenderIpRanges $csv.BlackListIPAddressList -DeleteMessage $True -StopRuleProcessing $True -Comments "Regra para bloqueio de endereços IP"

    - **Blacklist para Domain List:**
        - **Formato do arquivo CSV:**

          BlackListDomainList

          xgmail.com

          mfacebook.com

          sgoogle.com
        - **Cmdlet:**

$csv = import-csv "C:\CSV\BlackListDomainList.csv"

New-TransportRule "BlackList – Domain List" -senderdomainIs $csv.BlackListDomainList -DeleteMessage $True -StopRuleProcessing $True

    - **Bloquear endereços de email específicos:**
        - **Formato arquivo CSV:**

          BlackListEmailAddressList

          xxxx@*hotmail*.com

          @gmail.com

cte@*test*.com

wsws@*soccer*.com

- **Cmdlet:**

$csv = import-csv "C:\CSV\BlackListEmailAddressList.csv"

New-TransportRule "BlackList – Email Address List" -

AnyOfRecipientAddressContainsWords $csv.BlackListEmailAddressList -

DeleteMessage $True -StopRuleProcessing $True

- **Bloquear extensões de arquivos**: para bloqueio de determinadas extensões de arquivos, os **cmdlets** disponibilizados abaixo contém sintaxes diferentes para a ação a ser tomada caso a extensão seja detectada.
  - **Formato arquivo CSV:**

    FileExtensionsToBlock

    exe

    pif

    bat

    scr
  - **Cmdlet**: neste exemplo rejeitando a mensagem enviada e notificando o remetente com um NDR (*Non Delivery Report*) personalizado.

$csv = import-csv "C:\CSV\FileExtensionsToBlock.csv"

New-TransportRule "Regra Bloqueio de Extensoes - EXE" –

AttachmentExtensionMatchesWords $csv.FileExtensionsToBlock –

RejectMessageReasonText "Extensao de arquivo não permitida. Categoria EXECUTAVEIS"

  - **Cmdlet**: neste exemplo enviando a mensagem para a quarentena e notificando o destinatário com uma mensagem personalizada,

$csv = import-csv "C:\CSV\FileExtensionsToBlock.csv"

New-TransportRule "Regra Bloqueio de Extensoes - EXE" –

AttachmentExtensionMatchesWords $csv.FileExtensionsToBlock -

GenerateNotification 'O remetente %%From%% enviou um anexo na mensagem com o assunto %%Subject%% em %%MessageDate%% que foi classificado na categoria de arquivos Executaveis, que atualmente não é permitido pelas

políticas de uso. A sua mensagem foi enviada para quarentena.' -Quarantine $True

- As mensagens e notificações configuradas podem utilizar outros "*placeholders*" de campos presentes na mensagem. O campo precisa estar entre "%%".

    - **Bloquear palavras no assunto das mensagens:**
        - **Formato arquivo CSV:**

          WordsToBlock

          1000 mulheres

          Fique rico

          Importante abra agora

          Atualização do seu homebanking
        - **Cmdlet:**

```
$csv = import-csv "C:\CSV\WordsToBlock.csv"
New-TransportRule "Words in subject to Block" –SubjectContainsWords
$csv.WordsToBlock –FromScope NotInOrganization -Quarantine $True
```

h. Regras especificas

- *Malware:* regra para notificação personalizada ao usuário caso seja detectado vírus / malware na mensagem:

```
Set-MalwareFilterPolicy -Identity 'Default' -FileTypes $null -CustomAlertText 'Os
anexos contidos na mensagem enviada para o usuário %%To%% foi bloqueada.'
-Action 'DeleteAttachmentAndUseCustomAlertText'
```

- Bloqueios adicionais: regras que bloqueiam *emails* originados de um domínio e palavras especificas no assunto e no corpo da mensagem. Inicialmente três regras estão sendo criadas, uma para bloquear os domínios conhecidos, outra para bloquear alguns termos no remetente e outra para identificar a palavra "TESTE" no corpo ou assunto.
- Para a regra que bloqueia os domínios relacionados a "TESTE" foi utilizado o cmdlet abaixo, que procura os domínios especificados e coloca a mensagem na quarentena (Hosted Quarantine), possui ainda a exceção caso o usuário faça parte de um grupo:

New-TransportRule "Bloqueio TESTE por Nome de Dominio" -senderdomainIs "teste.com.br","teste.com.br","teste.campanhasdemkt.net" -Quarantine $True -StopRuleProcessing $False -Comments "Regra de bloqueio para remetentes com os dominios conhecidos de TESTE" -ExceptIfSentToMemberOf grupo-Exceto@empresa.com.br

- Regra para bloquear termos especificados com a palavra "TESTE" e algumas variantes. Domínios que possuem nomes que possam ser identificados incorretamente é sugerido que sejam colocados na *WhiteList*.

  New-TransportRule "Bloqueio TESTE por palavras no Remetente" -RecipientAddressContainsWords @('.teste.','@teste.','^teste$','@teste$','@teste') -Quarantine $True -StopRuleProcessing $False -Comments "Regra de bloqueio para palavras especificas contidas no remetente com o domínio da TESTE" -ExceptIfSentToMemberOf grupo-Exceto@empresa.com.br

- Para bloqueio de termos com a palavra "TESTE" no corpo ou no assunto da mensagem:

  New-TransportRule "Bloqueio TESTE por palavras no Assunto e Corpo da mensagem" -SubjectOrBodyContainsWords @('^TESTE$','TESTE') -Quarantine $True -StopRuleProcessing $False -Comments "Regra de bloqueio para palavras especificas contidas no Assunto ou Corpo da mensagem" -ExceptIfSentToMemberOf grupo-Exceto@empresa.com.br

- Outras regras com expressões regulares também podem ser utilizadas, abaixo alguns exemplos práticos:

  •\d\d\d\d\s\d\d\d\d\s\d\d\d\d\s\d\d\d\d (MasterCard Visa)

  •\d\d\d\d\s\d\d\d\d\d\d\s\d\d\d\d\d (American Express)

  •\d\d\d\d\d\d\d\d\d\d\d\d\d\d\d\d (any 16 digit number)

  •\d\d\d\-\d\d\-\d\d\d\d (Social Security Numbers)

- Bloqueio de mensagens em branco. Para bloquear mensagens com o assunto e corpo da mensagem em branco, na console do EOP - *Spam Filter* - *Default*. Selecionar a

opção *"On"* no ítem *"Mark as Spam"*. Ou ainda pode ser utilizado o cmdlet abaixo para ativar:

Set-HostedContentFilterPolicy -Identity 'Default' -MarkAsSpamEmptyMessages 'On'

- Mensagens com o campo *Sender* em branco já são bloqueadas por padrão.
- Bloqueio de mensagens que falharam no teste de SPF (*Hard Fail*). É recomendável ativar a configuração de *Hard Fail* para o SPF, aumentando a proteção contra o spoofing. Ou utilizar o cmdlet para ativar o recurso na *list Default*:

  Set-HostedContentFilterPolicy -Identity 'Default' -TestModeAction 'AddXHeader' -MarkAsSpamSpfRecordHardFail 'Off

- Bloqueio de mensagens com tamanho superior a 15MB. Para inspecionar e bloquear mensagens com base no anexo foi criada a regra para restringir o tamanho a 15MB e notificar o Destinatário:

  New-TransportRule -MessageSizeOver '15 MB (15,728,640 bytes)' -GenerateNotification 'De Acordo com a politica, o remetente **%%From%%** enviou uma mensagem que ultrapassou o tamanho maximo permitido de 15MB.' **-Name 'size exceeds:** "15.00 MB"' **-StopRuleProcessing:$true -Mode 'Enforce' -Comments** 'Bloqueio de mensagens com anexo superiores a 15MB.' **-Quarantine $true**

- Ou ainda o modelo abaixo onde o cmdlet rejeita a mensagem e notifica o remente:

  New-TransportRule -Name "Bloqueio de anexo 15MB" **-MessageSizeOver** '15 MB (15,728,640 bytes)' **-RejectMessageReasonText** 'A mensagem excedeu o tamanho maximo de 15MB' **-StopRuleProcessing:$true -Mode 'Enforce' -Comments** 'Bloqueio de mensagens com anexo superiores a 15MB.'

i. Quarentena

- A quarentena pode ser acessada pela console do EOP em *"**Protection - Quarantine**"*;
- A quarentena também pode ser acessada via PowerShell:

  Get-QuarantineMessage | ? {$_.Senderaddress -like "*@integracao.gov.br"}

- As mensagens também podem ser liberadas com o cmdlet abaixo:

Get-QuarantineMessage -MessageID "<5c695d7e-6642-4681-a4b0-9e7a86613cb7@exemplo.com.br>" | Release-QuarantineMessage -User julia@integracao.gov.br

j. *Reporting*

- O EOP oferece relatórios completos do ambiente, incluindo estatísticas e gráficos avançados. Para acessar a área de *Reports* abra o *Exchange Admin Center* e localize no painel esquerdo o item "***Reports***":
- A auditoria de *mailboxes* é desabilitada por padrão no *Office* 365, é possível ativa-la para os *Owners, Delegates* e *Admins*.
- Quando habilita o log de auditoria de caixa de correio para uma caixa de correio, o acesso à caixa de correio e algumas ações executadas por administradores e representantes são registrados no log por padrão. Para registrar em log as ações tomadas pelo proprietário da caixa de correio, precisa especificar quais ações do proprietário devem ser auditadas.
- Depois de habilitar o log de auditoria de caixa de correio, é possível pesquisar o log de auditoria do *Office* 365 para verificar atividades relacionadas à caixa de correio.
- Entradas no log de auditoria de caixa de correio são mantidas por 90 dias. É possível alterar a quantidade de tempo que as entradas são mantidas.
- Deve-se usar o *PowerShell Remoto* conectado à organização do *Exchange Online* para habilitar o log de auditoria de caixa de correio. Não pode usar o Centro de Administração do *Exchange* (EAC) para isso.
- Um administrador que recebeu a permissão de Acesso Completo à caixa de correio de um usuário é considerado um usuário representante.

k. *Procedimentos para habilitar a auditoria:*

- Para ativar a auditoria é necessário se conectar ao *Exchange Online*:

$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
Import-PSSession $Session

- Para efetivamente habilitar a auditoria para um único usuário:

  Set-Mailbox -Identity "Jose Silva" -AuditEnabled $true

- Para ativar a auditoria para todos os usuários:

  Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -AuditEnabled $true

- Para ativar a auditoria do *Owner* da *mailbox*, com os itens de *"MailboxLogin"* e *"HardDelete":*

  Set-Mailbox "Jose Silva" -AuditOwner MailboxLogin,HardDelete

l. Procedimento para a configuração do redireciomento do OWA no IIS (antes verificar sobre o split DNS):

- Configurando redirecionamento para /owa no IIS
  - Com o web site selecionado, duplo clique em HTTP Redirect
  - Selecionar "Redirect requests to this destination"
  - Entrar com https://<fqdn>/owa
  - Marcar "Only redirect requests to content in this directory (not subdirectories)"
  - Selecionar "Found (302)" no drop box "Statuscode"
  - Aplicar a configuração
  - Para cada vdir dentro do web site, desativar o redirecionamento em "HTTP Redirect"
    - aspnet_client
    - Autodiscover
    - Ecp
    - EWS
    - Microsoft-Server-ActiveSync
    - OAB
    - Owa
    - PowerShell
    - PowerShell-Proxy
    - Rpc

- Exigindo conexão SSL
    - No web site, não exigir SSL
    - Para cada vdir do Exchange, exigir SSL
        - Autodiscover
        - Ecp
        - EWS
        - Microsoft-Server-ActiveSync
        - OAB
        - Owa
    - No vdir OWA, configurar redirecionamento para https
        - Selecionar o vdir owa
        - Duplo clique em error pages
        - Duplo clique em 403
        - Selecionar "Respond with a 302 redirect"
        - Entrar com https://<fqdn>/owa

- O filtro de *Spam* do EOP foi configurado do seu padrão: mover mensagens classificadas como *SPAM* para a pasta lixo eletrônico dos usuários, para passar a mover mensagens para a área de Quarentena do EOP. com base na configuração do *AntiSpam* do SERPRO.
- As opções/configurações abaixo foram habilitadas para tornar a filtragem de *SPAM* do EOP mais restritiva e com isto, diminuir a quantidade de *spoofed* e *phishing e-mails*. Estes recursos devem ser avaliados periodicamente pela equipe de TI do Ministério da Integração Nacional e habilitados ou desabilitados para tornar o filtro de *SPAM* mais ou menos restritivo, conforme necessário.
    - *Increase Spam Score*
        - Numeric IP address in URL
        - URL redirect to other port
        - URL to .biz or .info websites
    - *Mark as Spam*
        - Empty messages
        - JavaScript or VBScript in HTLM
        - Objects tags in HTLM

    - SPF record: hard fail
    - Conditional Sender ID filtering: hard fail
    - NDR backscatter
- É recomendada a implementação do ***Junk Email Reporting Add-in for Microsoft Outlook***, o qual permite que os usuários do *Exchange Online* e *Exchange Online Protection* reportem *SPAM* com facilidade para análise a *Microsoft*, com o objetivo de aumentar a efetividade do filtro de *SPAM* do EOP. Este *add-in* é compatível com o *Microsoft Outlook* 2013, o *Outlook* 2010 ou o *Outlook* 2007, sendo executados no *Windows* 7, 8 ou 10.
- Como parte do *fine-tuning* (ajuste fino) das configurações do EOP para aumentar ainda mais a proteção contra *spoofing* e *phishing*, recomenda-se a configuração da funcionalidade *DomainKeys Identified Mail* (DKIM) para os domínios SMTP que o Ministério da Integração Nacional tenha propriedade.