UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

E-MAIL AUTENTICADO E COM CRIPTOGRAFIA

ALEXANDRE PEREIRA MOLINA

ORIENTADOR: JOÃO GONDIM

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: JUL/2012

BRASÍLIA / DF: JUL/2012

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

EMAIL AUTENTICADO E COM CRIPTOGRAFIA

ALEXANDRE PEREIRA MOLINA

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 ESPECIALISTA.

APROVADA POR:

JOÃO GONDIM, Mestre, UnB
(ORIENTADOR)

LAERTE PEOTTA, Mestre, UnB
(EXAMINADOR INTERNO)

DINO MACEDO, Mestre, Banco do Brasil
(EXAMINADOR EXTERNO)

NOME DO MEMBRO DA BANCA, Título, Instituição
(SUPLENTE)

DATA: BRASÍLIA/DF, 20 DE JULHO DE 2012.

FICHA CATALOGRÁFICA

MOLINA, ALEXANDRE PEREIRA
E-mail Autenticado e com criptografia [Distrito Federal] 2012.
xii, 116p., 297 mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2012).

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

1. E-mail Autenticado
2. Postfix
3. SMTP
4. Criptografia
5. Entidades Governamentais

I. ENE/FT/UnB.
II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

MOLINA, A. P. (2012). E-mail autenticado e com criptografia. Monografia de Especialização, Publicação LabRedes.MFE.002/2012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, (116)p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Alexandre Pereira Molina
TÍTULO DA MONOGRAFIA: E-mail Autenticado e com Criptografia.
GRAU/ANO: Especialista/2012.

Alexandre Pereira Molina
QE 26 Conjunto E Casa 34, Guará II
CEP 71060-051 – Brasília – DF – Brasil

AGRADECIMENTOS

Aos meus familiares pelo costumeiro apoio e ânimo para realização de mais uma etapa acadêmica.
Ao meu orientador Prof. Msc. João Gondim por sua de orientação, dedicação, profissionalismo e suas observações relevantes para aprimoramento deste trabalho de especialização.
À Embrapa pelo apoio financeiro, total abertura para desenvolvimento e capacitação e oportunidade de estar participando deste curso lato sensu.
Aos coordenadores do Ministério da Agricultura Pecuária e Abastecimento pela liberação e compreensão do tempo gasto para se produzir este trabalho e acreditar na minha capacitação profissional.
Aos colegas de trabalho pelo incentivo e debates produtivos essenciais para melhor produção deste trabalho.

RESUMO

O trabalho descrito nesta monografia objetiva analisar mecanismos, métodos, práticas e outras soluções para acrescentar uma maior confiabilidade, segurança e robustez no serviço de mensageiria eletrônica no âmbito de entidades governamentais.

Logo, para se buscar tais características deverão ser aplicadas técnicas de criptografia, bem como a autenticação do protocolo de envio de e-mail, uma vez que este não trabalha desta forma por padrão.

Para isso, deverá haver um embasamento teórico nos preceitos de James F. Kurose, Andrew S. Tanenbaum, Kyle D. Dent e Wildson de Macedo Oliveira e algumas RFCs como 1939, 2045, 2049, 3501, 4422, 4648, 4954, 5321, 5322 e 5751 que norteiam os protocolos de e-mail, de modo a propiciar um ambiente de e-mail mais seguro em órgãos do governo.

PALAVRA-CHAVE

1. EMAIL AUTENTICADO; POSTFIX; SMTP
2. CRIPTOGRAFIA
3. ENTIDADES GOVERNAMENTAIS

ABSTRACT

The work described in this thesis aims to analyze the mechanisms, methods, practices and other solutions to add greater reliability, security and robustness in the electronic message service for the government entities.

Therefore, to get that features will be implemented encryption techniques and authentication of email sending protocol, since this does not work in this way by default.

For this, there should be a theoretical foundation in the precepts of James F. Kurose, Andrew S. Tanenbaum, Kyle D. Dent and Wildson de Macedo Oliveira and some RFCs like 1939, 2045, 2049, 3501, 4422, 4648, 4954, 5321, 5322 e 5751 that guide the e-mail protocols, so as to propitiate an e-mail environment safer in government's bodies.

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

GLOSSÁRIO

SGSI – Sistema de Gestão de Segurança da Informação

SMTP – *Simple Mail Transfer Protocol* (SMTP) é o protocolo padrão para envio de e-mails através da Internet.

LDAP – *Lightweight Directory Access Protocol* é um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP.

OpenLDAP - O OpenLDAP é um software livre de código aberto que implementa o protocolo LDAP.

SASL - "*Simple Authentication and Security Layer*" ou Camada de Simples Autenticação e Segurança.

Backbone - Designa o esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho. É uma espinha dorsal para a comunicação com a Internet.

No-break - Uma fonte de alimentação ininterrupta, também conhecida pelo acrônimo UPS (sigla em inglês de *Uninterruptible Power Supply*) é um sistema de alimentação elétrico que entra em ação, alimentando os dispositivos a ele ligados, quando há interrupção no fornecimento de energia.

Malware – O termo *malware* é proveniente do inglês *malicious software*; é um *software* destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não)

S/MIME – *Secure Multi-Purpose Internet Mail Extensions* (Extensões de Correio de Internet Multi-propósito Seguras): método seguro de enviar e-mail que usa o sistema de encriptação.

RSA - RSA é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT (fundadores da atual empresa RSA Data Security, Inc.), Ronald Rivest, Adi Shamir e Leonard Adleman, que inventaram este algoritmo;

SERPRO - O Serviço Federal de Processamento de Dados (Serpro) é a maior empresa pública de prestação de serviços em tecnologia da informação da América Latina.

MTA – *Mail Transfer Agent* (Agente de transporte de e-mail). O MTA é um *software* para transferir mensagens eletrônicas entre servidores de e-mail através do protocolo SMTP.

POSTFIX - O Postfix é um agente de transferência de e-mails (MTA), um software livre para envio de e-mails.

CGI.BR - Comitê Gestor da Internet no Brasil

CERT.BR - Entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil (CGI.br) desde dezembro de 2005.

Cyrus - Cyrus é um sistema de alta escalabilidade para correio eletrônico de empresas. Este software é responsável pela autenticação nos protocolos de recebimento de e-mail (POP3 e IMAP), bem como as operações de aquisição e manipulação de mensagens de e-mail.

IMAP - IMAP (*Internet Message Access Protocol*) é um protocolo de gerenciamento de correio eletrônico superior em recursos ao POP3.

DOVECOT - Dovecot é um servidor de IMAP e POP3 open source para sistemas Linux e UNIX, escrito primariamente com segurança em mente.

Integridade é propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

Autenticidade é a certeza absoluta de que a informação provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo.

Certificação Digital [ICP-Brasil]: É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.

AC- Raiz [ICP-Brasil]: A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete a AC raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. Como também, revogar e emitir seus próprios certificados.

AC - Autoridade Certificadora [ICP-Brasil]: Uma Autoridade Certificadora é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. De usuários e cadeias de certificação subsequentes Desempenha como função essencial, a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (público-privada).

Assinatura Digital [CECD]: A assinatura digital é uma modalidade de assinatura eletrônica resultado de uma operação matemática que utiliza criptografia e permite aferir, com segurança, a origem e a integridade do documento.

TLS - *Transport Layer Security* - TLS (em português: Segurança da Camada de Transporte) e o seu predecessor, *Secure Sockets Layer* - SSL (em português: Protocolo de Camada de *Sockets* Segura), são protocolos criptográficos que conferem segurança de comunicação na Internet para serviços como e-mail (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados.

SPF - *Sender Policy* Framework ou SPF é um sistema que evita que outros domínios (endereço da internet) enviem e-mails não autorizados em nome de um domínio.

PAM - *Pluggable Authentication Modules* é uma suíte de bibliotecas distribuídas que viabilizam ao administrador do sistema especificar a forma que as aplicações autenticam os seus usuários. Basicamente, é um mecanismo bastante flexível para autenticação de usuários.

Auditoria - Define as atividades para determinar adequação aos requisitos, planos e ao SGSI.

Ação corretiva - Ação para eliminar a causa de uma não conformidade identificada ou outra situação indesejada.

Ação preventiva - Ação para eliminar a causa de uma potencial não conformidade ou outra situação potencialmente indesejável.

PDCA – *Plan, Do, Check and Act* - TLS (em português: Planejar, Executar, Verificar, Agir Corretivamente). É uma ferramenta de gerência de projeto muito utilizada e conhecida internacionalmente. Com a aplicação desse conceito, gerentes podem garantir se metas e objetivos poderão ser alcançados.

1. INTRODUÇÃO

O servidor de e-mails é largamente utilizado em entidades governamentais para troca de informações, contudo medidas para assegurar a segurança da informação devem ser consideradas neste contexto. Esta monografia vem propor um ambiente que oferte um nível de segurança aceitável no que diz respeito à segurança da informação, assim acarretando um provimento do serviço de e-mail com valor agregado.

O tema proposto por esta monografia abordará uma estrutura de correio eletrônico utilizando, como servidor, o Postfix. O ambiente do projeto sumulará uma empresa governamental como a de um ministério do poder executivo.

Entidades governamentais ministeriais são peças importantes na configuração do país como gerenciador, normatizador e fiscal sendo o e-mail uma das principais ferramentas utilizadas para troca de informações. Sem ele, questões evolutivas e econômicas do Brasil podem ser perdidas ou retardadas. Pode-se acrescentar também que mensagens eletrônicas trafegadas no ambiente corporativo servem como instrumento de prova de um produto (e-mail gerado por um sistema aprovando uma fiscalização de um produto) ou como prova de solicitação ou realização de uma demanda.

Alguns problemas relacionados à segurança da informação causam grandes impactos caso ocorram em organizações governamentais. Dentre eles cita-se a falta de um método de autenticação do protocolo SMTP. Além disso, a ausência de certificado digital reconhecido por uma autoridade certificadora confiável para o webmail proporciona uma vulnerabilidade no escopo da integridade e do não repúdio dos dados. Outro empecilho no ambiente de correio eletrônico é a não disponibilização de criptografia nos protocolos de recepção de e-mail (POP3, IMAP) e nem no de envio (SMTP).

Assim para se realizar todas essas soluções serão necessários agregar conceitos e informações sobre e-mails que serão encontradas em obras de James F. Kurose, Andrew S. Tanenbaum, Kyle D. Dent e Wildson de Macedo Oliveira e algumas RFCs como 1939, 2045, 2049, 3501, 4422, 4648, 4954, 5321, 5322 e 5751.

1.1. OBJETIVOS

Objetivo Geral

- Analisar os mecanismos de criptografia e autenticação, embasados nos preceitos de James F. Kurose, Andrew S. Tanenbaum, Kyle D. Dent e Wildson de Macedo Oliveira e os seguintes documentos especificadores de protocolos como as RFCs 1939, 2045, 2049, 3501, 4422, 4648, 4954, 5321, 5322 e 5751, de modo a propiciar um ambiente de e-mail mais seguro em entidades governamentais.

Objetivos Específicos

- Implementar mecanismo de autenticação nos protocolos e-mail.
- Utilizar certificados digitais válidos em webmails em entidades governamentais.
- Aplicar criptografia nos protocolos de e-mails.
- Controlar acessos nos protocolos de e-mail por meio de configurações otimizadas requisitadas por normas e boas práticas.
- Utilizar referências normativas (ISO 27001, ISO 27002, ISO 27003, ISO 27005) para identificação, análise, avaliação e propor tratamentos aos riscos inerentes ao ambiente de mensageiria eletrônica.

1.2. JUSTIFICATIVA

A pesquisa almeja discutir a respeito dos problemas encontrados com provimento de mensageiria eletrônica de maneira insegura e sem confiabilidade. Assim maneiras, métodos e práticas serão discorridos objetivando mitigar, em entidades governamentais, despesas exorbitantes relativas à parada do serviço de mensageiria eletrônica devido aos ataques que possam ocorrer em servidores de e-mail suscetíveis.

O e-mail é uma ferramenta crucial para troca de informações, pois independe da distância das partes integrantes de uma comunicação. Logo, para aprimoramento no processo do serviço prestado para a sociedade, que é uma característica inerente de uma entidade governamental, a continuidade do funcionamento do e-mail é de suma importância, uma vez

que estas informações trocadas são relevantes para melhorar o atendimento dos anseios desta comunidade.

Portanto, uma vez aplicado corretamente mecanismos de autenticação e criptografia nos protocolos POP3, IMAP e SMTP associado com uma política de treinamento e educação dos usuários deste serviço pode-se haver uma maior confiabilidade dele. Como consequência disso, os critérios de segurança da informação (confidencialidade, integridade e disponibilidade) pode ter uma crescente na probabilidade de ser alcançado.

1.3. METODOLOGIA

A pesquisa abordará sobre os principais protocolos envolvidos na estrutura de e-mail que são o POP3, IMAP, SMTP e MIME. Além disso, *frameworks* como SASL e PAM serão discutidos e aplicados ao longo do trabalho. Assim, para poder validar as pesquisas efetuadas nesta monografia, duas infraestruturas de e-mail serão constituídas com a finalidade de verificar as vulnerabilidades dos ambientes.

Um primeiro cenário de serviço de mensageiria eletrônica deverá ser montado sem aplicar mecanismos de segurança fator este que pode ocorrer também em entidades governamentais. Implementações técnicas de cifragem de dados, autenticação e ajustes restritivos do protocolo SMTP não estarão contempladas neste contexto. Logo, a estrutura exibida conterá praticamente uma instalação padrão consoante alguns administradores de rede o fazem.

E um segundo ambiente serão aplicados os mecanismos de criptografia, autenticação do SMTP e algumas configurações sugeridas nas RFC 1939 (POP3), RFC 2045 a 2049 (MIME), RFC 3501 (IMAP), RFC 4422 (SASL), RFC 4648 (*Data Encodings*), RFC 4954 (SMTP *Service Extension for Authentication*), RFC 5321 (SMTP), RFC 5322 (Formato de mensagens de e-mail) e RFC 5751 (S/MIME). O objetivo deste cenário é propor aumento na segurança e confiabilidade do serviço de mensageiria.

Como resultado disso, serão demonstrados alguns ataques que visam explorar vulnerabilidades no âmbito de servidores de e-mail nos dois cenários e deverá ser comparado os seus resultados com relação ao sucesso do atacante e demais informações relevantes.

1.4. ESCOPO

O escopo selecionado, dentro das universalidades de assuntos encontrados em entidades governamentais, é a utilização do envio de e-mails para comunicação da informação em suas dependências. Esse assunto diz respeito às informações trafegadas nestes órgãos os quais usam os protocolos de recepção e envio de e-mails para realizar essa tarefa. No contexto deste projeto, o *software* abordado como servidor de correio eletrônico para tramitações de mensagens será o POSTFIX e DOVECOT.

A metodologia aplicada para abordar o escopo selecionado usará, primeiramente, as normas ISO 27001, 27002, 27003 e 27005 para um estabelecimento de procedimentos e melhores práticas, execução da identificação e análise de riscos acerca do serviço de mensagem eletrônica. Posteriormente, uma proposta de tratamento ocorrerá objetivando erradicar ou mitigar os riscos encontrados no órgão.

1.5. DESCRIÇÃO DO DOCUMENTO

Esta seção visa descrever sucintamente o conteúdo desenvolvido em cada capítulo desta monografia. Seguem eles:

Capítulo 4 – Referencial conceitual: Realiza uma introdução sobre a estrutura das organizações governamentais e a importância da aplicação de uma política de segurança e um SGSI nos moldes da ISO 27001, ISO 27002, ISO 27003 e ISO 27005.

Capítulo 5 – Correio eletrônico: Aborda a respeito dos protocolos envolvidos na recepção e envio de e-mails, bem como os documentos orientadores que definem o formato de mensagens de e-mail, mensagens com conteúdo diferente do US-ASCII e outras bases de codificações usadas no âmbito de e-mail. A estrutura e a configuração padrão do Postfix também é contemplada assim como alguns problemas provenientes do serviço de e-mail.

Capítulo 6 – Política de segurança a luz da ISO 27002:2005: Contextualiza a ideologia e controles encontrados na ISO 27001, ISO 27002, ISO 27003 e ISO 27005 no ambiente de

uma entidade governamental. Envolve aspectos de acesso lógico, acesso físico, política de uso do e-mail, monitoramento, política de criação, bloqueio e desativação de e-mail e demais itens.

Capítulo 7 – Identificação dos riscos: Identifica os riscos, com auxílio da ISO 27001, ISO 27002, ISO 27003 e ISO 27005, aos quais organizações governamentais estão propensas e comenta sobre os danos que estes podem causar.

Capítulo 8 – Análise e avaliação dos riscos: Analisa e avalia os riscos encontrados, calcados na ISO 27001, ISO 27002, ISO 27003 e ISO 27005, e determina o nível do risco por meio do produto das variáveis probabilidade, severidade e relevância. Desta forma, é possível selecionar o que está crítico e deverá ser sanado bem como os riscos que poderão ser aceito pela organização.

Capítulo 9 – Tratamento dos riscos: Propõe erradicar ou mitigar riscos identificados na seção anterior os quais foram assinalados para receber tratamento. É explanado neste capítulo metodologias que almejam tornar o ambiente de e-mail mais confiável e seguro.

Capítulo 10 – Experimento: Exibe um contexto prático de mensageiria eletrônica. Ilustra um servidor de e-mail com técnicas e metodologias aplicadas que buscam conferir mais segurança ao serviço de e-mail e outro com configurações padrões as quais podem ser encontradas em entidades governamentais.

2. FUNDAMENTOS E CONCEITOS

Esta seção visa apresentar a base empírica utilizada no escopo delimitado visando compreender suas peculiaridades e requisitos. Logo, a análise de itens como estrutura, estratégia, volume de informações e demais são cruciais para atingimento dos objetivos traçados.

2.1. NORMAS REFERENCIADAS

As seguintes normas foram usadas para desenvolver esta seção:

- ABNT NBR ISO/IEC 27001:2006 – Norma brasileira que contém os requisitos embasados em técnicas de segurança para implementar um SGSI
- ABNT NBR ISO/IEC 27002:2005 – Norma brasileira que especifica o código de prática para a gestão da segurança da informação
- ISO/IEC 27003:2010 – Padrão internacional que normatiza técnicas de segurança e serve como um guia de implementação de um SGSI
- ABNT NBR ISO/IEC 27005:2008 – Norma brasileira que contempla técnicas de segurança atuando na área de gestão de riscos de segurança de informação

2.2. ENTIDADES GOVERNAMENTAIS E O PROCESSO DE NEGÓCIO

Antes de se fazer qualquer consideração a respeito do serviço de mensageiria eletrônica sobre as organizações governamentais, é plausível, primeiramente, compreender a estrutura governamental, bem como os fatores críticos de sucesso para atingir um índice minimamente satisfatório nas implantações de segurança.

2.2.1. Obtendo apoio da alta gerência

Entidades ministeriais são órgãos federais do poder executivo. Como ocupantes desta posição estratégica do governo brasileiro, eles recebem várias incumbências da presidência da república.

Observando décadas passadas, o Brasil era conhecido apenas como um cultivador de produtos agrícolas. Porém, devido ao dinamismo do comércio mundial, à tecnologia crescente nas organizações e à maturação dos processos, pode-se dizer que com o uso de políticas e padrões tem-se agregado valor à produção nacional.

Cada Ministério da administração pública federal estabelece políticas, diretrizes e prioridades na aplicação dos recursos públicos para os setores que representam. Portanto, as atividades de uma equipe de gestão estratégica exercem um papel fundamental para estabelecer os objetivos e metas para atendimento da missão da entidade governamental.

Assim, cada tarefa ocorrida dentro destas empresas demanda valores advindos de cofres públicos, portanto, cada recurso deve ser utilizado com bastante cautela.

No entanto, para que as missões, objetivos e metas sejam cumpridos, é de suma importância que os órgãos federais contenham toda a infraestrutura necessária para o tráfego seguro das informações correlatas aos seus anseios. A existência de um canal confiável, seguro e eficaz para a circulação das informações vêm se consolidando cada vez mais uma realidade.

2.2.2. Importância no cenário brasileiro

O custo da informação pode ter valor inestimável para uma organização, por exemplo, a produção oriunda do agronegócio, segundo [50] o qual se calcou nas bases do CEPEA-USP / CNA, MAPA e IPEA, respondeu por 24% a 30% do Produto Interno Bruto (PIB), de 38% a 43% das exportações e de 36% a 40% dos empregos gerados no País. Estes dados tiveram como ano base o de 2009.

Logo, pode-se inferir que a informação envolvida nessas organizações e modo como estas são realizadas são importantes se tentar ampliar a prosperidade da nação.

2.2.3. Chefia e hierarquias

Em ministérios do poder executivo, o responsável maior são os ministros. A ocupação e posse deste cargo é incumbência do presidente da república. Assim, os objetivos estabelecidos pelos ministros devem estar de acordo com os anseios da presidência da república.

Suas atividades são inúmeras e todas elas estão voltadas para estabelecer as diretrizes políticas da organização. Portanto, novas melhorias que venham a ser realizados dentro das dependências, sejam elas de quaisquer departamentos e que utilizem ou não de tecnologia, e que onerem gastos governamentais são submetidas à autorização do ministro.

Especificamente no assunto tratado, correio eletrônico com SMTP autenticado e com criptografia, a implantação de uma política de segurança se torna uma necessidade, uma vez que este serviço é de suma importância para desenvolvimento e sustentabilidade dos objetivos estratégicos do órgão em questão. Portanto, para aprovação da política de segurança, deve-se percorrer a estrutura hierárquica da empresa para obtenção da autorização do ministro. Logo, este projeto necessita ser primeiramente apresentado para o chefe da coordenação de informática que encaminhará o documento, se aceito, para a secretaria executiva que por fim submeterá ao ministro.

2.2.4. Aprovação da política de segurança

No serviço de e-mail, devemos implantar uma política de segurança de modo a garantir que não haja acesso indevido, que as informações sejam protegidas e que os riscos referentes aos processos sejam mitigados.

Entidades governamentais são peças importantes na configuração do país como gerenciador, normatizador e fiscal de políticas no território brasileiro. O e-mail é a principal ferramenta utilizada para troca de informações. Sem ele, questões evolutivas e econômicas da organização poderiam ser perdidas ou retardadas.

Outro aspecto que alimenta o apoio da alta gerência é o fato destas entidades possuírem um tráfego de envio de e-mails superior a 10 mil mensagens diárias. Além disso, os órgãos possuem em média mais de 7 mil contas de e-mails, uma quantidade aproximada de 5 mil usuários na sua rede e um volume de dados de e-mail aproximado a 5 MB por e-mail. O volume de aproximadamente 50 GB pode ser encontrado através de um calculo rápido. Isso

tudo caracteriza que muitas informações cruciais ao processo de negócio são interagidas entre seus usuários internos e externos, o que melhora a qualidade do serviço ofertada pela entidade e agiliza a escalabilidade da produção.

A conformidade com as diversas boas práticas em segurança da informação, encontradas em normatizações brasileiras e internacionais, pode ser maximizada na empresa com a adoção do plano de SGSI. Assim, riscos associados a problemas de segurança aos dados, vazamento de informações e vulnerabilidade de ativos podem ser reduzidos.

Outro ponto é que os produtos fiscalizados pelas entidades governamentais exibirão um diferencial no mercado, pois obterão certificados e estarão em conformidade com os padrões internacionais o que resulta em maior valor de mercado.

Qualquer tipo de problema que venha a prejudicar o serviço de e-mail é devastador para o processo do negócio das entidades governamentais. As despesas relativas à parada do serviço do e-mail chegam à casa dos milhões. Dentro da empresa, o e-mail é considerado como mecanismo de prova ou certificação de um produto ou demanda. Sendo assim, pode-se imaginar uma situação onde todas filiais federais esperando um e-mail gerado pelo sistema para liberar um produto ou uma demanda crítica. As despesas de espera são exorbitantes. Aliado a isso, qualquer tipo de retardo, afeta todas as transações da filial, pois negócios que poderiam estar ocorrendo estarão sendo perdidos naquele exato momento. Como consequência disso, é gerada uma situação insustentável em sua gerência e na continuidade do negócio.

Visto isso, devem-se minimizar ao máximo os problemas provenientes de serviço de e-mail. Com a implantação de uma política de segurança, o valor pago para sua implementação terá sido revertido em lucro com o passar do tempo porque reduzirá bastante a ocorrência dos problemas no que tange a segurança da informação.

A organização da empresa referente à sua estrutura, bem como as suas atividades e processos são vantagem ganhas com a política de segurança proposta. Com isso, o setor responsável pelo envio de e-mails estará mais preparado caso ocorram falhas de processos ou quando ocorra um problema inédito.

2.2.5. Cases de sucesso

A Tabela 2.1 demonstra as instituições brasileiras certificadas ISO 27001.

Tabela 2.1: Empresas brasileiras certificadas ISO 27001:2005

Nome da Organização	País	Número do Certificado	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
Atos Origin Brasil Ltda	Brasil	IS 98429	ISO/IEC 27001:2005
Axur Information Security	Brasil	IS 509742	ISO/IEC 27001:2005
BT	Brasil	LRQ 4003984	ISO/IEC 27001:2005
Cardif do Brasil Vida e Previdencia S/A	Brasil	IS 521855	ISO/IEC 27001:2005
CIP Camara Interbancaria de Pagamentos	Brasil	IS 96934	ISO/IEC 27001:2005
Fucapi-Fundacao	Brasil	IS 504391	ISO/IEC 27001:2005
IBM ITD Brasil	Brasil	62.691	ISO/IEC 27001:2005
Módulo Security Solutions S/A	Brasil	IS 510466	ISO/IEC 27001:2005
Poliedro - Informática, Consultoria e Serviços Ltda.	Brasil	44121081309	ISO/IEC 27001:2005
Prodesp	Brasil	IS 512881	ISO/IEC 27001:2005
Promon Engenharia Ltda.	Brasil	IS 500248	ISO/IEC 27001:2005
Promon Tecnologia Ltda	Brasil	IS 500564	ISO/IEC 27001:2005
Samarco Mineração S/A.	Brasil	IS 524157	ISO/IEC 27001:2005
SERASA S.A.	Brasil	262326 ISMS	ISO/IEC 27001:2005
Serviço Federal de Processamento de Dados - SERPRO	Brasil	IS 515421	ISO/IEC 27001:2005
Superior Tribunal de Justiça	Brasil	IS 538457	ISO/IEC 27001:2005
Telefonica Empresas S/A	Brasil	IS 501039	ISO/IEC 27001:2005
Tivit Tecnologia da Informacao S.A.	Brasil	00017-2006-AIS-OSL-NA	ISO/IEC 27001:2005
TIVIT TERCEIRIZAÇÃO DE TECNOLOGIA E SERVIÇOS S.A.	Brasil	16203-2007-AIS-BRA-NA	ISO/IEC 27001:2005
T-Systems Brasil	Brasil	336227 ISMS	ISO/IEC 27001:2005
T-Systems do Brasil Ltda.	Brasil	341898 ISMS	ISO/IEC 27001:2005
UNISYS Global Outsourcing	Brasil	IS 97102	ISO/IEC 27001:2005
Zamprogna S/A Importacao	Brasil	IS 518855	ISO/IEC 27001:2005

Segundo [24], segue as companhias brasileiras que possuem a certificação ISO 27001

Infere-se dentro das organizações apresentadas na Tabela 2.1, o SERPRO utiliza de boas práticas de segurança da informação. E como a rede diversos órgãos governamentais estão inseridos em seu *backbone*, seria bastante interessante eles seguirem a referência deste órgão. Realização de análise de requisitos de segurança da informação.

3. CORREIO ELETRÔNICO

A existência do serviço de mensageiria eletrônica é uma realidade desde os primórdios da internet. Este é, inclusive, bem mais antigo que o protocolo HTTP. Inicialmente, ela era utilizada experimentalmente por estudantes de meios acadêmicos para troca de mensagens internas.

À medida que usuários foram ganhando mais experiência com a utilização de correio eletrônico, a normatização e padronização deste protocolo se fez necessário por meio de RFCs. Então, duas propostas mais elaboradas de RFCs relativo a correio eletrônico da ARPANET foram publicadas em 1982 e eram conhecidas como a RFC 821 (protocolo de transmissão, ou seja, o SMTP) e a RFC 822 (formato de mensagens). Revisões menores ocorreram nessas RFCs e suas atualizações foram publicadas nas RFCs 2821 e 2822 tornando-se assim os padrões da internet para mensageiria eletrônica. Hodiernamente, as RFCs 2821 e 2822 foram revisadas e atualizadas para RFC 5321 e 5322 respectivamente.

3.1. NORMAS REFERENCIADAS

As normas citadas abaixo foram usadas para desenvolver esta seção:

- RFC 1939 (POP3) – Detalha o funcionamento do protocolo de recepção e-mails usado para baixar mensagens de um servidor de caixa postal por um cliente de e-mail.
- RFC 2045 e 2049 (MIME) – Trata a respeito do protocolo desenvolvido para tramitar arquivos codificados em bases diferente do US ASCII de 7 bits.
- RFC 3501 (IMAP) – Aborda sobre o protocolo de acesso das mensagens de e-mails entre um cliente de e-mail ou webmail a um servidor de e-mail.
- RFC 4648 (*Data Encodings*) – Contém informações relativas aos possíveis modos de codificar dados.
- RFC 4954 (SMTP *Service Extension for Authentication*) Documento que descreve as extensões, como autenticação, sobre o SMTP original.
- RFC 5321 (SMTP) – Retrata o protocolo de envio de e-mails ocorrido entre MTAS

- RFC 5322 (Formato de mensagens de e-mail) – Contém as informações acerca do formato padrão das mensagens de e-mail
- RFC 5751 (S/MIME) – Diz respeito ao MIME incluindo o arcabouço de criptografia

3.2. TIPOS DE AGENTES DE E-MAIL

A configuração do cenário de mensageiria eletrônica é composta por três diferentes tipos de agentes. Cada um deles tem um objetivo específico no serviço de e-mail.

O MTA, cujo significado é *Mail Transport Agent*, é responsável pela transferência de e-mails entre os servidores de e-mail. O protocolo utilizado por este agente é o SMTP e o SMTPS se o arcabouço de criptografia for utilizado.

O MDA, *Mail Delivery Agent*, é o agente incumbido em fazer o despejo da mensagem recebida por um MTA ser adicionada na estrutura de armazenamento de e-mail.

Os MDAs podem ter a funcionalidade de fazer direcionamento de um endereço para outro e também categorizar e filtrar uma mensagem de e-mail.

O MUA, *Mail User Agent*, tem a finalidade acessar o servidor de caixas postais e fazer o *download*/acesso das mensagens residentes neste. Através do *software* cliente de e-mail, o usuário é capaz de compor, enviar, encaminhar e responder e-mails. Este agente, para fazer ao se conectar com o servidor, utiliza os protocolos POP3 e IMAP ou POP3S e IMAPS caso a criptografia esteja habilitada.

3.3. MODOS DE ARMAZENAMENTO DE MENSAGENS DE CORREIO ELETRÔNICO

Os *softwares* de correio eletrônico admitem dois possíveis modos para armazenamento de e-mail que são o mailbox e o maildir. O mailbox era a arquitetura mais utilizada em tempos passados. A facilidade de fazer backup e manuseio do arquivo de e-mail são os principais argumentos de ainda se utilizá-lo. Entretanto, como esta alternativa arquiva todas as mensagens de e-mail em um único arquivo, usuários que armazenam centenas de e-mails na sua caixa postal correm um grande risco de ter o arquivo de armazenamento corrompido.

Outra problemática causada deste modo está relacionada à capacidade de escrita do sistema de arquivo para um único arquivo. É sabido que cada sistema de arquivo contém uma limitação máxima no tamanho de um único arquivo. Sendo assim, caso um arquivo de e-mail se apresentar muito grande existe risco do sistema de arquivo parar de escrever o arquivo do e-mail. Por essas razões administradores do serviço de e-mail adotam o modo Maildir.

O modo Maildir surgiu junto com o MTA Qmail. Este servidor de e-mail apresentou robustez e segurança, porém apresenta-se, atualmente, em descontinuidade. Relativo à estrutura Maildir, os arquivos de e-mails são organizados em estruturas de diretórios, onde cada mensagem de e-mail é um arquivo residido dentro destas estruturas.

3.4. ENVIO DE E-MAILS

O SMTP, protocolo responsável por fazer a emissão, exibe atualmente uma grande flexibilidade e qualidades interessantes, entretanto ele ainda contém algumas características arcaicas. Um exemplo disso é a restrição de uma correspondência eletrônica que admite apenas um formato ASCII de 7 bits que será explorada com mais detalhes em seções posteriores. Essa limitação era entendível em décadas passadas, pois o uso do correio eletrônico não tinha popularidade e a capacidade de transmissão era escassa. Além disso, a pequena largura de banda atrelada com essa escassez do canal comunicativo trouxe como única alternativa a tramitação de mensagens de texto simples.

Diferentemente do tempo hodierno, o sistema de e-mail possibilita envio de arquivos anexados, imagens e vídeos no corpo do texto e demais funcionalidades agregadas. Porém, sempre há a necessidade de codificar os dados binários de multimídia em ASCII antes do envio e decodificá-lo após o transporte SMTP.

O protocolo SMTP, que é definido na RFC 5321, é destinado a realizar a transferência de e-mails entre servidores de e-mails e também entre cliente de e-mail e um servidor de e-mail. A Figura 3.1 exibe uma comunicação típica de um envio de e-mail usando o referido protocolo.

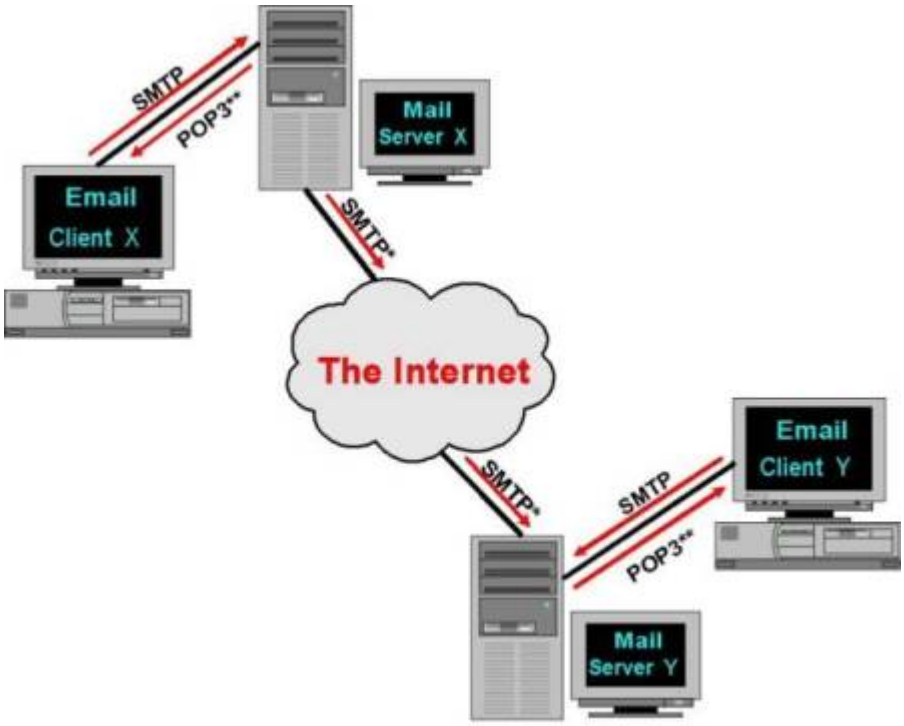

Figura 3.1: Fluxo de e-mails entre clientes de e-mail
[46]

Acima se pode analisar o fluxo de uma troca de mensagens entre pessoas. Primeiramente, o cliente de e-mail X instalado na máquina do usuário remetente estabelece uma comunicação com o servidor de e-mail. O número da porta usada pelo cliente é um valor alto, enquanto a porta utilizada pelo servidor é a 25, caso este não aplique criptografia.

Uma tramitação qualquer de e-mail pode ser acompanhada utilizando o programa chamado telnet. Por meio dele, o entendimento do protocolo SMTP e seus comandos se tornam mais prático e didático para aprendizagem do protocolo em questão. Sendo assim, para enviar um e-mail via telnet é exposto detalhadamente na Tabela 3.1.

Tabela 3.1: Comunicação SMTP via *telnet* entre cliente e servidor

Comunicação SMTP
1. Cliente: telnet servidor.dominio.br 25
2. Servidor: 220 servidor.dominio.br SMTP Postfix
3. Cliente: HELO cliente.dominio.br
4. Servidor: 250 Hello cliente.dominio.br, pleased to meet you
5. Cliente: MAIL FROM: <joao@dominio.br>

6. Servidor: 250 Sender OK
7. Cliente: RCPT TO: <mario@dominio.br>
8. Servidor: 250 Recipient OK
9. Cliente: DATA
10. Servidor: 354 End Data with <CR><LF>.<CR><LF>
11. Cliente: To: Mario mario@dominio.br From: João joao@dominio.br Subject: Email SMTP Olá Mário, Viu como funciona o protocolo SMTP? Até mais. .
12. Servidor: 250 Message accepted for delivery
13. Cliente: QUIT
14. Servidor: 221 servidor.dominio.br closing the connection

Informação adaptada de [1] e [2]

A primeira linha do fluxo realiza a conexão com o servidor SMTP em sua porta TCP 25. Depois de estabelecida a conexão, o servidor exibe uma saudação ao cliente por meio de um *banner* previamente configurado. Visto isso, o cliente faz sua apresentação ao servidor por meio do comando HELO, o qual é uma abreviação da palavra *hello*. Esse comando é importante de ser informado porque um servidor ao aceitar conexões de e-mail nem sempre está disponível para se comunicar com algum cliente. O cliente, uma vez recebendo o aceite de sua saudação, começa a enviar os comandos importantes para constituição do envelope e a mensagem de e-mail, onde os comandos MAIL FROM, RCPT TO são responsáveis pelo envelope e o DATA incumbido de construir o cabeçalho e o corpo de uma mensagem de e-mail.

O MAIL FROM especifica o endereço do remetente da mensagem, enquanto o RCPT TO informa o e-mail do destinatário. No contexto DATA, o usuário redige o cabeçalho da mensagem, e separado por uma linha em branco, escreve o corpo do texto que é a carga útil da mensagem eletrônica. Após finalizar a composição da mensagem, o servidor de e-mail aceita a mensagem. Por sua vez, o cliente finaliza a comunicação com o MTA por meio do

comando QUIT. Para fazer a entrega, o MTA verifica se fará a entrega em seu domínio local ou se deverá se conectar ao servidor SMTP do destinatário para entregar a correspondência.

3.4.1. Formato de mensagens

O formato da mensagem eletrônica diz respeito ao modo como é estruturado o cabeçalho e o corpo de texto de um e-mail. A regulamentação da estrutura das correspondências de correio eletrônico necessitava ser padronizada cada vez mais à medida que este sistema crescia. Através da publicação da RFC 822, a composição do conteúdo dos e-mails, ou seja, seu cabeçalho e corpo passaram a respeitar uma hierarquia predeterminada. Vale ressaltar que todo conteúdo de uma correspondência eletrônica é codificada em 7 do formato ASCII .

Nessa referida RFC, é especificado que a delimitação entre o cabeçalho e o corpo de uma mensagem eletrônica deverá ocorrer através de uma linha em branco. Outras observações a respeito do cabeçalho também são encontradas neste documento. É visto que cada linha do cabeçalho deverá conter uma palavra-chave seguida do sinal de dois pontos que, por fim, receberá um valor ainda na mesma linha. A Tabela 3.2 abaixo explicita os campos mais comuns encontrados nos cabeçalhos dos e-mails e que são referenciados na RFC 5322 (versão revisada da antiga 822).

Tabela 3.2: Cabeçalhos mais importantes da RFC 5322

Cabeçalho	Significado
To:	Endereço(s) de e-mail do(s) destinatário(s) principal(is)
Cc:	Endereço(s) de e-mail do(s) destinatário(s) secundário(s)
Bcc	Endereço(s) de e-mail do destinatário(s) que deverá(ão) ser ocultado(s)
From:	Endereço(s) de e-mail do(s) autor(es) da mensagem
Sender:	Endereço de e-mail do remetente da mensagem
Received:	A linha incluída por cada MTA ao longo da rota do e-mail
Return-Path:	Informar como voltar ao remetente. Geralmente recebe o valor do endereço do remetente
Date:	Data e hora de envio do e-mail

Reply-To:	Endereço de e-mail que receberá as respostas dos destinatários
Message-Id:	Número exclusivo identificador de uma mensagem de e-mail
In-Reply-To:	*Id* da mensagem original precedido de uma numeração de resposta
References:	Outras *Ids* de mensagens relevantes
Keyword:	Palavra-chave do e-mail
Subject:	Informa o assunto tratado ao longo do e-mail

Cabeçalhos de e-mail adaptados de [2]

Depois de fornecido o cabeçalho e respeitando a delimitação entre este e o corpo de e-mail citado em momentos anteriores, o usuário dispõe de liberdade para redigir o corpo do e-mail conforme desejar. Porém, usuários geralmente começam o corpo do e-mail usando um vocativo e terminam a mensagem com uma assinatura, *slogan* ou citações de autores e etc.

3.4.2. Multipurpose Internet Mail Extensions

A RFC 5322 se encarregou em delinear completamente a estrutura do cabeçalho de uma correspondência eletrônica, porém deixou a cargo do usuário o modo de compor o corpo de um e-mail. O problema encontrado foi que, com explosão do uso do sistema de mensageiria eletrônica, os usuários precisavam trocar dados que não se resumiam somente em mensagem de textos.

Portanto, o MIME (*Multipurpose Internet Mail Extensions*) visa suprir a limitação do corpo de e-mail que é expressa na codificação US-ASCII. Sua implementação foi projetada inicialmente pela RFC 1341 e atualizado nas RFCs de 2045 a 2049. Dentre as diversas dificuldades encontradas com a popularização de e-mails, os principais empecilhos foram os seguintes:

- Mensagens escritas em idiomas que usam acentuação (português, alemão e etc).
- Mensagens escritas em alfabetos não latinos (russo, hebraico e etc).
- Mensagens escritas em idiomas sem alfabeto (chinês, japonês e etc).
- Mensagens que não contém texto (áudio, imagens e etc).

A ideia básica do MIME é continuar usando a RFC 5322 como padrão de formato de e-mails, porém determinando o modo pelo qual os corpos dos e-mails devem ser estruturados. Além disso, este padrão define regras para mensagens que não utilizam o formato US-ASCII.

Pelo fato de mensagens MIME manter compatibilidade com a RFC de formato de mensagens, não houve dificuldade de implantação desse padrão em todas as partes integrantes do serviço de e-mail.

O MIME desenvolveu 5 novos cabeçalhos para mensagens de e-mails. O seu primeiro cabeçalho identifica a versão do MIME utilizado na correspondência eletrônica. Além disso, a ausência deste campo indica que o conteúdo e-mail conterá apenas texto em formato ASCII de 7 bits. O campo de número 2, conhecido como *Content-Description*, armazena uma breve descrição, em formato US-ASCII, do conteúdo da mensagem. Isso serve para o usuário decidir se quer ou não decodificar o corpo do e-mail, uma vez que essa decodificação pode onerar bastantes recursos da máquina do usuário.

O próximo campo MIME é o *Content-Id*. Ele registra o identificador do conteúdo de um e-mail. O penúltimo campo, *Content-Transfer-Enconding*, informa o modo em que o corpo do e-mail está codificado. Esse parâmetro permite 5 modos de codificação os quais podem ser trafegados sobre o protocolo de transmissão de mensagens de e-mail. São eles:

1. 7bit => Modo que utiliza a tabela ASCII de 7 bits. É transmitido diretamente pelo protocolo SMTP, desde que não ultrapasse a quantidade de 1000 caracteres por linha.
2. 8bit => Esquema semelhante ao anterior, porém utilizando 8 bits de caracteres, ou seja, todos os valores de 0 a 255. Esse modelo viola o protocolo original de mensageiria eletrônica, mas é aceito por clientes que implementam uma extensão do protocolo original. Seus e-mails declaram a utilização 8 bits, entretanto isso não significa que os clientes estão aptos a entendê-lo.
3. Base64 => Utiliza tamanhos de dados de 3 em 3 octetos do caractere ASCII e o subdivide em 4 grupos de 6 bits cada totalizando 24 bits. Este tipo de codificação contém um alfabeto próprio conforme pode ser visto na Figura 3.2.

Binary	ASCII	Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/

Figura 3.2: Alfabeto da Base64
Adaptada de [10]

Além dos caracteres dispostos acima, esse modo utiliza do símbolo “=” para representar o *padding*. Esse *padding* ocorre porque a divisão de 6 em 6 bits nem sempre termina com todos os bits completos do octeto. Ou seja, quando se tem *strings* com 16 bits de tamanho, haverá ausência de 8 bits na codificação base64 Portanto, ao ocorrer uma codificação desse tipo, se a *string* resultante possuir em seu fim um “==” significa que a última unidade contém 8 bits de tamanho e caso ela apresente “=” infere que a última unidade possui 16 bits.

4. *Quoted-printable* => Modalidade representada por todos os caracteres ASCII imprimíveis. Pode-se transmitir 8 bits de dados por meio de um canal que suporte transferência de dados de 7 bits, como no caso de correio eletrônico. *Quoted-printable* faz uso do sinal “=” seguido de dois caracteres hexadecimais para representar o valor codificado.
5. Lacuna cedida para novos métodos de codificação de corpos de mensagens de e-mail.

Em suma, para representação de dados binários, a melhor alternativa é aplicar a codificação base64 ou a *quoted-printable*. Dessa forma, eles podem ser trafegados via e-mail por meio do padrão US-ASCII. Essas codificações deverão acontecer antes do envio da mensagem e sua decodificação deverá ocorrer após o transporte do e-mail ter sido realizado.

Para finalizar, o último campo proposto pelo MIME é o *Content-Type*. Ele tem a finalidade de prover a natureza do corpo da mensagem. São 7 os tipos admitidos pela RFC 2045 e cada um dele pode possuir um ou mais subtipos. O tipo e subtipo são delimitados pelo símbolo "/". Na Tabela 3.3, os tipos e subtipos especificados na RFC 2045:

Tabela 3.3: Tipos e Subtipos do campo *Content-Type* MIME

Tipo	Subtipo	Descrição
Text	*Plain*	Texto sem formatação
	Enriched	Texto incluindo comandos de formatação
Image	Gif	Foto no formato Gif
	Jpeg	Foto no formato Jpeg
Áudio	*Basic*	Som audível
Vídeo	Mpeg	Filme no formato Mpeg
Application	*Octet-stream*	Sequência de bits não interpretada
	PostScript	Documento que pode ser impresso em PostScript
Message	RFC 5322	Email encapsulado no formato RFC 5322
	Partial	Email foi dividido para ser enviado
	External-body	Email deve ser obtido por meio da rede
Multipart	*Mixed*	Artes independentes na ordem especificada
	Alternative	Mesmo e-mail em diferentes formatos
	Parallel	Pedaços devem ser vistos simultaneamente
	Digest	Cada parte é um e-mail RFC 5322 completo

Os atributos do campo MIME *Content-Type* foram adaptados de [2]

3.5. POST OFFICE PROTOCOL VERSION 3

A solução ofertada pelo protocolo SMTP realiza o trabalho de entregar a mensagem ao servidor de e-mail do destinatário pertinente. Todavia, uma vez residida nesse servidor, o usuário final precisará fazer uma conexão com este servidor para receber suas correspondências eletrônicas. Devida à existência dessa nova requisição, o protocolo POP foi elaborado para suprir essa necessidade.

O POP3 (*Post Office Protocol Version* 3) tem por finalidade se conectar no servidor de e-mails onde possui uma caixa postal e realizar o *download* de seus e-mails. Suas definições estão dispostas na RFC 1939. Ele é um protocolo extremamente simples e com poucas funcionalidades. Em seu funcionamento, um cliente, por meio de um agente de usuário de e-mail (MUA), requisita uma conexão TCP no servidor em sua porta 110 se a funcionalidade de cifragem não estiver acoplada ao POP3.

Uma vez estabelecida a conexão, o POP3 exibe três estados de sequência conhecidos como autorização, transação e atualização. A fase autorização contempla a autenticação do usuário via o seu programa local de e-mail. Caso a comunicação não forneça criptografia, o usuário e a senha são passados às claras. A próxima etapa, a transação, promove a recuperação das mensagens eletrônicas. Além de baixar os e-mails, o cliente de e-mail do usuário poderá fazer marcações de deleção e obter estatísticas de correio. O último estado realiza efetivamente a exclusão das mensagens marcadas para serem excluídas. Este entra em ação no momento posterior ao término do *socket* POP3.

Uma conexão POP3 pode ser feita com o programa telnet. A situação descrita na Tabela 3.4 abaixo exibe os comandos suportados pelo protocolo e o comportamento do servidor em relação a eles.

Tabela 3.4: Fase autorização POP3 via telnet entre cliente e servidor

Fase de autorização POP3
1. **Cliente:** telnet servidor.dominio.br 110
2. **Servidor:** + OK POP3 *server ready*
3. **Cliente:** USER Mario
4. **Servidor:** +OK
5. **Cliente:** PASS senhaMario
6. **Servidor:** +OK *user successfully logged on*

Dados adaptados de [1]

Esse pedaço de comunicação POP3 representa a fase de autorização. Informações de usuário e senha são transmitidos para o servidor o qual fará a verificação em sua base de usuários para realizar a validação. Se, porventura, a acontecer alguma falha na autenticação

devido ao fornecimento da senha ou usuário incorreto, o servidor retornará ao invés de "+OK" o valor "-ERR".

Agora, relativo a estado transação, a Tabela 3.5 demonstra um fluxo de comunicação.

Tabela 3.5: Fase transação POP3 via telnet entre cliente e servidor

Fase de transação POP3
1. **Cliente:** LIST
2. **Servidor:** 1 533 2 942 3 613 .
3. **Cliente:** RETR 1
4. **Servidor:** (Envia o conteúdo do e-mail número 1)
5. **Cliente:** DELE 1 RETR 2
6. **Servidor:** (Envia o conteúdo do e-mail numero 2)
7. **Cliente:** DELE 2 RETR 3
8. **Servidor:** (Envia o conteúdo do e-mail número 3)
9. **Cliente:** DELE 3 QUIT
10. **Servidor:** +OK POP3 server signing off

Tabela adaptada de [1]

O servidor imprime uma lista de e-mails, um por linha, e seus respectivos identificadores e tamanhos quando o cliente envia o comando LIST. O cliente recebendo essas informações recupera cada mensagem através do comando RETR (abreviação da palavra inglesa *retrieve*) e posteriormente marca a mensagem para ser deletada do servidor por meio da expressão DELE (abreviação de *delete*).

Depois de decorrida toda a transferência de todos os e-mails do usuário autenticado, o cliente envia o comando QUIT. Este comando determina a finalização do estado de transação

e inicia a fase de atualização. Nesta fase, o servidor apaga as mensagens até então marcadas para serem removidas.

O POP3, consoante visto, é um protocolo que funciona apenas descarregando todas as mensagens do servidor de e-mail. Essa característica tornou-se uma problemática no ambiente de mensageiria eletrônica moderna. Imagine um funcionário que não possui uma estação de trabalho fixa para trabalhar, ou até mesmo, que este viaje por diversas unidades de trabalho e acesse seu correio periodicamente em máquinas diferentes. O POP3 não atenderia bem seus anseios, pois cada computador armazenaria mensagens diferentes e resultando em um espalhamento de seus e-mails por diversas máquinas. Clientes de e-mails modernos sanam essa necessidade com a opção de deixar uma cópia do servidor de e-mails, porém não são todos os programas de e-mail que ofertam essa funcionalidade.

Outro empecilho encontrado neste protocolo é referente ao backup de mensagens. Um usuário que sempre mantém seu cliente de e-mail ativo está sempre sincronizando o recebimento e envio de e-mails. Clientes de e-mail suportam até configurar uma quantidade de tempo determinada para fazer a sincronização automática. Desta forma, quando um usuário recebe um e-mail quase que instantaneamente a mensagem é baixada para sua máquina. Então, como a mensagem fica pouco tempo armazenado no servidor, esta fica a critério do usuário manipular a mensagem inclusive a sua remoção. Logo, uma política de backup que envolva e-mails de usuários que utilizem o POP3 fica inviável.

3.6. INTERNET MESSAGE ACCESS PROTOCOL

Visando solucionar a principal dificuldade encontrada no POP3, o protocolo IMAP (*Internet Message Access Protocol*) surgiu para provê acesso as mensagens eletrônicas diretamente no servidor de caixas postais, trazendo aos usuários maior conveniência de acesso de lugares múltiplos e uma enorme facilidade e possibilidade de fazer backup das caixas postais.

Este novo protocolo foi publicado pela RFC 3501 e usuários *road warriors* conseguiam então manter um local centralizado de acesso aos e-mails. A função do IMAP é a mesma do POP3 cujas intenções são dispor o acesso de e-mails do servidor aos seus usuários. Todavia, esse protocolo oferece uma riqueza maior de recursos, o que implica também em uma complexidade estrutural maior que o POP3.

Diferentemente do POP3 que supõe que os usuários farão conexão com o servidor e extrairão todas as mensagens deste e trabalharão *offline*, o IMAP manterá as mensagens armazenadas no servidor e trabalhará de maneira *online*.

O IMAP fornece funcionalidades de leitura de e-mail que deixam os usuários decidirem se farão ou não o *download* de anexos de mensagens principalmente os grandes como áudios e vídeos. Isto é importante para clientes que possuem conectividade por meio de modems lentos ou que tenham pequena largura de banda.

A criação de hierarquia de pastas para os usuários manipularem e organizarem os e-mails é outra característica possível deste protocolo. Pastas podem aparentar ocultas em clientes de e-mails por meio de inscrições e desinscrições de pastas IMAP. A Tabela 3.6 representa uma analogia relacionando algumas características fundamentais dos protocolos de recepção de mensagens eletrônicas.

Tabela 3.6: Analogia entre POP3 e IMAP

Característica	POP3	IMAP
Local de definição do protocolo	RFC 1939	RFC 3501
Porta TCP utilizada	110	143
Local de armazenamento de e-mails	PC do usuário	Servidor
Modo de leitura do cliente de e-mail	*Offline*	*Online*
Tempo de conexão	Pequeno	Grande
Uso dos recursos do servidor	Mínimo	Enorme
Responsável pelo backup dos e-mails	Usuário	Administradores
Dispõe facilidades para usuários em trânsito	Não	Sim
Controle do download de mensagens	Pequeno	Grande
Oferta download de mensagens parciais	Não	Sim
Problemas de quotas de disco no servidor	Não	Sim
Protocolo possui fácil implementação	Sim	Não

Dados adaptados de [2]

3.7. WEBMAIL

Este modo de acesso a e-mails agrega o protocolo HTTP estabelecendo, por meio de funções de linguagem de programação, conexão IMAP localmente no servidor de e-mail. Tais webmails oferecem diversas funcionalidades e pode-se acoplar *plugins* a este *software* à medida que novas necessidades vão surgindo no ambiente de mensageiria eletrônica.

Em tempos modernos, o webmail é uma ferramenta que disponibiliza ao usuário agendas compartilhadas, catálogo global de endereços de e-mail, lista de discussão de e-mail, mensageiria instantânea e demais recursos. Tais recursos reunidos em um único programa são conhecidos como ferramenta colaborativa.

Para finalizar, a comunicação feita do usuário até o cliente de e-mail é toda comunicada sob HTTP, assim como o retorno do servidor para o usuário é realizada por HTTP. Para acontecer à tramitação de e-mails, o programa webmail encapsula comandos IMAP e SMTP através de códigos de programação sob uma conexão tunelada no protocolo HTTP.

3.8. SERVIDOR DE EMAIL

O software comumente utilizado para fornecer o serviço de correio eletrônico era o Sendmail. Porém, devido a suas falhas de segurança (hackers invadiam o servidor físico por meio da vulnerabilidade deste software) foi-se tornando necessário o desenvolvimento de um novo software para tramitação de e-mails de um modo mais seguro e eficiente. A falta de compatibilidade com outros softwares tais como antivírus, anti-spam e outros softwares facilitaram o declínio do uso deste programa, uma vez que o mundo do e-mail crescia cada vez mais e necessitava de programas que filtrassem o ambiente de mensageiria eletrônica com objetivo de bloquear spams e outras pragas virtuais que começaram a surgir. A dificuldade de configuração (arquivos de configuração pouco amigáveis aos usuários) deste software foi mais um agravante para este ter se tornado obsoleto no mercado.

Visto toda essa problemática, a IBM projetou, sob a liderança de Wietse Venema, um software de e-mail que substituísse o antigo Sendmail. Nessa nova solução, diversas correções no tocante à segurança do MTA de e-mail foram implementadas, bem como facilidades de configuração, visto que no Sendmail alterações eram bastante complexas. O resultado deste

projeto foi à criação do Postfix, programa este que possui a licença IPL (IBM *Public* License) que é parecida com a GPL, porém com algumas restrições adicionais. Outra característica desse software é a compatibilidade com diversos programas complementares de forma modular.

O Postfix é um dos softwares mais adotados em diversas instituições governamentais. Muitas distribuições Linux o escolheram como programa padrão para o serviço de e-mail. Vários aspectos o tornam uma excelente escolha como MTA para organizações. Devido robustez do serviço apresentado, o fato ser um software livre e facilidade de instalação e configuração do servidor de e-mail faz deste um grande ocupante no mercado de e-mail.

O Postfix é um software livre de servidor de e-mail que utiliza o protocolo SMTP para troca de mensagens eletrônicas entre servidores de e-mail. A porta reservada para o SMTP, de acordo com o que foi padronizado pela IETF, é a porta 25. Essa porta pode ser alterada nas configurações do serviço se algum administrador assim desejar.

3.8.1. Arquitetura do Postfix

A arquitetura do Postfix é composta por diversos programas que são gerenciados por um processo único denominado master. Este processo funciona coordenando seus subprocessos utilizando o modelo conhecido como “pai-filho”, mas mantendo a ideologia de processos cooperativos. Resumidamente, as tarefas do Postfix são independentes e provêm serviços umas as outras. Por exemplo, o programa que fornece *trivial-rewrite* (reescrita/tradução de endereços) faz esta atividade para todos os outros processos do programa.

Diferentemente do Sendmail, o Postfix não apresenta uma estrutura monolítica, conforme visto acima. Cada processo dentro Postfix foi desenvolvido para executar uma função específica dentro da gama de aspectos a se tratar neste ambiente.

A Figura 3.3 demonstra todo o fluxo percorrido por uma mensagem quando esta entra no sistema de e-mails do Postfix. As próximas 2 imagens tem como programas ou comandos os objetos elíptico e filas de mensagens os retângulos abaulados.

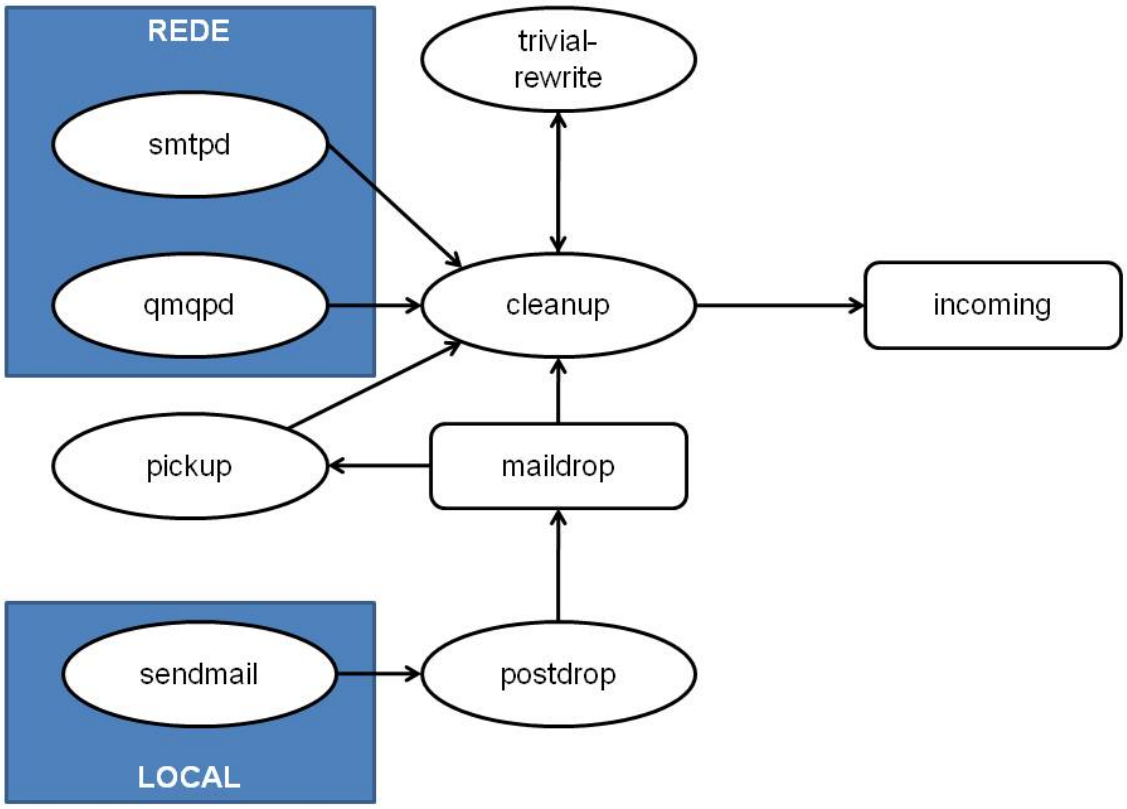

Figura 3.3: Recepção de mensagens no Postfix
Adaptada de [42]

Conforme apresentada pela Figura 3.3, o Postfix recebe mensagens de duas maneiras: através da rede e localmente. Existem 4 alternativas para se receber mensagens pelo Postfix. São elas:

- A mensagem pode ser gerada localmente por um programa ou comando (existe compatibilidade com Sendmail).
- A mensagem chega ao servidor a partir da rede por protocolo SMTP ou QMQPD e outros.
- Uma mensagem já aceita pode ser reencaminhada ou redirecionada para outro endereço de e-mail (tabelas canônicas, arquivos de *forward* e etc).
- Postfix gera uma mensagem de retorno ao usuário quando o destinatário não é alcançado (destinatário não recebe a mensagem).

Este fluxo é muito importante para ser conhecido por administradores do serviço de correio eletrônico, pois com o conhecimento disso ele estará mais capacitado para gerenciar o serviço de e-mail e configurá-lo de maneira mais eficiente.

Ao se fazer a análise da recepção de um e-mail, quando o mesmo chega pela da máquina local, ele é entregue ao programa *postdrop* que é responsável por despejar a mensagem em uma fila de e-mail chamada *maildrop*. Essa fila contém e-mails os quais estão à espera de serem abrigados na fila de entrada (*incoming*) de e-mail. O *daemon pickup*, então, retira a mensagem da mencionada fila e alimenta o próximo programa *cleanup*. A função deste programa é verificar a sanidade da mensagem, e também, fazer a inspeção dos campos requeridos que não estão preenchidos ou não estão no formato esperado. Logo após esta etapa, o *deamon trivial-rewrite* é invocado para completar os campos requeridos que estão vazios, colocar o e-mail no formato esperado pelos programas que compõe o Postfix e finalmente faz consulta as tabelas de e-mails canônicos e virtuais para reescrita das informações contidas no e-mail. No desfecho, o programa *cleanup* entrega a mensagem para a fila de entrada do Postfix chamada *incoming*.

Quando um e-mail chega através da rede, o que difere do processo acima, é que este, após sair do protocolo de rede, chega ao programa *cleanup* e daí segue o fluxo segundo visto na figura e na explanação do e-mail gerado localmente.

Enquanto isso, a Figura 3.4 dispõe o modo pelo qual uma mensagem é entregue na caixa postal de um usuário, ou seja, quando ela atinge a fila *incoming* a espera de ser entregue ao seu destinatário final por intermédio de seus programas.

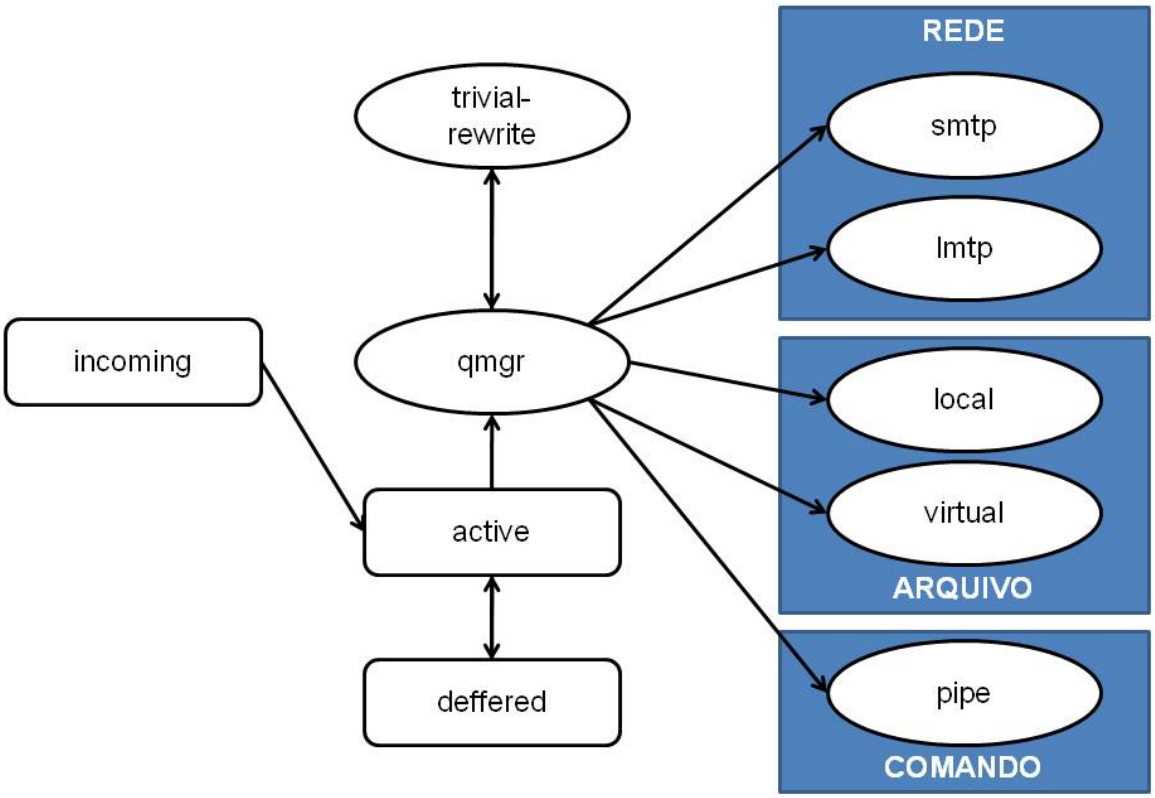

Figura 3.4: Entrega de mensagens no Postfix
Adaptada de [42]

Quando uma nova mensagem atinge a fila *incoming*, esta alerta o programa *queue manager* (qmgr), que é o coração do Postfix, e esse *deamon* consulta o endereço do destinatário em suas tabelas de pesquisa. Caso seja encontrado em suas tabelas, o *queue manager* utiliza do programa *trivial-rewrite* para fazer as alterações necessárias, por exemplo, um e-mail canonical deverá ser convertido para o e-mail real do destinatário e o deposita no sistema de arquivamento do servidor de e-mail. Assim, o usuário final utilizando o seu cliente de e-mail poderá acessar a mensagem usando os protocolos POP3 e IMAP.

Agora, se o e-mail do destinatário for de propriedade do MTA externo ao domínio local, o queue manager entrega a mensagem ao *daemon* SMTP para entrega final. Ao tentar fazer entrega em outro MTA, deverá ser consultado o dns do domínio do destinatário para obtenção do registro MX (mail *exchanger*) deste domínio. Com isso a comunicação dos dois MTAs ficará viável para entrega do e-mail ao seu destino.

O *queue manager* pode, também, por falhas de entrega, seja um arquivo de pesquisa mal escrito ou *timeout* de outro MTA externo e demais situações, armazenar a mensagem na

fila *deferred*. Estando nessa fila a mensagem fica a disposição para uma nova entrega e uma nova tentativa ocorre de acordo com o tempo que for configurado no Postfix.

3.9. CONFIGURAÇÃO DO POSTFIX

Uma das grandes evoluções do Postfix é a sua facilidade de configuração e adaptação de módulos de softwares ao mesmo, conforme informado em momentos anteriores.

Os caminhos padrões dos arquivos, em um momento posterior a instalação do Postfix, são os descritos abaixo:

- /etc/postfix: Arquivos de configuração
- /usr/libexec/postfix: Postfix daemons
- /var/spool/postfix: Arquivo de filas
- /usr/sbin: Comandos Postfix

Informações dos arquivos constituintes e seus caminhos do colocados no sistema operacional pela instalação do pacote Postfix são exibidos no Quadro 1:

Quadro 1: Arquivos constituintes do pacote Postfix

```
#rpm -ql postfix
```

3.9.1. Configuração do Postfix genérica

No Quadro 2, as linhas da são configurações relevantes para o funcionamento padrão para o protocolo SMTP de servidor de correio eletrônico. Estas são encontradas no arquivo /etc/postfix/main.cf.

Quadro 2: Configuração do arquivo /etc/postfix/main.cf

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix
myhostname = mx.empresa.br
mydomain = empresa.br
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 550
mynetworks = 192.168.100.0/24
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

```
home_mailbox = Maildir/
smtpd_banner = Servidor de e-mail da empresa.br
debug_peer_level = 2
debugger_command =
      PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
      $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
     readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
```

A sintaxe desse arquivo de configuração do Postfix é composta por um parâmetro seguido de um valor como "parâmetro = valor". Outra flexibilidade disponível no arquivo de configuração do Postfix é utilizar um parâmetro recebendo um valor de outro parâmetro já especificado acima. Segue um exemplo dessa configuração: "parâmetro = $parâmetro_especificado". Nota-se que o parâmetro que já foi configurado recebeu um "$" que significa que este parâmetro deve ser substituído pelo valor configurado em linhas anteriores no arquivo de configuração.

É observado que ao se instalar o programa Postfix, a maioria das linhas mostradas na figura acima se apresentam iguais as mostradas acima, com exceção de algumas linhas onde o administrador deve inserir as informações necessárias para funcionamento do serviço. Neste ponto geralmente ocorre o grande problema nesse serviço, pois administradores apenas fazem esta configuração básica, esquecendo-se de incluir softwares como anti-spam, autenticação do e-mail, criptografia e configurações refinadas em sua configuração. Assim, os alicerces da segurança da informação tornam-se frágeis e algumas fraudes conhecidas podem ser realizadas.

Na ilustração mostrada acima, para o serviço de mensageiria entrar em funcionamento é necessário configurar alguns parâmetros. O Postfix aproveita o registro do nome da máquina local para preencher o parâmetro myhostname. Caso o nome da máquina esteja no padrão FQDN (*fully qualified domain name*), a configuração deste não se faz necessária. Porém, em caso contrário, o nome da máquina deve ser inserido manualmente e obrigatoriamente no arquivo de configuração. Outros parâmetros tais como mydomain, mydestination, mynetworks, home_mailbox são importantes de serem configurado inicialmente. Como pode ser visto, é bastante simples para iniciar o serviço de forma fácil e prática.

3.9.2. Configuração do Dovecot genérica

Além da configuração correta do arquivo main.cf, para o provimento adequado do serviço de correio eletrônico vigorar, uma configuração mínima do servidor POP3/IMAP precisa ser realizada. O arquivo responsável por efetivar as características de funcionamento do serviço mencionado é localizado no caminho /etc/dovecot/dovecot.conf ou em seus subarquivos encontrados no diretório /etc/dovecot/conf.d.

Para atuação do servidor POP3/IMAP, de tal serviço entrar em funcionamento de modo genérico, é exemplificada no Quadro 3. Note que a primeira seção é relativa ao arquivo /etc/dovecot/conf.d/10-auth.conf e a segunda o /etc/dovecot/conf.d/10-mail.conf.

Quadro 3: Configuração genérica do Dovecot

Parte 1:

```
disable_plaintext_auth = no
```

Parte 2:

```
mail_location = maildir:~/Maildir
```

3.10. ESTRUTURA DOS SERVIDORES DE E-MAIL

A comunicação por correio eletrônico torna o processo dos negócios muito ágil, ao passo que uma pessoa em qualquer local do globo pode trocar informações em instantes.

Primeiramente, a tecnologia de correio eletrônico do órgão deverá ser analisada, para que em um momento posterior ela seja avaliada e criticada construtivamente em aspectos de segurança da informação. Sendo assim, a Figura 3.5 retrata uma situação ideal da estrutura do serviço de e-mail.

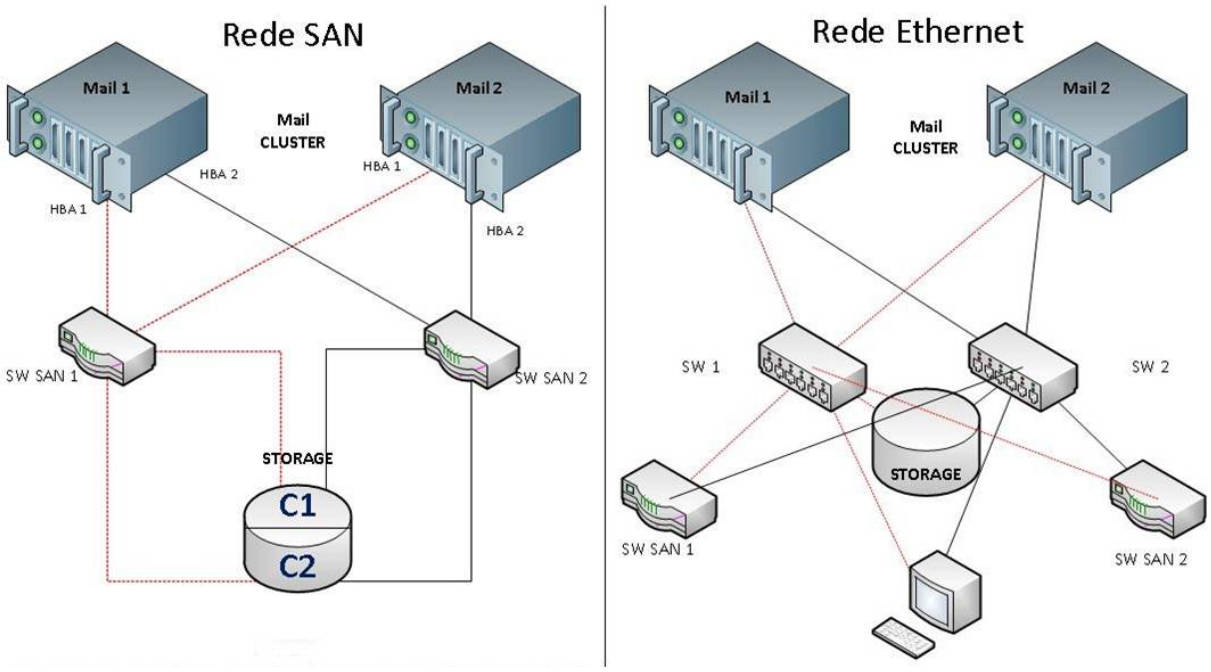

Figura 3.5: Estrutura física com alta disponibilidade de correio eletrônico

Este diagrama representa uma estrutura otimizada dos servidores de e-mail em cluster. Tem como objetivo aumentar a disponibilidade e desempenho desse importante serviço provido pela empresa.

A esquerda da Figura 3.5 está representado o diagrama SAN (Storage *Area* Network) o qual apresentada a estrutura de cluster ligada a um *storage* por meio de fibras óticas.

No diagrama Ethernet, que está disposto à direita da Figura 3.5, há a representação da mesma estrutura, mas sob o formato *ethernet*. Esta estrutura troca informações entre os servidores de e-mail com o restante da rede.

Percebe-se que a finalidade do esquema proposto é evitar que paradas no serviço de correspondência eletrônica ocorram, seja por falhas de *hardware*, excessivo processamento de dados ou qualquer outro gargalo que cause indisponibilidade deste, que atualmente, necessita está em funcionamento praticamente todos os dias do ano.

3.11. CRESCIMENTO DA MENSAGEIRIA ELETRÔNICA E DIFICULDADES ENCONTRADAS

O serviço de correio eletrônico é um dos serviços da Internet que mais cresce no ambiente corporativo. Essa evolução vem acarretando vários problemas para as organizações no que tange principalmente os tipos de informações que circulam dentro da rede corporativa.

As mensagens enviadas através do correio eletrônico podem ser interceptadas, caso mecanismos de seguranças não estejam dispostos, por pessoas as quais não são destinadas. A garantia de privacidade no uso do correio eletrônico, em diversas instituições, não existe. A mensagem, uma vez enviada, passa por uma série ativos de rede e em rotas variadas para finalmente ser armazenada no servidor. Desta forma, o usuário se autentica neste servidor e acessa a mensagem eletrônica.

Segundo CGI.br, no ano de 2009, diversos relatórios e estatísticas apontaram um crescimento na quantidade de spams que são, supostamente, originados em redes brasileiras. A maior parte destes relatórios não são, necessariamente, uma novidade, e são consistentes com diversos estudos que o CERT.br têm realizado nos últimos anos. A Figura 3.6 ratifica a pesquisa do CERT.br.

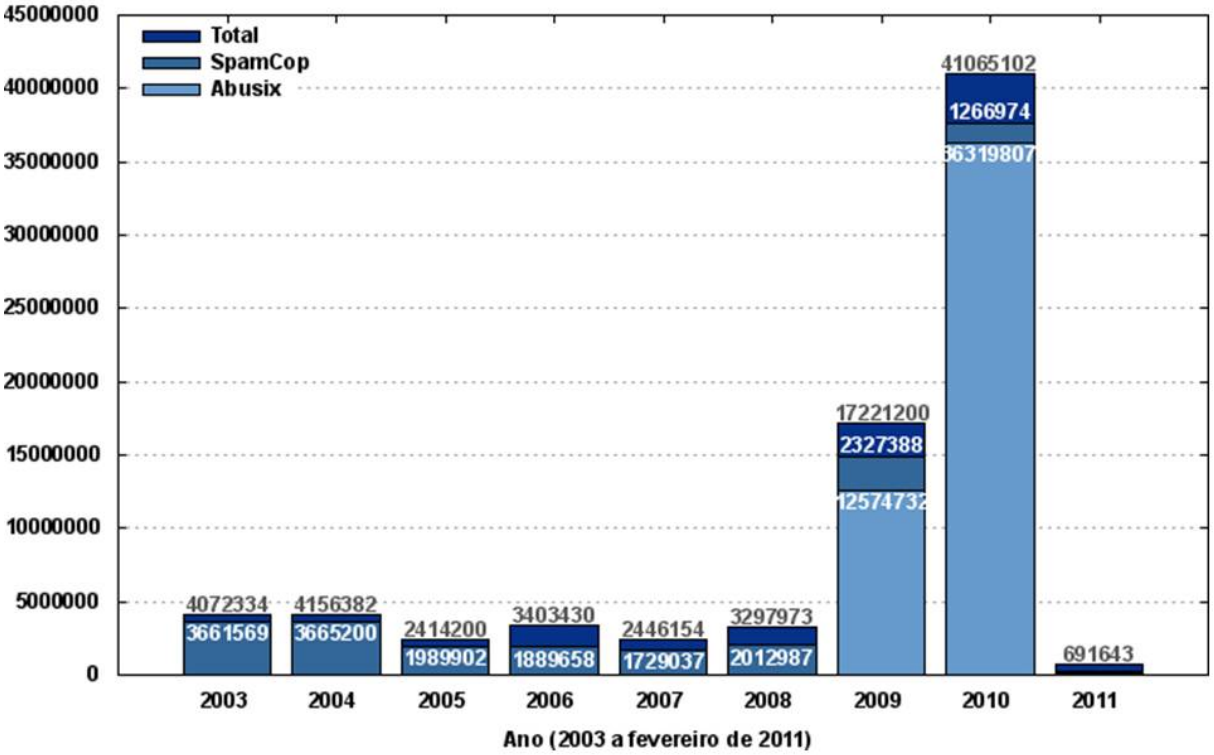

Figura 3.6: Spams reportados ao CERT.BR por ano
[15]

Segundo estudos feitos pela CT-Spam, o Brasil assumiu em 2009 a liderança no seguinte problema: “De acordo com as diversas estatísticas, somos o país com o maior número de máquinas comprometidas ou mal configuradas sendo abusadas por *spammers* do mundo todo”.

Estas mesmas conclusões também estão presentes em uma matéria da Forbes sobre o relatório da Cisco, em particular as seguintes afirmações:

“Brazil's spam boom is no mystery. The country, says Cisco security researcher Patrick Peterson, is suffering the same junk mail epidemic that other fast-growing nations have experienced as they plug into the Internet. "Brazil has had very fast broadband rollout, but without the user education, antivirus, firewalls and Internet service provider programs that are cutting off spam in the U.S.

Neither Brazil nor India is directly responsible for the flood of spam that has emanated from the two countries as their digital economies come online. Both nations are likely being exploited by global cybercriminals who see cheap domains and large numbers of unprotected PCs as an opportunity to funnel junk mail around the world.”

Levando em conta a relevância da entidade governamental no cenário político/econômico nacional, uma alta quantidade de spam não é o único problema enfrentado por esse órgão. Soares, Lemos e Colcher.

O que ameaça a estabilidade da empresa não só nos quesitos do CID (Confidencialidade, Integridade e Disponibilidade), mas em outros fatores como a confiança e imagem já que no caso dos e-mails se lida com imagens tanto da empresa quanto das pessoas que a representam. Em um simples caso de roubo de senha arrisca-se duplamente já que uma pessoa pode enviar em nome de outra, informações falsas que comprometam tanto a instituição quanto ao usuário.

A aplicação do plano tem por fim a mitigação dos riscos provenientes das ameaças às quais estão vulneráveis os ativos da organização.

A adoção de uma política de segurança, para o contexto de e-mail, servirá como documento norteador das ações e processos dentro da entidade governamental.

4. POLÍTICA DE SEGURANÇA A LUZ DA ISO 27002:2005

Conforme observado em tópicos anteriores, a estrutura, os protocolos, o software, o cabeamento e demais itens do contidos no serviço de mensageiria eletrônica são elaborados para provê segurança e disponibilidades das informações tramitadas nesse meio.

Porém, uma vez que o usuário manipule de maneira insegura o serviço de correio eletrônico, todo esse esquema de segurança é posto em xeque. Podem-se imaginar usuários realizando procedimentos inseguros como expor senha de e-mail próximo ao teclado de sua máquina, envio de e-mails com conteúdos duvidosos, disparo de diversos e-mails com a finalidade de divulgar um produto ou serviço e dentre outras atividades.

Para isso, uma política de segurança que oriente uma maneira desejável da utilização do sistema de e-mail é um fator crítico de sucesso para se propor um ambiente que almeje ter uma boa segurança de e-mail.

Além disso, a implantação da política de segurança agrega uma visão de gestão de segurança da informação, uma vez que esta filosofia contém requisitos de como constituir um SGSI (calcadas na ISO 27001) e também técnicas e melhores práticas no âmbito de segurança da informação (localizadas na ISO 27002). Nesta última ISO existem controles que regem a maneira como o serviço de e-mail deverá se portar, entretanto ela será utilizada de modo genérico porque outras sugestões encontradas ao longo do referido documento também são relevantes de serem adotadas.

Para constituição da citada política, a ISO 27003 é consultada para guiar a estrutura do documento gerado, bem como a ISO 27005 para fornecimento de tópicos atrelados com a gestão de riscos utilizando técnicas de segurança da informação.

Os capítulos da política de segurança da informação, identificação, análise, avaliação e tratamento dos riscos propõem instaurar um lado mais gerencial por meio de consolidações de procedimentos e rotinas, visto que o assunto abordado costuma possuir seu enfoque técnico na maioria das documentações existentes.

4.1. NORMAS REFERENCIADAS

As normas citadas abaixo foram usadas para desenvolver esta seção:

- ABNT NBR ISO/IEC 27001:2006 – Norma brasileira que contém os requisitos embasados em técnicas de segurança para implementar um SGSI
- ABNT NBR ISO/IEC 27002:2005 – Norma brasileira que especifica o código de prática para a gestão da segurança da informação
- ISO/IEC 27003:2010 – Padrão internacional que normatiza técnicas de segurança e serve como um guia de implementação de um SGSI
- ABNT NBR ISO/IEC 27005:2008 – Norma brasileira que contempla técnicas de segurança atuando na área de gestão de riscos de segurança de informação

4.2. E-MAIL

- Os usuários devem conhecer a Política de Segurança da Informação, normas de segurança e regulamentações internas do órgão em vigor.
- O correio eletrônico corporativo só deve ser utilizado para assuntos de interesse da organização.
- O uso do correio eletrônico corporativo somente deve ser realizado pelo software de correio disponibilizado nas estações de trabalho ou equipamento portátil da entidade ou ainda por meio de browser de internet.
- Mensagens recebidas por remetentes desconhecidos não devem ser lidas e nem respondidas.
- A organização permite o uso parcimonioso do correio eletrônico particular para interesses particulares dos usuários, desde que esse uso não exceda os limites da ética, razoabilidade e não faça uso de informações de propriedade do órgão.
- O usuário deve realizar periodicamente manutenção em sua caixa de correio eletrônico de forma a garantir que o limite de tamanho não seja ultrapassado e manter o serviço sempre disponível. Mensagens já lidas ou sem utilidade devem ser apagadas regularmente pelo próprio usuário.

- Uma assinatura padrão deve ser colocada no final de cada mensagem e deve ser usada somente para identificar seu remetente.
- A senha padrão do correio eletrônico corporativo deve ser trocada no primeiro acesso do usuário.
- Mensagens de correio eletrônico que contenham informações sensíveis ao órgão devem, sempre que possível, ser criptografadas antes do envio de forma a preservar o seu sigilo e integridade.
- A utilização do serviço de correio eletrônico corporativo da entidade deve ser feita de forma a preservar o bom funcionamento e para isso o usuário deve:
    1. Não clicar em links de Internet que tenham origem desconhecida a fim de eliminar a possibilidade de instalação de softwares que contenham códigos maliciosos.
    2. Não executar arquivos anexados às mensagens recebidas pelo correio eletrônico corporativo de remetentes desconhecidos.
    3. Não divulgar o endereço do correio de trabalho corporativo em sites ou listas de discussão na Internet.
- O correio eletrônico corporativo não pode ser utilizado para armazenar, enviar ou receber, de forma consentida, mensagens com código malicioso, conteúdos pornográficos, atentatórios à moral, ofensivos, de incitação à violência, que contenham conteúdo criminoso ou ilegal ou que façam sua apologia, que não respeitem os direitos autorais, realização de SPAM ou qualquer e-mail que atrapalhe a condução e continuidade do trabalho.

4.3. CRIAÇÃO, BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE CORREIO ELETRÔNICO

- A utilização do correio eletrônico corporativo é uma concessão do órgão, não um direito do usuário e será obrigatoriamente cancelado quando do seu desligamento, ao final da vigência do contrato ou qualquer outro ato jurídico firmado ou por solicitação do chefe imediato ou superior do usuário.
- A conta de correio eletrônico corporativo deve ser vinculada ao tempo de permanência do usuário na organização e será bloqueada ou desativada caso:
    1. Seja detectada a ausência do usuário por período igual ou superior a 90 dias.

2. O usuário seja desligado do órgão.
3. Exista uma solicitação judicial.
4. Seja solicitado bloqueio ou cancelamento pela chefia da área.

4.4. MONITORAMENTO

- O correio eletrônico corporativo pode ser monitorado e restringido pela coordenação de TI, quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados).
- Nos casos de suspeita de infração à Política de Segurança da Informação em vigor e normas correlatas, a coordenação de TI poderá acessar a caixa postal corporativa do usuário em questão.
- O chefe imediato ou superior pode solicitar formalmente à coordenação de TI acesso a caixa postal corporativa de um de seus usuários, para si ou para outro usuário, nas seguintes situações:
  1. Desligamento do usuário.
  2. Término do contrato.
  3. Afastamentos do usuário por motivos de licenças.
  4. Falecimento do usuário.
  5. Suspeita de infração à Política de Segurança da Informação em vigor e normas correlatas.

4.5. CONTROLE DO ACESSO FÍSICO

- O órgão deve criar identificação física diferenciada para cada local de suas instalações.
- As pessoas que transitam pelas instalações do órgão devem ser identificadas nos pontos de entrada e saída da organização e portarem de forma visível uma identificação física que informe o local de destino.

1. Ao sair das instalações do órgão, o visitante deve obrigatoriamente entregar nos pontos de entrada e saída da entidade a identificação física que lhe foi concedida.

- A organização deve implementar mecanismos de controle de acesso físico diferenciado de acordo com a criticidade de cada ambiente.
- A organização deve implementar e manter atualizado um mecanismo de registro de incidentes de segurança física do ambiente.

4.6. INSTALAÇÕES FÍSICAS

- As instalações do órgão devem conter sistemas de detectores de fumaça como meio de alerta de incêndio.
- Os quadros de controle e caixas de passagem do cabeamento lógico (dados e voz) devem permanecer trancados, sendo seu acesso restrito à Coordenação de TI.
    1. A infraestrutura do cabeamento lógico (dados e voz) deve ser instalada conforme orientações das normas da ABNT específicas.
    2. Os cabos lógicos (dados e voz) existentes na infraestrutura devem ser identificados de forma única.
- As áreas onde estão instalados os recursos computacionais considerados críticos para o atendimento dos objetivos do órgão devem possuir sistema de ar-condicionado separado das demais instalações e manterem uma climatização apropriada para este tipo de recurso.

4.7. SISTEMAS DE ENERGIA

- Os circuitos elétricos do órgão devem ser dimensionados para suportarem a demanda de consumo de energia.
- Os circuitos elétricos devem ser divididos conforme as características do tipo e porte dos equipamentos a eles conectados.

- Os circuitos elétricos devem possuir mecanismos de bloqueio aos seus quadros e painéis de controles sendo que o acesso a eles deve ser restrito à área responsável por sua manutenção ou administração.
- Os circuitos elétricos devem ser providos de geradores de energia e no-breaks como forma de contingência no fornecimento de energia aos recursos computacionais considerados críticos, de maneira a garantir a continuidade dos objetivos da entidade.
    1. Estes sistemas de contingência do fornecimento de energia devem ser verificados, pelo menos, quinzenalmente quanto ao seu funcionamento e sua fonte de energia, tais como óleo diesel e níveis de bateria.
    2. Simulações de chaveamento entre os sistemas de fornecimento de energia devem ser realizadas mensalmente.
- Os circuitos elétricos que fornecem energia para os recursos computacionais considerados críticos devem ser estabilizados e separados dos demais circuitos elétricos nas instalações do órgão.

4.8. CONTROLE DO ACESSO LÓGICO

- O acesso lógico à rede local somente deve ser disponibilizado por meio da utilização de mecanismos de autenticação dos usuários, de forma única e intransferível.
- Um processo de concessão e revogação das permissões de acesso à rede local deve ser elaborado, mantido e revisado periodicamente pela Coordenação de TI.
- Para cada usuário do órgão deve ser disponibilizada somente uma conta de acesso à rede local. Esta conta deve permitir a identificação do usuário de forma única, pessoal e intransferível.
    1. Nos casos dos usuários responsáveis pela administração dos recursos computacionais é facultada a disponibilização de uma conta alternativa para a realização exclusiva de tais tarefas. Esta conta também deve possibilitar identificar o usuário de forma única, pessoal e intransferível.
- A rede local deve conter mecanismos que permitam identificar e rastrear os endereços de origem, destino, e serviços utilizados pelos usuários.
- Os recursos computacionais considerados críticos para os objetivos estratégicos da organização devem ser configurados de forma a registrarem, em arquivo de *log*, os

eventos relevantes realizados pelos usuários. O grau de detalhamento das informações a serem gravadas deve ser definido pela Coordenação de TI juntamente com o respectivo Gestor da informação.

5. CICLO DE GESTÃO DE RISCOS

Órgãos governamentais lidam com informações de aspecto valioso já que está submetido a órgãos superiores a ele tais como a presidência da republica e por lidar com informações de vital importância ao país.

5.1. NORMAS REFERENCIADAS

As normas citadas abaixo foram usadas para desenvolver esta seção:

- ABNT NBR ISO/IEC 27001:2006 – Norma brasileira que contém os requisitos embasados em técnicas de segurança para implementar um SGSI
- ABNT NBR ISO/IEC 27002:2005 – Norma brasileira que especifica o código de prática para a gestão da segurança da informação
- ISO/IEC 27003:2010 – Padrão internacional que normatiza técnicas de segurança e serve como um guia de implementação de um SGSI
- ABNT NBR ISO/IEC 27005:2008 – Norma brasileira que contempla técnicas de segurança atuando na área de gestão de riscos de segurança de informação

5.2. IDENTIFICAÇÃO DOS RISCOS

Tudo aquilo que possui valor dentro destas entidades são ativos. Calcado na estrutura atual destas entidades, encontram-se, na Tabela 5.1, os seguintes ativos e ameaças envolvidos no processo de envio de e-mails:

Tabela 5.1: Relação de ameaças e ativos no ambiente de e-mail

Ameaças/Ativos	Servidor	Pessoas	Dados do e-mail	Sala Cofre
Fraude no envio de mensagens	X	X	X	
Violação e acesso dos dados	X	X	X	
Servidores mal configurados		X		
Falta de monitoramento	X	X		X
Fenômenos naturais				X
Dano a imagem da organização		X	X	
Acesso indevido ao servidor		X		X
Ataques no serviço de e-mail		X		
Falha de hardware	X			
Queda de desempenho		X	X	
Códigos Maliciosos		X		

Tabela adaptada de [47]

A identificação de riscos é uma etapa contínua, pois novos riscos podem aparecer durante o ciclo da analise de riscos. Logo, esta não é a única etapa que sofre revisões e consultas durante o processo de análise.

Os riscos que foram identificados no contexto citado foram os seguintes:

5.2.1. REPÚDIO

A falta de autenticação no serviço de correio eletrônico pode trazer consequências devastadoras, uma vez que qualquer usuário pode configurar o cliente de e-mail para poder se passar por outra pessoa, violando a autenticidade, que é um dos princípios básicos de segurança. Em alguns casos há como comprovar a origem.

Principal Impacto: Perda de credibilidade da imagem da empresa.

5.2.2. CONFIDENCIALIDADE

A ausência de criptografia oferece, a usuários mais avançados, espaço para aproveitar de alguma vulnerabilidade ao meio de comunicação para, desta maneira, realizar a "escuta" do mesmo. Assim, este usuário pode capturar a informação que percorre ao longo do caminho em texto plano, e a utilizar de maneira ilegal ou para benefício próprio.

Principal Impacto: Vazamento de informações

5.2.3. INTEGRIDADE

Uma mensagem eletrônica pode alcançar o seu destino modificada uma vez que ocorre algum tipo de ataque, caso mecanismos de autenticação no ambiente de correio eletrônico não sejam aplicados. Neste risco citado, ataques conhecidos como "*man in the middle*" são bastante utilizados e são eficazes.

Principal Impacto: Perda de confiabilidade no serviço de e-mail prestado.

5.2.4. INDISPONIBILIDADE OU PROBLEMA NA ENTREGA DE MENSAGENS

Sem o simples monitoramento fica impossível saber quem está invadindo e quando ocorreu o incidente com exatidão, dificultando a aplicação de um tratamento. Outro malefício é a não mensuração do ambiente. A falta de informações a respeito da quantidade de e-mails enviados no ambiente, o tamanho das mensagens, a quantidade de spams e mensagens com códigos maliciosos são indispensáveis para prever se este serviço está tendo um bom desempenho.

Principal Impacto: Prejuízo nas transações envolvidas no processo do negócio.

5.2.5. QUEDA DE ENERGIA E OU EFEITOS CLIMÁTICOS

O meio físico que o servidor de e-mail está inserido deverá ser protegido de riscos provenientes de fenômenos naturais e outros tais como: o abastecimento de energia, a

umidade e temperatura da sala cofre e demais problemas que possam afetar o bom funcionamento do hardware neste ambiente. A aplicação de soluções de alta disponibilidade que envolvam no-breaks e geradores de energia devem ser estudadas.

Principal Impacto: Prejuízo nas transações envolvidas no processo de negócio do órgão.

5.2.6. PROPAGAÇÃO DE VÍRUS

Um software antivírus deverá ser contemplado em uma estrutura de serviço de e-mails. Seu objetivo é verificar o e-mail e reparar ou eliminar a mensagens contaminadas, bem como alertar o usuário no caso de existência de algum link externo na mensagem que possa vir a acessar algum *malware*. É bastante recomendado sempre estar com a versão do banco de dados do antivírus atualizada.

Principal Impacto: Prejuízo aos dados das caixas postais e perda de performance do serviço de e-mail.

5.3. ANÁLISE E AVALIAÇÃO DOS RISCOS

De acordo com Peter Drucker, o qual foi um escritor, professor e consultor administrativo, e sua conhecida frase “Se você não pode medir, não pode gerenciar” no âmbito da administração, relata que onde não existe mensuração não se pode gerenciar algo. Portanto, para fazer a análise do risco é necessário primeiro adotar os critérios de risco que servirão de base para análise. Então, serão percorridos os seguintes passos:

- Observar os eventos – As ameaças são eventos que ocorrem periodicamente e, desta forma, devem ser criadas métricas para observação e quesitos que serão utilizados na etapa de avaliação.
- Probabilidade – Este passo serve para contabilizar e relacionar, tanto os eventos quanto as consequências de um risco. É a etapa que permite a mensuração dos riscos, facilitando a identificação de níveis graves a leves e ou aceitáveis.
- Consequências – O evento em geral produz efeitos, sendo eles possíveis em qualquer esfera, como gerencial ou computacional. Essas consequências devem ser observadas e métricas devem ser atribuídas para serem usadas na etapa de avaliar os riscos.

Na determinação de níveis de risco, o processo é consolidar rótulos para cada grau de criticidade, ou seja, nomear. As escalas abaixo retratam suas probabilidades de acontecerem e seus rótulos.

5.3.1. ESCALA DE PROBABILIDADE

A Tabela 6.1 relaciona a situação do ambiente de mensageiria eletrônica a qual o serviço de e-mail está propenso a ocorrer falhas. Sua mensuração é realizada por uma determinada quantidade de horas e, dependendo do intervalo de tempo de ocorrência das falhas, é atribuído um valor que classifica a probabilidade da referida falha.

Tabela 6.1: Classificação da probabilidade de um ativo

Probabilidade da Falha	Taxa de Ocorrência da Falha	Valor
Muito Alta: A falha praticamente inevitável	1 em 24 horas	5
Alta: Falhas Frequentes	1 em 168 horas	4
Moderada: Falhas Ocasionais	1 em 744 horas	3
Baixa: Relativamente Pouca Falha	1 em 4380 horas	2
Remota: Falha Improvável	1 em 8.760 horas	1

Adaptada de [48]

5.3.2. ESCALA DE SEVERIDADE

A Tabela 6.2 apresenta uma escala de severidades de uma falha de acordo com o grau do impacto causado por ela. Quanto maior o impacto causado no serviço ofertado maior o grau estabelecido para a falha.

Tabela 6.2: Classificação da severidade de um ativo

Efeito	Severidade do Efeito	Valor
Muito Alto	Ameaça de grande interrupção na infraestrutura de TI atingindo de forma geral o negócio e a imagem corporativa, envolvendo a não conformidade com a legislação governamental. Passível a prisão, demissão, multas e advertências estabelecidas pela Constituição.	5
Alto	Ameaça de grande interrupção na infraestrutura de TI atingindo	4

	parcialmente o negócio corporativo	
Moderado	Ameaça de interrupção em algum ativo. O usuário sente alguma insatisfação. Defeito notado pela maioria dos usuários.	3
Baixo	Ameaça de pequena interrupção em algum ativo. Uma parte do processo de ser retrabalhada envolvendo outros processos do negócio. Defeito notado por alguns usuários	2
Muito Baixo	Ameaça que não afeta a performance de algum ativo e não prejudica o processo envolvido com o mesmo.	1

Adaptada de [48]

5.3.3. ESCALA DE RELEVÂNCIA

A relevância diz respeito ao tamanho da importância estratégica cujo um ativo está inserido. Um grande exemplo disso é uma entrada única de link na empresa. Caso o cabeamento par trançado que venha do switch de fibra até o firewall da empresa apresente algum problema significa queda da conexão com a internet de toda empresa. Veja que outros tipos de cabeamentos existentes entre outros servidores podem não apresentar a mesma relevância que o exemplo citado. Portanto, a Tabela 6.3 especifica critérios para classificar os níveis de relevância.

Tabela 6.3: Classificação da relevância de um ativo

Relevância	Relevância do ativo para o negócio e a organização	Valor
Muito Alto	A área afetada do ativo para a organização e a visão do negócio é muito alta.	5
Alto	A área afetada do ativo para a organização e a visão do negócio é alta.	4
Médio	A área afetada do ativo para a organização e a visão do negócio é média	3
Baixo	A área afetada do ativo para a organização e a visão do negócio é baixa	2
Muito Baixo	A área afetada do ativo para a organização e a visão do negócio é muito baixa	1

Adaptada de [48]

5.3.4. NÍVEL DO RISCO

Por meio da multiplicação das variáveis probabilidade, severidade e relevância pode-se adquirir um valor que, segundo a *Modulo Security S.A*, identifica o nível de risco que um ativo está sujeito. A Tabela 6.4 representa os graus de risco consoante a instituição citada.

Tabela 6.4: Nível do risco de um ativo

Risco = Probabilidade x Severidade x Relevância (Fórmula PSR)		
Relevância	**Interpretação e ações a serem tomadas**	**Índice de nível variado**
Muito Alto	A área afetada do ativo para a organização e a visão do negócio é muito alta.	60,64,75,80,100,125
Alto	A área afetada do ativo para a organização e a visão do negócio é alta.	32,36,40,45,48,50
Médio	A área afetada do ativo para a organização e a visão do negócio é média.	18,20,24,25,27,30
Baixo	A área afetada do ativo para a organização e a visão do negócio é baixa.	8,9,10,12,15,16
Muito Baixo	A área afetada do ativo para a organização e a visão do negócio é muito baixa.	1,2,3,4,5,6

Adaptada de [48]

Tendo como fonte as escalas apresentadas, podemos calcular o nível do risco a qual os ativos da organização estão sujeitos.

Desta forma, foram estabelecidos cinco níveis de risco, onde aquele que apresenta o maior o valor do índice do risco está propenso a ocorrer e causar efeitos devastadores no órgão analisado.

5.4. TRATAMENTO DOS RISCOS

O primeiro passo nesta etapa consiste na identificação do contexto que será tratado, em um universo bastante extenso, esta etapa será possivelmente a mais lenta e que poderá gerar logo de início um desgaste, provocando em muitos casos um índice elevado de insucesso.

5.4.1. PLANO DE TRATAMENTO DOS RISCOS

Após análises e avaliações dos riscos, a entidade governamental deverá considerar que riscos altos e gravíssimos devam ser tratados. A ordem do tratamento obedecerá a criticidade que o risco apresentar.

Para os demais riscos, almejará transferir os riscos contratando empresas especializadas no assunto, se o orçamento for suficiente ou mitigá-lo ao máximo possível. Serão considerados riscos aceitáveis quando a verba não existir para transferência dos riscos muito específicos ou quando a mitigação tornou o risco aceitável e que não impacte muito no negócio da organização.

5.4.1.1. Penalidades

As infrações que venham a ocorrer seguirão as penalidades decorrentes dos riscos e estabelecidas abaixo:

- Em casos de Gravíssimo: Sansões administrativas severas tendem a processo disciplina.
- Em casos de Alto: Advertência e processos administrativos.
- Em casos Médios: Estudos para reduzir probabilidade e impactos.
- Em casos Baixos: Processo de evolução para reduzir impactos.

5.4.1.2. Metodologias de Análise de Risco

Soluções são possíveis e viáveis para sanar tal problema por isso um plano de segurança se faz necessário e em tal plano é importante constar mecanismos que façam controle seguro das informações tais como:

- Proteção das mensagens contra acesso não autorizado, modificação ou negação de serviço;
- Assegurar que o endereçamento e o transporte da mensagem estejam corretos;
- Que o serviço mantenha-se com confiabilidade e disponibilidade geral;

- O uso de aspectos legais, como, por exemplo, requisitos de assinaturas eletrônicas;
- Aprovação prévia para o uso de serviços públicos externos, tais como sistemas de mensagens instantâneas e compartilhamento de arquivos;
- Níveis mais altos de autenticação para controlar o acesso a partir de redes públicas;
- Hierarquia de importância das informações.

A ISO 27001 recomenda fortemente na página 26 a instituição de tais mecanismos de controle como forma de garantir a autenticidade e proteger a integridade das mensagens nas aplicações, entretanto os mesmos devem ser rigorosamente identificados antes de implementados, já que uma ferramenta mal instalada pode gerar tanto estrago quanto o problema anterior.

Uma mentalidade da segurança se faz necessária no ambiente da entidade governamental, é através do plano SGSI e da política de segurança implantada que os usuários serão instruídos para as boas práticas e do uso correto das ferramentas a eles disponíveis. O e-mail conforme mencionado na problemática do trabalho é um poderoso instrumento que lida tanto com a imagem institucional quanto a pessoal e por isso um rigoroso programa de treinamento e consciência se faz necessário.

Tirando o lado humano, a parte técnica não pode ser deixada de lado, é de primordial importância que sejam aplicados mecanismos de certificação digital e criptografia para os usuários, assim evitando os riscos já mencionados anteriormente tanto como a padronização dos processos através de documentação oficial da empresa.

A ciência dos funcionários aos papéis e responsabilidades pela segurança da informação, já que é esperado deles a colaboração na documentação exigida de acordo com a política de segurança da informação da organização.

Assim como deve ficar claro que os dados das mensagens de trabalho (e não pessoais) devem ser mantidos sob sigilo e não divulgadas para pessoas estranhas ao processo.

5.4.1.3. Treinamento de usuários

Os usuários do serviço de mensagens, relacionados como ativos, devem antes de operar o sistema, possuir conhecimento sobre os tipos de classificação da informação, como também a capacidade de classificar as mensagens que serão manipuladas e ou produzidas pelo próprio.

Este conhecimento deve ser revisto através de um ciclo de treinamento geralmente definido como reciclagem ou atualização.

O sistema deve ser capaz de automaticamente exigir do usuário a autenticação, este requisito é necessário em todos os tipos de classificação da informação, pois todos os dados produzidos devem ter seus devidos autores identificados, desta forma será reduzido ao máximo o trafego de informações sem autoria.

O usuário deve ser capacitado a operar o sistema de correio eletrônico com os mecanismos de segurança para garantir a si próprio fatores de segurança. Alguns fatores que serão transmitidos a todos que participam da sua rede de comunicação geram segurança tais como a autenticação, é possível garantir autoria, a cifragem, confere a integridade, com a junção de ambos temos o não repúdio, com registro de tempo, teremos à hora exata da transmissão da informação. Estas características devem ser apresentadas aos usuários como benefícios, reduzindo o fluxo de papéis, aumentando a confiança no serviço, dentre outras qualidades.

Os integrantes do sistema de e-mails, por ser um ativo do contexto, devem ser motivados a entender que a correspondência eletrônica trafegada faz parte de todo o conhecimento acumulado pela instituição e que em muitas vezes deve ser gerenciada para não haver o mau uso desta informação, para isto já é feito uma triagem que pretende realizar o filtro e reduzir *spams* e endereços de e-mail falsos.

Após o devido treinamento dos usuários, os mesmos estarão aptos a trafegar informações com maior segurança, visto que estas antigamente aconteciam por meio de correspondências de cartas pelos correios, garantido que ele saberá gerenciar os e-mails recebidos e enviados e erradicar a impressão indevida de dados.

A Figura 7.1 sugere um plano para treinamento e aperfeiçoamento, não somente de todos os usuários do serviço de mensagens eletrônicas, mas também contempla os gestores e gerentes ligados a solução.

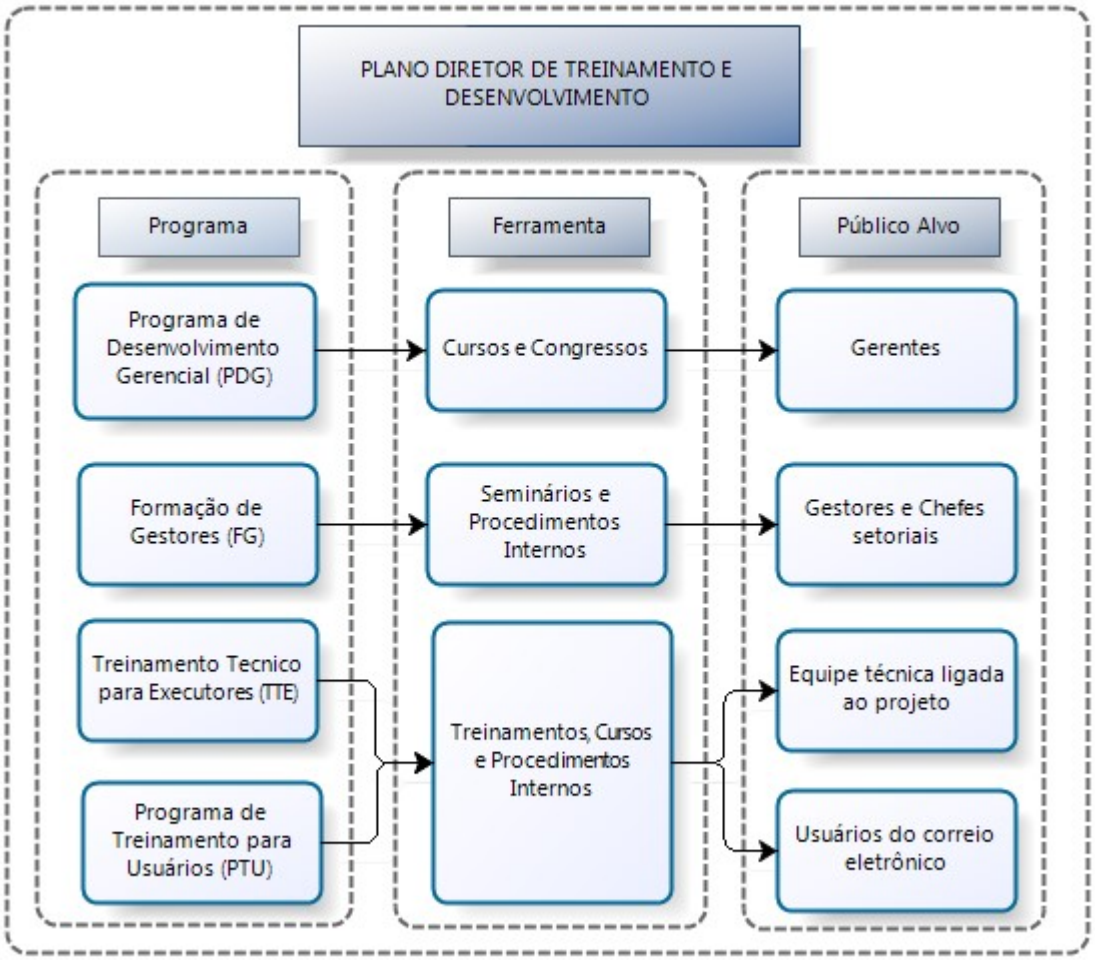

Figura 7.1: Plano diretor de treinamento e desenvolvimento
Adaptado de [49]

5.4.1.4. Boas práticas e configurações restritivas

Nesta parte, será exibido e explanado o refinamento na configuração do servidor Postfix. Antes de tudo, o primeiro cuidado que se deve ter está atrelado com a versão do programa instalado. É recomendado sempre possuir a ultima versão estável disponibilizada pelo mantenedor por questões de segurança (correções de vulnerabilidades do serviço, falhas de funcionamento, aprimoramentos e etc). Associado a isso, o servidor que abriga o serviço de e-mail deve, também, estar com o seu sistema operacional atualizado e com *patches* de segurança aplicados para evitar impactos no ambiente de e-mail.

O próximo passo é executar backup das informações de e-mail, bem como os arquivos de configuração pertinentes para o bom funcionamento do serviço. As mídias que contenham

esse backup devem especificar a data do backup, a versão corrente do Postfix, nome do servidor e ip do servidor. Além disso, as fitas devem ser armazenadas em uma localidade distante do servidor e resididas de preferência dentro de cofres com intuito de manter cópias de segurança para reposição do dado perdido, caso ocorra alguma catástrofe no ambiente operacional.

Outro ponto que se deve ter cuidado está relacionado ao período de retenção dos backups. Em instituições governamentais, o tempo mínimo de retenção oscila próximo a 6 meses de backup guardados das caixas postais, até mesmo para as contas dos usuários perderam o vínculo com a organização.

A Figura 7.2 esclarece uma troca de mensagem do protocolo SMTP e as restrições cabíveis de serem feitas no Postfix.

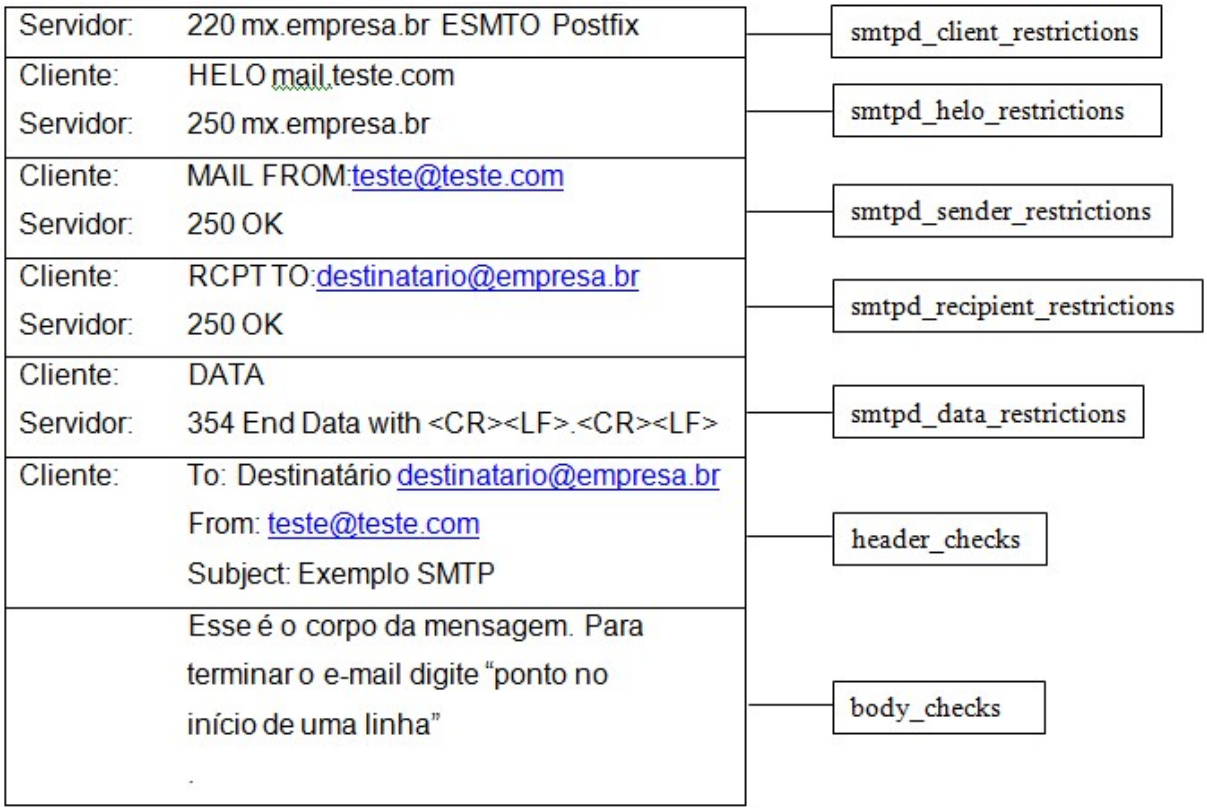

Figura 7.2: Restrições Postfix nos comandos SMTP
[3]

Na seção 8 da monografia, a qual se refere ao experimento, existem diversos exemplos de configurações no servidor Postfix. Tais implementações, que atuam nos contextos da gravura acima, ilustram a importância de aplicação de restrições no protocolo SMTP.

5.4.1.5. Autenticação do protocolo de envio de e-mails

O protocolo SMTP, por padrão, não provê uma camada de autenticação de seus usuários. Facilmente um usuário pode alterar suas informações de remetente sem que o protocolo original SMTP forneça algum mecanismo para bloquear essa vulnerabilidade. Tal problema encontrado vem de afronte a integridade da mensagem a qual é um dos pilares da segurança da informação.

O SASL (*Simple Authentication and Security Layer*) é um *framework* utilizado para provimento de autenticação para diversas implementações de protocolos de aplicação, dentre eles o SMTP, por meio de uma gama de métodos de autenticação conhecidos, sejam estes novos ou velhos. Sua publicação está documentada na RFC 4422. Adicionalmente, essa interface de comunicação entre protocolo de aplicações e mecanismos de autenticação pode fornecer, também, confidencialidade dos dados que são trafegados em seu canal.

O funcionamento básico deste programa consiste em atuar como uma camada abstrata a qual negocia o método de autenticação disponível com qualquer aplicação que faça seu uso. No caso do serviço de e-mail, o SASL auxilia na consulta do remetente de e-mail em uma base especificada na configuração desse programa, base esta que pode ser OpenLDAP, Active Directory, usuário local, Kerberos e etc, e retornar se ele é o dono da conta a qual autenticou no início da sessão no sistema de correio eletrônico.

Alguns softwares, tais como Dovecot e Cyrus e outros, suportam a autenticação do SMTP por meio deste *framework*.

O SASL, para realizar a atividade de autenticação, utiliza de alguns mecanismos que estão citados e comentados abaixo:

- PLAIN

Método que envia o usuário e a senha para autenticação codificada em base64. Esse esquema sozinho não provê criptográfica na autenticação das credenciais do usuário, mas existe a possibilidade deste integrar com o TLS para preencher essa lacuna.

- LOGIN

É um mecanismo não é oficialmente registrado ou suportado. Ele é ainda utilizado por cliente de e-mails mais antigos e provavelmente deverá ser habilitado no seu ambiente para manter o legado com estes tipos de softwares. Esse mecanismo de autenticação funciona da mesma forma que o PLAIN.

- OTP

Este mecanismo significa *one time passwords*. Tal método não fornece compatibilidade com criptografia. Clientes de e-mails devem estar aptos para funcionar com o mecanismo OTP.

- DIGEST-MD5

Funciona utilizando uma chave secreta entre o cliente e o servidor. Essa chave nunca é trafegada pela rede. Através de um sistema de desafio/resposta que utilizam a chave secreta, o cliente criptografa o desafio com sua chave secreta e envia ao servidor. Este faz o mesmo procedimento que o cliente e compara as respostas. Caso sejam as mesmas a comunicação poderá ser realizada. É um método seguro porque a chave propriamente dita não trafega na rede.

- KERBEROS

Kerberos é um protocolo de autenticação de rede largamente utilizado. Caso não utilize o Kerberos na sua rede ele não é necessário, mas se ele é usado este se encaixa muito bem com a sua infraestrutura para autenticar o SMTP.

- ANONYMOUS

Mecanismo que é interessante para alguns protocolos, porém não traz muitos benefícios para o SMTP.

Quando um cliente se conecta com o servidor no ambiente de e-mail, o servidor lista os mecanismos de autenticação suportados por ele em sua ordem de preferência (conforme configurado neste serviço). O cliente tenta pelo primeiro método, e caso falhe, vai seguindo a sequência fornecida pelo servidor. Caso nenhum deles obtenha sucesso, a autenticação resultará em falha.

Cada método de autenticação exige uma especificidade peculiar integrante do mecanismo selecionado. Por exemplo, existem esquemas que requisitam senhas, outros que solicitam informações a cerca do domínio o qual o cliente está inserido e alguns que necessitam de *tickets* Kerberos, certificados e etc. Logo, a flexibilidade produzida por esta camada abstrata facilita bastante no contexto de autenticação e independe do protocolo da aplicação usado.

A Figura 7.3 representa a solução ideal do Postfix com autenticação. Nota-se que existem métodos do SASL que habilitam também a técnica de criptografia para garantir confidencialidade dos dados e proteger o acesso indesejado.

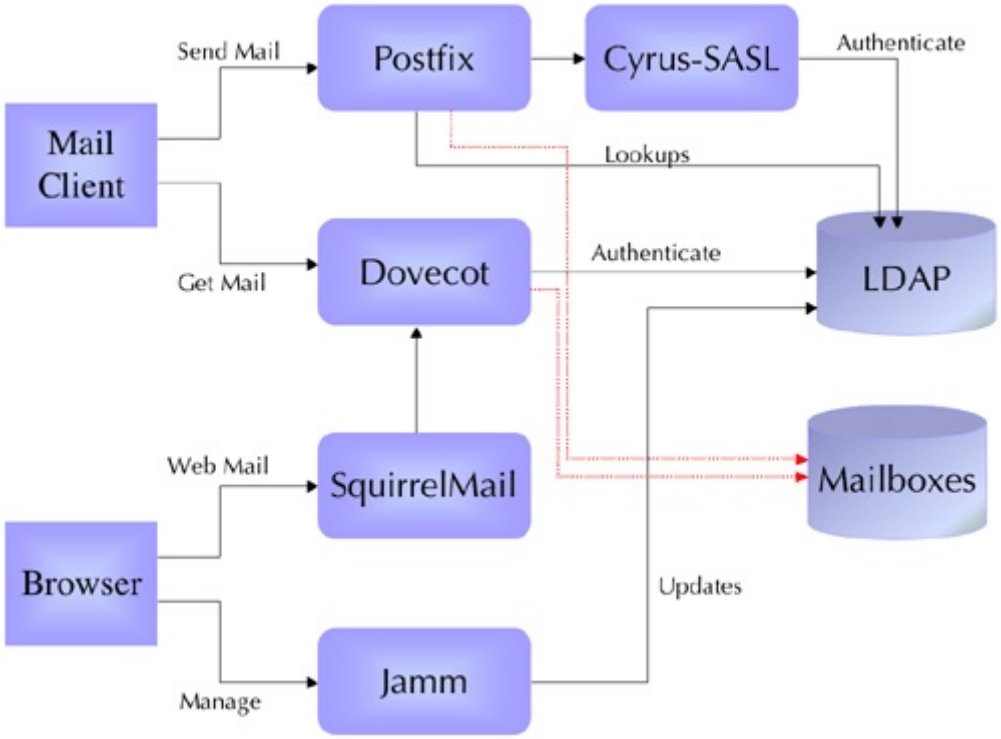

Figura 7.3: Diagrama Postfix com autenticação SMTP via SASL
[41]

5.4.1.6. Criptografia

A criptografia e a autenticação no envio do e-mail são excelentes alternativas encontradas para mitigar os problemas discutidos ao longo do trabalho. No entanto, a utilização das mesmas apenas não assegura que o sistema de correio eletrônico está com um nível de segurança adequado para organizações.

Criptografia é o método de cifrar mensagens para enviá-las de modo cifrado ou em código. Em segurança da informação é usada na atualidade para proteção de dados considerados importantes e ou sigilosos. Visando em principio autenticar a identidade dos usuários, a proteção do sigilo das comunicações sejam elas de cunho pessoal, empresarial ou bancário e por fim proteger a integridade de transferências eletrônicas de fundos.

A criptografia eletrônica se baseia no uso de chaves simétricas ou assimétricas.

A criptografia simétrica usa uma única chave tanto para criptografar quanto para decifrar mensagens. Embora ela seja eficiente e rápida no que diz respeito a codificar e

decodificar dados, o uso ao longo de meios de comunicação que não sejam 100% torna este esquema arriscado, pois um atacante pode capturar a troca de chaves neste canal.

A criptografia assimétrica se viabiliza por meio de mecanismo que contém duas chaves, uma publica que todos os usuários alvo possuem e uma privada que apena uma pessoa possui. Assim, uma cifra gerada com essa chave pública só poderá ser aberta por sua respectiva chave privada. Por meio deste método, o grande problema encontrado no ambiente de criptografia, a distribuição de chaves, encontrou uma maneira segura para usuários criptografarem mensagens.

5.4.1.7. Certificação Digital

O correio eletrônico é largamente utilizado nesta instituição para trafegar informações que muitas vezes são sigilosas e estratégicas para o Governo Federal, daí surge à necessidade de proteger esta ferramenta que é essencial para o bom funcionamento da instituição.

Geralmente, a implementação de sistemas de Certificação Digital não existe no âmbito de diversas organizações. Com isso, a criação, alteração e circulação de documentos de modo fácil geram situações de acessos não autorizados bem como o repúdio e a falta de confiança nas informações tramitadas por este duto de comunicação. Além da possibilidade de acesso indevido a informação ou o próprio furto desta.

Tudo isso põe em risco a credibilidade do uso do e-mail para tráfego de informações relevantes.

O objetivo é aumentar a segurança para os usuários do serviço de mensagens eletrônicas da entidade, dificultando assim o acesso indevido, o extravio e o furto de informações. A implementação de certificação digital promove integridade e autenticidade às informações, impedindo os problemas supracitados e beneficiando não só todos os usuários desta ferramenta, bem como a imagem do órgão do governo federal do Brasil.

Abaixo é exibido um resumo de ativos, levando em conta somente o escopo da Certificação Digital:

- Autoridade Certificadora (AC): É a entidade subordinada à hierarquia da ICP-Brasil, responsável pelo ciclo de vida do par de chaves;
- Configuração dos clientes de e-mails com a finalidade de suportar o uso de Certificação Digital;

- Conscientização dos usuários para que seja incorporada a necessidade de aprimoramento da segurança no uso da correspondência eletrônica;
- Treinamento e conscientização de todos os envolvidos em tarefas de implantação e administração dos certificados digitais.

É necessária a aquisição de hardware e software que ficará dedicado para ser a CA da entidade do governo. A este equipamento apenas o grupo infra citado terá acesso através de uma política forte de senhas e certificados. Este equipamento deve observar os regimentos e normas de segurança para servidores críticos da entidade em questão.

Somente será criado certificado para os funcionários que, de algum modo, manipulam informações classificadas como sigilosas ou críticas. A solicitação deve ter procedência comprovada da chefia ou departamento de pessoal.

Os certificados que por ventura foram de qualquer maneira perdidos, extraviados, furtados ou de algum modo comprometidos, devem ser revogados o mais rapidamente possível. A geração de outro se dará mediante a expressa solicitação do usuário.

A instalação e administração da estrutura de certificação ficam a cargo de um grupo de indivíduos devidamente conscientizados da responsabilidade inerentes ao serviço. Este grupo vai trabalhar em conjunto com os funcionários responsáveis pelo serviço de mensagens eletrônicas, objetivando a maior integração possível entre as equipes de modo a promover o máximo de disponibilidade para a solução final.

É essencial que a equipe que vai trabalhar diretamente com os certificados tenha o devido treinamento técnico para a respectiva função que pretende desempenhar.

Caso o certificado seja de algum modo perdido, extraviado, furtado ou comprometido cabe a seu respectivo dono comunicar ao grupo responsável para que sejam tomadas as medidas cabíveis.

Todos os envolvidos devem assinar um documento de responsabilidade e confidencialidade sobre o próprio certificado. As informações geradas, trafegadas ou visualizadas com o certificado pessoal.

Após devidamente implementado e homologado, todas as mensagem classificadas como sigilosas ou críticas devem trafegar assinadas digitalmente.

5.4.1.8. Divulgação da política de segurança

O propósito dessa política é assegurar o uso apropriado do sistema de mensagens eletrônicas no ambiente do órgão governamental em questão.

Todas as mensagens distribuídas pelo sistema da empresa, até e-mails pessoais, são de propriedade do órgão. O usuário não deve manter quaisquer expectativas de privacidade sobre quaisquer mensagens que crie, armazene, envie ou receba através do sistema de e-mail corporativo.

Todas as mensagens podem ser monitoradas sem prévia notificação caso a chefia julgue necessário. Se existir quaisquer evidências que o usuário não está aderindo às regras citadas nessa política, a entidade governamental se reserva ao direito de tomar medidas disciplinares, incluindo demissão e/ou ação judicial.

A chefia imediata será o canal competente para saneamento de dúvidas e solicitação de auditorias.

É estritamente proibido:

- Enviar ou encaminhar e-mails contendo comentários difamatórios, ofensivos, racistas ou obscenos. Caso o usuário venha receber algum e-mail dessa natureza, o envie no mesmo instante para seu supervisor.
- Encaminhar mensagens ou copiar uma mensagem ou anexo pertencente a outro funcionário sem obter primeiro a permissão desta pessoa.
- Enviar Spam ou “correntes”.
- Forjar ou tentar forjar mensagens de e-mail, ou disfarçar ou tentar disfarçar sua identidade quando enviando um e-mail.

Cuidados necessários:

- Os usuários devem ter os mesmos cuidados em escrever um e-mail quanto em qualquer outro tipo de comunicação escrita seguindo os critérios de classificação dispostos neste SGSI.
- Para evitar fraudes, recomendamos fortemente que seja utilizado o certificado digital em todas as mensagens. Mensagens com informações críticas ou sigilosas devem usar o certificado digital.

Uso Pessoal:

- Apesar do sistema de e-mail da entidade governamental ser para assuntos relacionados ao trabalho, o ela permite o uso pessoal se for necessário e não interferir com o trabalho a ser executado.
- A inserção automática, manual, ou adquirida por qualquer meio, de qualquer endereço eletrônico de usuários do em listas de mala direta, anúncios comerciais, sem prévia autorização de seu responsável (usuário) é terminantemente proibida. Mensagens não reconhecidas pelo usuário serão consideradas como SPAM e deverão ser recusadas pelo sistema. A persistirem as mensagens o usuário deverá notificar a administração dos sistemas e redes para tomar as medidas legais cabíveis.

Isenção de Responsabilidade (*Disclaimer*)

- Todas as mensagens devem finalizar com a seguinte comunicação de isenção:

Aviso 1: 'Esta mensagem é direcionada apenas para os endereços constantes no cabeçalho inicial. Se você não está listado nos endereços constantes no cabeçalho, pedimos-lhe que desconsidere completamente o conteúdo dessa mensagem e cuja cópia, encaminhamento e/ou execução das ações citadas estão imediatamente anuladas e proibidas'.

Aviso 2: 'Apesar de a instituição governamental tomar todas as precauções razoáveis para assegurar que nenhuma virose esteja presente nesse e-mail, o ela não poderá aceitar a responsabilidade por quaisquer perdas ou danos causados por esse e-mail ou por seus anexos'.

5.4.1.9. Padronização dos processos

Os sistemas de e-mail devem primar pela segurança e utilizar SMTP/MIME para o transporte de mensagens. Para acesso às mensagens, devem ser utilizados os protocolos POP3 e/ou IMAP, sendo encorajado o uso de interfaces web para correio eletrônico, observados todos os aspectos de segurança mencionados neste SGSI.

Acesso a caixas postais:

- O acesso à caixa postal deverá ocorrer através do cliente do software de correio eletrônico utilizado. No caso de utilização de outro cliente devem-se considerar as vulnerabilidades de segurança deste software.
- Quando for necessária acessar a caixa postal através de redes não seguras devem-se utilizar HTTPS de acordo com os padrões de segurança de transporte descritos na RFC 2595, que trata da utilização do TLS com IMAP e POP3.

Conteúdo de e-mail:

- O S/MIME V3 deverá ser utilizado sempre que o conteúdo que estiver trafegando seja classificado como sigiloso ou confidencial ou ainda se a informação for estratégica para a organização segundo as RFCs 3369, 3370, 2631, 3850, 3851 e 3852.

Transporte de e-mail:

- No transporte dos e-mails é importante utilizar SPF (*Sender Policy* Framework) nos termos da RFC 4408 de modo a prover maior confiabilidade para as mensagens.

Certificado Digital:

Deve-se utilizar certificado padrão ICP-Brasil para assinatura de e-mail, quando exigido. Em conformidade com o disposto na Medida Provisória nº 2.200-2, de 24/08/2001 e Decreto nº 3.996 de 31/10/2001.

5.4.1.10. Aspectos legais e éticos

Os aspectos legais compreendem elementos importantes para o sucesso do SGSI, pois eles regem as obrigações das organizações, determinam as responsabilidades, definem as penalidades, delimitam os limites de atuação e criam as proteções legais, além de proporcionarem oportunidades de negócios. (Harris, 2004)

No âmbito da administração pública federal brasileira, encontramos o Decreto nº 4.553 de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, o qual determina, por exemplo, que "para a guarda de documentos ultrassecretos e secretos é obrigatório o uso de cofre forte ou estrutura que ofereça segurança equivalente ou superior, (...), e na impossibilidade de se adotar o disposto, os documentos ultrassecretos deverão se mantidos sob guarda armada" (BRASIL, 2002, art. 30).

De acordo com Pinheiro (2007), os aspectos legais contribuem para identificar os limites de ação da Gestão da Segurança da Informação, principalmente nos processos de auditoria, na criação de políticas de aceitação de uso, nas investigações de fraudes e de outros incidentes. Dado que as garantias de privacidade e sigilo de informações pessoais são regidas por leis, a GSI deve compreendê-las para evitar invasões ou danos legais que prejudiquem os negócios das organizações.

6. EXPERIMENTO

O experimento que será disposto abordará duas estruturas de mensageiria eletrônica.

A primeira conterá uma configuração padrão de correio eletrônico, conforme é bastante visto em instituições governamentais.

Uma segunda solução de e-mail será exibida contendo as configurações restritivas de SMTP, POP3 e IMAP associadas com autenticação do protocolo SMTP, característica que não é disponível por padrão do protocolo, e também, criptografia nos protocolos de recepção e envio de e-mail com intuito de garantir a confidencialidade da informação trocada.

Ao construir os ambientes propostos, uma analogia entre as estruturas deverá ser apresentada destacando os critérios da informação ganhos, vulnerabilidades de ataques suscetíveis e outros quesitos relevantes.

6.1. RECURSOS DE INFRAESTRUTURA

O experimento será composto de 2 ambientes de e-mail, onde cada uma conterá 2 máquinas virtuais, sendo a primeira o servidor Postfix e Dovecot para fornecimento do serviço de correio eletrônico e a segunda realizando o papel de uma estação de trabalho com cliente de e-mail para fazer a comunicação com o servidor e executar a tramitação de mensagens eletrônicas.

As máquinas virtuais servidor compartilhará do host físico um processador, memória de 768 MB de memória randômica (RAM), disco rígido de 20 GB e 2 interfaces de rede, onde a primeira tem acesso apenas à rede local para comunicação com o cliente, e, a segunda disponível para comunicação com a internet.

As máquinas virtuais cliente compartilhará do host físico um processador, memória de 512 MB de memória randômica (RAM), disco rígido de 20 GB e 2 interfaces de rede, onde a primeira tem acesso apenas à rede local para comunicação com o servidor, e, a segunda disponível para comunicação com a internet.

6.2. SISTEMA OPERACIONAL

Antes mesmo da instalação do sistema operacional, atividades como atualização de firmware dos dispositivos, configuração da rede de gerência (funcionalidade que é independente do sistema operacional e serve para administração remota e exibição de informações a respeito do estado da máquina) e configuração do RAID devem ser feitas a fim de garantir a segurança e disponibilidade da informação.

O RAID (*redundant array* independent disks) é a metodologia que objetiva fornecer tolerância a falhas de discos e dados através de duas maneiras distintas, ou por hardware ou por software. O RAID por software oferece mais flexibilidade em sua construção porque discos, partições e outros elementos podem ser utilizados na composição desta estrutura de redundância. Porém, sua configuração é mais complexa e apresenta menos desempenho do que a outra modalidade. No RAID por hardware, como é implementado por firmwares de controladoras RAID, apresenta uma enorme performance e sua configuração é bem simplória.

Dentro das diversas modalidades de RAID, deve-se escolher aquela que dispõe de redundância de dados e bom desempenho para o serviço de correio eletrônico trabalhar de maneira otimizada. Tais características são adquiridas nos modos RAID 1, RAID 3, RAID 5 e RAID 10. A informação sobre os tipos de RAID mais usados são expostas na Tabela 8.1 abaixo:

Tabela 8.1: Tipos de RAID mais usados e características

Tipo	Descrição
RAID 0	Consiste em agregar 2 ou mais HDS para se obter mais performance tanto na leitura ou na escrita. Os dados são subdivididos em faixas e cada faixa é armazenada em um HD diferente simultaneamente. Neste modo o ganho é alta velocidade de escrita e leitura. Porém, neste modo não há discos de paridade.
RAID 1	Agrega 2 discos com objetivo de espelhamento, ou seja, existe um *array* de disco para dados e outro *array* com uma cópia idêntica do *array* principal. A redundância a característica principal deste tipo, mas seu usar a funcionalidade conhecida como paridade. Outra dificuldade está associada ao aumento no tempo de escrita dos dados.
RAID 3	São necessários 3 discos ou mais para construir esse modo. Os dados são

	gravados em todos os discos com exceção do último que fica incumbido exclusivamente para guardar a paridade dos dados inseridos nos outros HDs. Esta modalidade oferece leitura e escrita rápida, controle de erros e tolerância a falha de um disco. Mas como ponto negativo esse modo possui a vulnerabilidade de ter um disco único de paridade.
RAID 5	Necessita de 3 HDs ou mais. Todos os discos presentes armazenam dados e as informações de paridade, que fica alterando sua localização de um disco para outro de forma homogênea, evitando assim a vulnerabilidade vista no RAID 3. Esse modo oferece leitura rápida, controle de erros e tolerância a falha de um disco. Porém, sua desvantagem é que a escrita não é tão rápida quanto à leitura.
RAID 6	Padrão novo adotado por algumas controladoras RAID. Trabalha do mesmo modo que o RAID 5, diferindo-se apenas que oferece em dobro a quantidade de informações de paridade, ou seja, suporta falha de até 2 HDs.
RAID 10	4 discos ou mais são requeridos para compor este RAID. Ele é uma mescla do RAID 1 (*mirroring*) e RAID 0 (*striping*). Com este modo, é ganho redundância e performance, porém o custo para a escrita e a alta quantidade de HDs para sua formação são problemáticas encontradas. A característica de paridade não é implementada em sua redundância.

Dados adaptados de [32]

Uma vez aplicadas soluções, o próximo passo é escolher um sistema operacional que seja condizente com o esquema de segurança almejado por este serviço. Logo, o sistema operacional instalado nas máquinas virtuais de provimento do serviço correio eletrônico será o CentOS. A escolha deste sistema ocorreu devido à compatibilidade com o programa Postfix adicionada à alta robustez e segurança deste sistema operacional uma vez que tal sistema é uma versão com alterações da distribuição Linux conhecida como Red Hat.

O sistema operacional instalado nas máquinas virtuais clientes de correio eletrônico será o Windows XP. Esse sistema foi selecionado por ser econômico devido ao baixo consumo de recursos gráficos aliado com a facilidade de uso da maioria geral dos usuários. Com este software podemos simular a situação real dos usuários, uma vez que, quase em sua maioria, as estações de trabalho usam esse software Microsoft.

Um fator crítico de sucesso no oferecimento de um serviço é a ligação intima com o provimento de uma plataforma anterior ao serviço, o sistema operacional, se apresentar segura em sua funcionalidade. Portanto, para finalidades de segurança da informação, a escolha de

um sistema operacional e sua versão é um quesito que deva ser estudado com bastante cautela.

6.2.1. Particionamento de disco

O servidor de correio eletrônico apresentando no experimento será, também, o mesmo que armazenará as caixas postais. Logo, ao fazer o particionamento do disco, deve-se levar em conta o tamanho do sistema de arquivo que abrigará os arquivos de e-mails dos usuários.

No experimento realizado, os servidores dispõem de uma pequena capacidade de armazenamento de 20 GB de disco rígido, as quais foram entregues integralmente para a raiz (/). A divisão desejável para um bom particionamento de disco em um ambiente de produção escalável pode ser acompanhada na Tabela 8.2:

Tabela 8.2: Particionamento de disco do servidor

Filesystem	Tamanho Mínimo	Comentário
/ (Raiz)	15 GB	Esse *filesystem* armazena toda a estrutura de arquivos do Linux, e, além disso, será o mesmo *filesystem* que conterá a instalação dos programas instalados na máquina.
/home ou /var	De 80% a 90% do armazenamento disponível	As caixas postais dos usuários podem ser configuradas no /home ou /var. Portanto, o local que for escolhido deve possuir uma grande área disponível para armazenamento das mensagens eletrônicas.
/scripts	De 5 GB a 10 GB	Local idealizado para residir scripts para administração do serviço de mensageiria, bem como armazenamento de pequenos arquivos ou pacotes relativos ao servidor de e-mail. Esse *filesystem* é opcional.
/var	De 20 GB a 30 GB	Caso as caixas postais estejam localizadas no /home, o *filesystem* /var deve ser criado com intuído de armazenar os arquivos de logs do sistema e serviço de

		e-mail, além dos demais arquivos importantes para o funcionamento do sistema que se encontra nesse diretório.

A criação de uma área destina para swap deve ser lembrada na hora do particionamento do disco. Como não existe mais uma regra para o tamanho da área de swap, um tamanho mínimo de 8 GB é suficiente para ser usado caso a memória RAM seja exaurida pelo sistema operacional. A área de swap pode ser criada como uma partição ou como um arquivo, sendo a segunda opção o modo mais desejável para a não ocupação da tabela de partições do sistema operacional.

6.2.2. Sistema de arquivos

O sistema de arquivos é a maneira estruturada a qual o sistema operacional armazena os arquivos no disco rígido. O sistema de arquivos mantém atualizados os metadados dos arquivos, informações essas cruciais para que o sistema operacional tenha total controle em suas operações de manipulação (leitura, escrita, exclusão) dos dados.

O sistema de arquivos almejado na estrutura de e-mail deve ser selecionado para ofertar um bom desempenho e segurança no armazenamento, leitura e busca de dados no servidor. Dentre os sistemas de arquivos encontrados, o ReiserFS, ext3, ext4 e NTFS são os mais indicados para desempenhar este papel. O sistema de arquivo adotado nos ambientes de experimento foi o ext4, pois provê um excelente desempenho e se integra bem com o ambiente Linux do servidor.

6.3. PRIMEIRO AMBIENTE

Os requisitos dispostos neste ambiente visam simular a situação real de ambiente de mensageiria eletrônica encontrada em diversas instituições governamentais. Este cenário proverá os protocolos de recepção (POP3 / IMAP) e envio de e-mail (SMTP) aos seus usuários, porém não contemplará a utilização de cifras, nem a autenticação do protocolo SMTP, autenticação está que não vem disposta por padrão neste protocolo.

Configurações e ajustes executados nesta estrutura ocorrerão focados apenas no provimento do serviço, ou seja, configurações adicionais de segurança, recomendações de RFC e boas práticas não serão aplicadas.

As instruções dispostas nas seções abaixo deverão, também, ser aplicadas no segundo ambiente, pois as informações aqui presentes são essenciais para o serviço de e-mail entrar em vigor.

6.3.1. Instalação do Postfix

Uma vez de posse do sistema operativo instalado e apto para uso (hostname, ip, dns, arquivos de host configurados), o passo posterior é instalar o programa que disponibiliza o serviço de correio eletrônico, dependências e programas auxiliares segundo visto no Quadro 4.

Quadro 4: Instalação dos programas

```
# yum install postfix dovecot httpd php php-imap squirrelmail
openssl awstats
```

Com o comando acima, a máquina busca nos repositórios ativos, localizados no diretório /etc/yum.repos.d, os pacotes referenciados após a diretiva install e os instala no host. Caso o pacote já esteja instalado e a versão do software encontrada no repositório for superior que a da máquina corrente, o servidor faz a atualização dos mesmos na máquina.

Além disso, com este comando, as dependências de cada pacote informado são procuradas nos repositórios ativos e são instalados no sistema local.

Os pacotes referenciados na linha destacada acima são essenciais para o servidor de correio eletrônico e tem a seguinte relevância no ambiente de e-mail:

- Postfix => Servidor SMTP responsável pela entrega de e-mails entre MTAs.
- Dovecot => Servidor POP3 / IMAP responsável por sincronizar conexões de recepção de mensagens via download / acesso.
- Httpd => Servidor de aplicação onde será abrigada a aplicação de acesso a e-mails através do browser.
- Php e php-imap => Módulos do apache necessários para interpretação da linguagem php usada pelo software de webmail.

- Squirrelmail => Software webmail que funciona sobre o servidor de aplicação e provê mais uma alternativa de acesso aos e-mails sem requerer um programa cliente de e-mail.
- Openssl => Programa fundamental para provimento de criptografia para garantir a confidencialidade da informação
- Awstats => Responsável por gerar informações estatísticas do correio eletrônico baseado em scripts pearl.

6.3.2. Arquivos de configuração

Os principais arquivos de configuração do programa Postfix estão localizados no diretório /etc/postfix. Dentre eles, os crucias a para levantamento do serviço são o main.cf e virtual e devem ser customizados obrigatoriamente. As suas atribuições destes são, respectivamente, fornecer todos os parâmetros globais para funcionamento adequado do Postfix e oferecer uma tabela de alias para os endereços de e-mail.

Outro arquivo de suma importância no Postfix é o master.cf. Sua incumbência é controlar todos os daemons utilizados pelo programa, bem como parâmetros pertinentes para a execução correta destes.

Antes de se começar a configuração, é recomendado por administradores Linux experientes fazer uma cópia de segurança do arquivo a ser manipulado. Um exemplo dessa tarefa pode ser feita com o comando visto no Quadro 5:

Quadro 5: Cópia de segurança do arquivo original

```
# cp /etc/postfix/generic /etc/postfix/generic_ORIG
```

Outra boa prática realizada caso não existe um arquivo de configuração padrão ou este foi bastante alterado consiste em copiar o arquivo exemplo encontrado geralmente no caminho /usr/share/doc/nome_do_programa. Geralmente, todo pacote instalado, por padrão, gera esses arquivos.

O main.cf é um arquivo o qual suporta diversas customizações por meio de suas centenas de linhas. Todas elas contêm um valor padrão sensato o que facilita e agiliza o trabalho do administrador do serviço. Dependendo do tipo do ambiente, basta manipular apenas 3 linhas deste arquivo para o servidor SMTP esteja apto para execução do seu trabalho.

O Quadro 6 contém todas as configurações necessárias para dispor o serviço de SMTP deste ambiente.

Quadro 6: Configuração do arquivo Main.cf do Postfix

```
1. myhostname = mx1.empresa.br
2. mydomain = empresa.br
3. mydestination = $myhostname, localhost.$mydomain, localhost
4. smtpd_banner = Servidor de e-mail da empresa.br
5. mynetworks = 192.168.1.0 / 24
6. inet_interfaces = all
7. inet_protocols = ipv4
8. home_mailbox = Maildir/
9. virtual_alias_maps = /etc/postfix/virtual
```

A primeira alteração consiste na identificação do host do servidor de e-mail. Nas linhas 1, 2 e 3 do Quadro 6 encontram-se esses parâmetros preenchidos.

O *myhostname* é adquirido por meio da função *gethostname()* fornecida pelo sistema operacional. Porém, este valor se obrigatório uma vez que o servidor em questão não apresentar seu nome no padrão FQDN.

O campo *mydomain* apresenta o nome do domínio da máquina local. Ele pode ser preenchido através da função *gethostname()*, desde que o seu retorno apresente o modo FQDN, com a subtração do primeiro termo. O parâmetro em questão dispõe da funcionalidade de suportar múltiplos domínios e eles devem ser delimitados por uma vírgula.

O parâmetro *mydestination* especifica a lista de domínios que a máquina usará para fazer a entrega final. Em caso de um domínio único, informações do hostname e suas referências de *localhost* devem ser feitas segundo exposto na linha 3 do Quadro 6.

O banner do servidor SMTP pode ser personalizado por meio da configuração exibida na linha 4 exibida no Quadro 6. A exibição do banner acontece sempre quando um cliente se conecta ao servidor SMTP.

O próximo passo é especificar as informações de rede. As linhas 5, 6 e 7 dispõem essa configuração no Quadro 6.

O valor informado no parâmetro *mynetworks* exibe uma lista dos clientes SMTP confiáveis que possuem mais privilégios que estranhos. Sumariamente, esta configuração possibilita que apenas clientes SMTP pertencentes à rede informada tenham permissão de fazer envio de mensagens. Sua implantação se torna muito importante no campo da segurança da informação porque, sem sua aplicação, máquinas externas a rede podem utilizar desse *relay* aberto do servidor para disseminar SPAMS, o que pode ocasionar a entrada deste servidor em uma *blacklist* de e-mails.

Já no campo *inet_interfaces* é responsável por informar qual interface de rede o Postfix usará da máquina local. Por padrão, a informação "*all*" já vem inserida nesse parâmetro.

Por fim, o ultimo parâmetro exibido na linha 7 informa qual a versão do protocolo IP o Postfix estará apto a trabalhar. O padrão é definido como "all", porém, como no ambiente do experimento faz apenas uso de IPv4, o valor "IPv4" foi configurado.

O modo o qual são armazenados as mensagens de e-mail são propiciados de duas formas distintas. Elas foram discutidas na seção 3.8.1 que retrata a arquitetura do Postfix, e sendo assim, de acordo com os benefícios adquiridos com a utilização de uma estrutura de diretórios, a linha 8 mostrou sua configuração como *Maildir* ao invés de *Mailbox*.

O parâmetro *virtual_alias_maps* apresenta uma tabela contendo um direcionamento para as contas locais ou remotas. Em suma, sua proposta é:

- Redirecionar um e-mail para um ou mais endereços
- Redirecionar um e-mail para endereços de outros domínios.

Nestes próximos parágrafos será abordado a respeito do software de entrada de mensagens eletrônicas. O Dovecot foi selecionado como servidor de recepção para fazer o acesso ou download de mensagens resididas no diretório de e-mail dos usuários no ambiente do experimento. Programas como clientes de e-mail, e até mesmo um browser acessando o webmail do site, fazem uso dos protocolos POP3 e IMAP ofertados por esse programa.

As configurações descritas a seguir exibem o mínimo necessário para servir acesso do usuário a suas caixas postais. Primeiramente, devido à segmentação do arquivo do Dovecot em diversos, deve-se editar e configurar a linha segundo exemplificado no Quadro 7.

Quadro 7: Configuração do arquivo /etc/dovecot/conf.d/10-auth.conf do Dovecot

```
disable_plaintext_auth = no
```

Por atribuição padrão, esse parâmetro vem habilitado como "sim". Todavia, para manter compatibilidade com clientes de e-mail que usam o método *plaintext*, a linha descrita acima torna apto o uso desse método de autenticação. Caso o cliente autentique via *plaintext* e o servidor não suporte esse método, o servidor informa algo semelhante à frase *"Disconnected (tried to use disabled plaintext auth)"***.**

Como desfecho da configuração do servidor Dovecot, falta apenas configurar onde é o caminho base de onde estão localizadas as mensagens dos usuários. Tal linha pode ser observada no Quadro 8.

Quadro 8: Configuração do arquivo /etc/dovecot/conf.d/10-mail.conf do Dovecot

```
mail_location = maildir:~/Maildir
```

Através dessa customização, o usuário pode, então, acessar as caixas postais, desde que as permissões do diretório informado estejam em conformidade com o acesso informado. Nota-se, na linha citada, que o local de armazenamento escolhido foi o home do usuário (representado pelo caráter "~" o qual significa /home/{usuáro_corrente}). Uma vez configurada esta linha, quando o servidor Dovecot recebe uma solicitação de conexão via porta 110 ou 143, o mesmo cria a estrutura de diretórios necessária dentro da base do usuário, caso esta conexão seja bem sucedida. Caso contrário, o Dovecot retorna uma mensagem de erro por meio do *log* de e-mail encontrado no arquivo /var/log/mailog. Esse erro é apresentado similar a *"Initialization failed: mail_location not set and autodetection failed: Mail storage autodetection failed with home=/home/{user}"*.

6.4. SEGUNDO AMBIENTE

Este ambiente visa oferecer recursos como configurações restritivas de SMTP, POP3 e IMAP adicionando criptografia nos protocolos envolvidos no serviço de e-mail, bem como autenticar o protocolo SMTP, característica que não é disponível por padrão do protocolo.

As instruções presentes na seção do primeiro ambiente devem, obrigatoriamente, serem aplicadas neste ambiente, pois são fundamentais para provimento do serviço de correio eletrônico. Porém, as configurações do ambiente anterior são genéricas e não estão focadas no escopo de segurança da informação.

A proposta almejada para esse segundo ambiente é ofertar uma camada de segurança mais fortalecida e espessa, seguindo documentos orientadores de protocolos tais como RFC 4422 (SASL), refinamento de configurações, boas práticas e fornecimento de um canal seguro para trafegar mensagens eletrônicas.

No caso do Postfix, esse *framework* desempenha uma função muito importante porque vem agregar integridade ao protocolo SMTP. Tal integridade, pilar essencial na segurança da informação, pode ser implementado configurando-se os arquivos do servidor Postfix e Dovecot.

6.4.1. Autenticação do SMTP

O SASL é um *framework* utilizado para provimento de autenticação para diversas implementações de protocolos de aplicação por meio de uma gama de métodos de autenticação conhecidos, sejam novos ou velhos.

A primeira informação necessária para aplicar a autenticação é saber se o Postfix está compilado com suporte ao Dovecot SASL. A extração deste dado é simples de ser realizada, vide o comando no Quadro 9, e pode ser conferida por meio do binário *postconf* encontrado após a instalação do Postfix.

Quadro 9: Comando que exibe programas compilados no Postfix

```
# postconf -a
```

Vale ressaltar que o Dovecot SASL passou a ser suportado pelo Postfix a partir da versão 2.3 deste último.

Através deste comando, o servidor exibe a lista todos os tipos de *plugins* SASL o qual o Postfix foi compilado. A saída esperada desse comando é a *string* “Dovecot”.

O Dovecot é invocado no processo de autenticação do SMTP que por sua vez faz chamada do PAM (*Pluggable Authentication Modules*), uma vez que este já é estabelecimento como autenticador padrão. Entretanto, o servidor Dovecot possibilita sua autenticação sobre outros métodos como SQL e LDAP.

O PAM é uma API que possibilita a autenticação do usuário de diversas maneiras. No caso deste ambiente, a autenticação ocorrerá localmente e a sua base é encontrada no arquivo /etc/passwd. Portanto, nenhuma personalização no PAM é requerida para fazer a referida autenticação.

Caso a autenticação do correio necessite integrar como alguma base externa a máquina local, o PAM fornece mecanismo de autenticação via rede como Kerberos e seu arquivo /etc/pam.d/dovecot necessitará de ajustes de configurações.

O Dovecot possibilita a autenticação SMTP de duas maneiras: via *socket* do domínio UNIX (suportado para Dovecot na versão 1) ou sobre um *socket* TCP. Neste ambiente será adotada a autenticação sobre *socket* TCP, uma vez que ele permite mais flexibilidade, pois em sua customização é aceito um servidor Dovecot e Postfix em máquinas distintas. As informações do Quadro 10 e Quadro 11 exibem as customizações precisas.

Quadro 10: Configuração do arquivo /etc/dovecot/conf.d/10-auth.conf do Dovecot

```
auth_mechanisms = plain login
```

Quadro 11: Configuração do arquivo /etc/dovecot/conf.d/10-master.conf do Dovecot

```
1. service auth {
2.    unix_listener auth-userdb {
3.    }
4.    inet_listener {
5.                port = 12345
6.    }
7. }
```

Os mecanismos de autenticação devem ser especificados pelo servidor Dovecot consoante mostrado no arquivo 10-auth.conf. O *plain* e *login* formam os valores fornecidos e são trafegados em texto em claro, todavia, como o SASL do segundo ambiente será implementado com SSL/TLS, não haverá perda da confidencialidade dos dados, pois o canal estará cifrado.

A criação de um *socket* Dovecot SASL para autenticação SMTP se faz necessário. O conteúdo contido na linha 4 do arquivo 10-master.conf é responsável pela geração desse *socket*. A linha 5 exibe a porta pela qual o *socket* do servidor deverá ficar a espera de requisições de autenticações do Postfix.

O Postfix faz reuso do programa Dovecot para autenticar o protocolo SMTP. Para isso, configurações no Postfix são necessárias para fazer a chamada do Dovecot. As linhas informadas no Quadro 12 realizam este propósito, e também, fornecem as informações relevantes para autenticar o SMTP.

Quadro 12: Configuração do arquivo /etc/postfix/main.cf do Postfix

```
1. smtpd_sasl_type = dovecot
2. smtpd_sasl_path = inet:127.0.0.1:12345
3. smtpd_sasl_auth_enable = yes
4. broken_sasl_auth_clients = yes
5. smtpd_sasl_local_domain = $mydomain
6. smtpd_sasl_security_options = noanonymous
7. smtpd_sender_login_maps = hash:/etc/postfix/virtual
8. smtpd_recipient_restrictions = permit_sasl_authenticated, reject
9. smtpd_sender_restrictions = permit_mynetworks
reject_sender_login_mismatch, permit_sasl_authenticated
```

O Postfix admite a autenticação do SMTP, através da camada abstrata SASL, por meio de suas duas implementações: Dovecot SAL e Cyrus SASL. A linha 1 informa qual o método foi selecionado (Dovecot SASL no caso do experimento).

A linha 2 exibe o IP do servidor Dovecot e a porta que o mesmo utilizará para criação do *socket* de autenticação segundo visto nas configurações do Dovecot na seção anterior.

Como a autenticação do servidor SMTP não é requerida para funcionamento deste protocolo, o parâmetro exibido na linha 3 deve ser habilitado para fins de autenticação e independe do modo de autenticação implementado. Depois de recarregar o serviço SMTP para efetivação das configurações, o servidor SMTP carrega os módulos Dovecot SASL quando inicia uma conexão sobre a porta SMTP. Uma conexão com o servidor do segundo ambiente foi realizada para validar se o servidor Postfix carregou, de modo correto, este módulo e foi exposto no Quadro 13.

Quadro 13: Comprovação de autenticação do Postfix

```
C. telnet server.example.com 25
S. 220 Servidor de e-mail da empresa.br
C. EHLO cliente.empresa.br
S. 250-mx2.empresa.br
S. 250-PIPELINING
S. 250-SIZE 10240000
S. 250-AUTH DIGEST-MD5 PLAIN CRAM-MD5
...
```

As linhas precedidas de C referem-se a linhas geradas pelo cliente e a letra S associada ao servidor. Infere-se que, em um momento posterior ao comando “EHLO” feito pelo cliente, a última linha retornada pelo servidor exibe a lista de mecanismos suportados para realizar a autenticação do SMTP. Logo, o servidor de correio eletrônico esta apto a autenticar o SMTP.

Entretanto, nem todos os clientes entendem comando AUTH conforme especificado na RFC do SASL. Para possibilitar integração com clientes de e-mail mais antigos, a customização da linha 4 provê um “=” após a palavra “AUTH”, forma que esses clientes esperam a lista dos mecanismos de autenticação do SMTP. A lista do Quadro 14 expõe os mecanismos após a linha 4 ser aplicada.

Quadro 14: Comprovação de autenticação do Postfix para clientes antigos

```
C. telnet server.example.com 25
S. 220 Servidor de e-mail da empresa.br
C. EHLO cliente.empresa.br
S. 250-mx2.empresa.br
S. 250-PIPELINING
S. 250-SIZE 10240000
S. 250-AUTH DIGEST-MD5 PLAIN CRAM-MD5
S. 250-AUTH=DIGEST-MD5 PLAIN CRAM-MD5
...
```

O domínio sobre qual a autenticação SASL ocorrerá deve ser especificado. A linha 5 foi customizada com o valor da variável *mydomain* aproveitando a flexibilidade de configuração que o Postfix dispõe.

A autenticação de modo anônimo dever ser rejeitada pelo servidor, pois o objetivo almejado é fornecer integridade ao protocolo SMTP. Logo, cada usuário deverá estar apto a enviar e-mails com o remetente igual ao usuário que autenticou no protocolo SMTP. A linha 6 nega a autenticação anônima e a linha 7 mostra o arquivo que contém um mapeamento dos e-mails e seus respectivos donos. Para o SMTP aceitar remetentes contidos neste arquivo e fazer as restrições necessárias no destinatário e remetente da mensagem, a linha 8 e 9 possuem as diretivas respectivamente.

As configurações de restrição uma sintaxe própria. Os argumentos integrantes passados em cada linha de restrição são percorridos linearmente e pelo menos um deles deve ser satisfeito.

As restrições aplicadas no contexto "RCPT TO" estão localizadas na linha 8. A política aplicada permite que apenas usuários autenticados possam enviar e-mails por meio da expressão *permit_sasl_authenticated*, restringindo assim os demais usuários através da diretiva *reject*. Ou seja, um usuário para inserir algum valor após o comando RCPT TO do SMTP deverá estar autenticado no esquema Dovecot SASL ofertado pelo servidor.

Agora, com relação ao comando MAIL FROM, as restrições estão presentes na linha 9 a qual contém 3 argumentos. A primeira restrição diz a respeito da rede que poderá enviar e-mails aos usuários. Ela é obtida por meio da expressão *permit_mynetworks* a qual extrai o valor da variável *mynetworks* encontrada neste mesmo arquivo. O próximo bloqueio é o *reject_sender_login_mismatch*. Tal argumento pesquisa o proprietário do remetente da mensagem de e-mail na base informada na linha 7 e compara se o usuário autenticado é o mesmo que o retornado pela consulta. A terceira e última restrição permite que apenas usuários autenticados via Dovecot SAL obtenham sucesso na requisição de um MAIL FROM para o servidor SMTP. Tal ajuste é alcançado por meio da diretiva *permit_sasl_authenticated*.

6.4.1.1. Cliente de email com SMTP autenticado

Uma vez preparado a estrutura do SMTP para autenticação, o software de mensageiria eletrônica do cliente deverá estar adequado para realizar a referida autenticação. O cliente utilizado para demonstrar este processo ocorrendo foi o *Outlook Express*.

Caso o cliente de e-mail não habilitado a opção de autenticação, o servidor de e-mail recusa o envio da mensagem eletrônica apresentando a seguinte afirmação *"Sender address rejected: not logged in"*.

Agora, se o cliente configurar seu *Outlook Express* para fazer autenticar o servidor de saída de e-mails e tentar, por algum motivo fortuito, informar outra credencial na validação do SMTP o servidor negará o envio e alertará em seu *log* a linha *"Sender address reject: not owned by user {user}"*.

Dessa forma, o protocolo SMTP oferece integridade garantindo, assim, que usuários não repudiem as suas mensagens enviadas.

6.4.2. Criptografia no correio eletrônico

O próximo item a se tratar em segurança da informação está associado à confidencialidade dos dados. No caso de correio eletrônico, a sua infraestrutura deverá trafegar mensagens eletrônicas em extremo sigilo.

Os protocolos de envio e recebimento de e-mails deverão prover suas informações dentro de canais criptografados. Para alcançar tal finalidade, os arquivos de configuração do Dovecot e Postfix conterão as modificações necessárias.

6.4.2.1. Cifragem no contexto de recepção de mensagens

Informações contidas dentro das mensagens eletrônicas são essenciais para a rápida troca de comunicação entre seus funcionários e, costumeiramente, tem o teor sigiloso. Quando uma mensagem eletrônica está apta para ser acessada ou baixada do servidor de e-mail, este processo deve ser feito com bastante cautela, pois entre os equipamentos de interconexão algum atacante pode atuar para conseguir interceptar essa informação.

No processo de acesso das mensagens, o servidor de correio via programa Dovecot para a disponibilização. O Dovecot, de maneira padrão, não fornece criptografia nos protocolos POP3 e IMAP os quais são os incumbidos de gerenciar o acesso ou download das mensagens.

A criptografia pode ser acrescida a esses protocolos por meio da customização do servidor Dovecot. A alteração de algumas linhas deste, exibidas no Quadro 15, habilita o uso de cifras no canal de recebimentos de e-mails.

Quadro 15: Configurações do arquivo /etc/dovecot/conf.d/10-master.conf do Dovecot

```
1.  service imap-login {
2.    inet_listener imap {
3.          #port = 143
4.    }
5.    inet_listener imaps {
6.          #port = 993
7.          ssl =yes
8.    }
9.  }
10. service pop3-login {
11.   inet_listener pop3 {
12.         #port 110
13. }
14. inet_listener pop3s {
15.         #port 995
16.         ssl = yes
17.   }
18. }
```

Da linha 1 a 9 do Quadro 15, estão dispostas as configurações associadas ao protocolo IMAP, enquanto da linha 10 a 18 referem-se ao protocolo POP3. Caso seja a intenção da empresa fornecer apenas protocolos cifrados, é preciso comentar o bloco *inet_listener_imap* e *inet_listener_pop3*.

A permissão para passagem de dados criptografados nesses protocolos é feita pro meio da remoção do comentário das linhas 7 e 16 que, originalmente, são comentadas. Observe que a linha que contém os números das portas as quais o protocolo irá atuar estão comentadas. Isso significa que o servidor Dovecot aplicará as portas definidas pelo IANA e podem ser conferidas no arquivo /etc/services. Caso o administrador deseje alterar a porta padrão basta retirar o "#" das linhas 6 e 15 e inserir o valor almejado para as portas tratadas em questão.

A configuração disposta acima habilita as portas a trabalharem com ssl, porém em nenhum momento foi parametrizado os certificados e chaves privadas para geração da criptografia. Essas instruções são encontradas no Quadro 16.

Quadro 16: Configuração do arquivo /etc/dovecot/conf.d/10-ssl.conf do Dovecot

```
1. ssl = yes
2. ssl_cert = </etc/pki/dovecot/certs/mail.pem
3. ssl_key = </etc/pki/dovecot/private/mail.pem
4. ssl_ca = </etc/pki/CA/certs/ca.pem
5. ssl_cipher_list = ALL:!LOW:!SSLv2:!EXP:aNULL
```

A primeira linha habilita a utilização do ssl no programa Dovecot. A linha 2 exibe o caminho do certificado do servidor de correio eletrônico quando a terceira informa o local onde a chave privada que gerou o certificado está residida. Tanto o certificado quanto a chave primária são essenciais para o processo de criptografia no ambiente de mensageiria eletrônica porque estes são os responsáveis pela cifragem dos dados. A linha 4 exibe o caminho do certificado da CA, que no caso do ambiente em questão, é auto assinado. Tal linha é importante, pois quando o cliente verificar o certificado do servidor de e-mail ele precisará checar as informações da CA com o certificado dessa CA em sua máquina. Em um tópico posterior será abordado como fazer a criação da chave e do certificado.

A quinta linha exibe a lista de cifras que o servidor Dovecot estará disponível para uso. A configuração feita nela permite todas as cifras com exceção das categorias *LOW*, *SSLv2*, *EXP* e *aNULL*. Essas categorias podem ser mais detalhadas no link www.openssl.org/docs/apps/ciphers.html.

Para finalizar a configuração do SSL/TLS no servidor Dovecot, basta configurar este para registrar os *logs* gerados pelo tráfego criptografado. Isso pode ser alcançado com a customização da seguinte linha vista no Quadro 17.

Quadro 17: Configuração do arquivo /etc/dovecot/conf.d/10-logging.conf do Dovecot

```
verbose_ssl = yes
```

Para fazer testes no servidor Dovecot para validar a inclusão da camada SSL/TLS é preciso executar o seguinte comando do Quadro 18.

Quadro 18: Comando para fazer conexão POP3S

```
openssl s_client -connect mx2.empresa.br:pop3s
```

O retorno desse comando são dados relativos ao certificado relatando que ele foi assinado por uma autoridade certificadora auto assinada, e também, as informações de identificação do servidor (disponibilizadas na geração da requisição de assinatura de certificado). Após isso, o servidor está disponível para fazer a autenticação no servidor Dovecot.

6.4.2.2. Cifragem no contexto de envio de mensagens

Além do processo de acesso as mensagens ocorrer de modo cifrado, a tramitação de e-mails entre MTAs devem acontecer de modo seguro também. A aplicação de cifras no contexto do servidor de envios de e-mail se torna essencial para manter a confidencialidade da mensagem. Sendo assim, a aplicação da camada SSL/TLS no Postfix deverá ser implementada por meio da seguinte configuração no servidor Postfix de acordo com o Quadro 19.

Quadro 19: Configuração do arquivo /etc/postfix/main.cf do Postfix

```
1. smtpd_use_tls = yes
2. smtpd_tls_key_file = /etc/pki/dovecot/private/mail.pem
3. smtpd_tls_cert_file = /etc/pki/dovecot/certs/mail.pem
4. smtpd_tls_CAfile = /etc/pki/CA/certs/ca.pem
```

A habilitação da camada SSL/TLS é habilitada via o argumento "*yes*" da primeira linha. A linha 2 e 3 apresentam, respectivamente, o local do certificado e o da chave privada do servidor de e-mail. A última linha exposta contém o caminho do certificado da autoridade certificadora. Essa informação é crucial, pois através dela validações do certificado do servidor de e-mail podem ser realizadas.

Para finalizar a configuração do servidor SMTP, uma alteração no Postfix, conforme visto no Quadro 20, se faz necessária para ativar a porta padrão, que é a 465, do SMTPS. Para fazer isso comente a linha 1 e descomente a linha 2 vistas no Quadro 20.

Quadro 20: Configuração do arquivo /etc/postfix/master.cf do Postfix

```
1.   smtp        inet  n       -       n       -       -       smtpd
2.   smtps       inet  n       -       n       -       -       smtpd
```

O número da porta foi alterado para o valor conferido no arquivo /etc/services. O valor encontrado inicialmente para a variável smtps é 465.

A validação da configuração da camada SSL/TLS no servidor Postfix pode ser testada por meio da instrução mostrada no Quadro 21.

Quadro 21: Comando para fazer conexão SMTPS

```
openssl s_client -connect mx2.agricultura.gov.br:smtps
```

A saída desse comando é informações referentes ao certificado e assinatura de sua CA, que nesse caso é auto assinada, bem como os dados cadastrados na geração da requisição de

assinatura de certificado. Após isso, o servidor está disponível para trocar dados relativos ao protocolo SMTP.

6.4.2.3. Criação de CA, chaves criptográficas e certificados

A comunicação estabelecida entre 2 partes, na área de criptografia, sempre foi uma problemática. Essa dificuldade acontece porque as partes integrantes precisam compartilhar um segredo o qual é a conhecida como chave criptografia. Ela é a responsável por ditar a maneira pela qual a cifragem dos dados ocorrem.

Porém, o problema de compartilhamento de chaves vem sendo sanado após a invenção da infraestrutura de chaves públicas (ICP). Através desse modelo, um par de chaves é criado: uma privada e outra pública. A chave privada é de propriedade exclusiva de seu dono enquanto a chave pública é de conhecimento geral.

O certificado digital, dentre esses elementos criptográficos, é a terceira parte que garante confiança da chave pública trocada entre clientes. Observando a importância desses elementos, a sua implementação na estrutura de correio eletrônico agrega confidencialidade a este serviço.

- Criando uma autoridade certificadora (*certified authority* - CA)

No primeiro passo deste ambiente do experimento, será criada uma CA auto assinada (CA está que não é homologada e reconhecida) que exercerá o papel da terceira parte e atuará como uma CA válida conforme visto em funcionamento no mercado. Para constituir a CA auto assinada, através do programa openSSL do Linux, basta seguir os passos explicitados no Quadro 22.

Quadro 22: Criando uma CA auto assinada

```
1. cd /etc/pki
2. openssl genrsa -des3 -out CA/private/ca.pem 4096
3. openssl req -new -x509 -key CA/private/ca.pem –out
CA/certs/ca.pem -days 1095
```

O local destinado para infraestrutura de chaves públicas no sistema operacional CentOS está demonstrado na linha 1. Dentro dessa pasta existe uma organização de diretórios para

melhor administração dos certificados da CA e dos demais programas que utilizam certificado.

A linha 2 exibe o comando para geração da chave privada. O parâmetro *genrsa* especifica o tipo da chave que, no caso em questão, é a RSA enquanto o des3 informa o algoritmo usado para criar a senha de acesso da chave privada. No caso da CA, é altamente recomendado utilizar senha, pois no caso de perda ou interceptação desta, assinaturas de novos certificados subordinados a essa CA sempre solicitarão a senha da chave privada. Além disso, a diretiva *out* exibe o local onde será depositada a chave privada e a numeração 4096 indica o tamanho de bits da chave gerada.

Por fim, a linha 3 contém o comando para criar o certificado da CA. O valor "req" representa uma requisição de certificado, o *-new* especifica que será uma nova solicitação e o argumento -x509 indica o padrão do certificado gerado. O caminho da chave privada usada na criação do certificado e o local do certificado criado estão precedidos pelas diretivas *-key* e *-out* respectivamente. A validade do certificado é parametrizada pelo argumento *-days* seguido da quantidade de dias validos do mesmo.

Um formulário interativo será apresentado depois da execução da instrução exibida na terceira linha. As informações fornecidas dizem respeito à localização da organização da CA e estes dados serão integrantes do certificado, bem como a chave pública da autoridade certificadora. Após preenchimento do formulário, a CA esta apta para assinar certificados terceiros, tornando-se assim, referência de comunicação entre duas entidades.

- Solicitando uma requisição de assinatura de certificado (*certificate* signing request - CSR)

O arcabouço de criptografia foi inserido no contexto de mensageiria eletrônica e foi demonstrada sua configuração no servidor Dovecot e Postfix em momentos anteriores. Estes servidores fizeram referência a certificados (do servidor de e-mail e da CA) e a chave privada os quais são cruciais para cifragem dos dados. Nesta etapa será visto como gerar uma requisição de assinatura de certificado para finalmente criar o certificado do servidor de e-mail. As instruções, presentes no Quadro 23, realizam estas atividades.

Quadro 23: Solicitando uma requisição de assinatura de certificado

```
1. openssl genrsa -out dovecot/private/mail.pem 2048 -nodes
2. openssl req -new -key dovecot/private/mail.pem –out
CA/newcerts/mail.csr
```

Primeiramente, deve-se gerar uma chave privada para o servidor de correio eletrônico conforme observado na linha 1. Os parâmetros fornecidos constituem uma chave do tipo RSA de 2048 bits, sem senha de acesso e sendo armazenada no local /etc/pki/dovecot/private/mail.pem. Neste caso não é obrigatório inserir senha na chave privada por se tratar de um servidor de mail (por meio da diretiva *-nodes*). Os procedimentos realizados devem ocorrer na máquina que abriga o serviço de e-mail que, no caso desse ambiente, é o mesmo do servidor de ICP.

O próximo passo, encontrado na segunda linha, ocorre também no servidor de correio e contém o comando que resulta em um arquivo .csr. Em suas entrelinhas, ele faz uma nova requisição por meio dos argumentos "*-new*" e "req" usando a sua chave privada exibida posterior a diretiva "*-key*" e criando um arquivo de requisição sendo armazenado no local informado após a expressão "*-out*". Caso o servidor de infraestrutura de chave pública se encontre em outro servidor, o arquivo .csr deverá ser exportado para o servidor ICP para ser assinado.

- CA assinando uma requisição de assinatura de certificado (CSR)

Quadro 24: Assinando uma CSR

```
1. openssl x509 -req -days 365 -in CA/newcerts/mail.csr –CA
CA/certs/ca.pem -CAkey CA/private/ca.pem -set_serial 01 -out
CA/certs/mail.pem
```

Para finalizar, o servidor ICP, atuando entidade de confiança para a comunicação, assina a requisição com sua chave privada e gera o certificado do servidor solicitante conforme visto no Quadro 24. Os parâmetros "x509" e "-req" especificam o formato do certificado gerado e que se trata de uma nova requisição. A validade do certificado gerado é referenciada pelo argumento "*-days*" seguido do valor em dias. O arquivo .csr é uma entrada e é fornecida após a diretiva "*-in*", bem como a chave privada da CA via argumento "CAkey", que é responsável pela assinatura e geração do hash do arquivo de requisição, e o certificado da CA pela expressão "-CA" também são requisitados. Como resultado dessa operação, o certificado do servidor de mensageiria eletrônica é constituído no local especificado pelo argumento "*-out*".

Como o certificado gerado para o servidor de correio foi assinado por uma autoridade certificadora não-confiável (auto assinada), a importação do certificado da CA deve realizado nos clientes de e-mail eletrônico. Isso ocorre porque certificados não confiáveis não vêm instalados nos sistemas operacionais e nem em *browsers*. A importação do certificado admite

dois modos de instalação: via console administrativa do Windows ou via *browser* na parte de certificados.

- Testando os certificados, requisições e chaves privadas

Toda infraestrutura de chave pública foi preparada para garantir a confidencialidade dos dados. Então, para assegurar que os elementos integrantes de grupo estejam em conformidade com a configuração esperada, um procedimento de verificação sobre os mesmo deverá ocorrer para que em um momento posterior eles possam vigorar.

Os comandos dispostos no Quadro 25 realizam essa tarefa aspirada.

Quadro 25: Verificação dos artefatos criptográficos

```
openssl rsa -noout -text -in mail.key
openssl req -noout -text -in mail.csr
openssl rsa -noout -text -in ca.key
openssl x509 -noout -text -in ca.pem
openssl x509 -noout -text -in mail.pem
```

6.4.3. Refinamentos na configuração do SMTP

Dois membros integrantes da segurança da informação, a integridade e a confidencialidade, foram abordados em etapas anteriores e aplicados por meio de aplicativos desenvolvidos para auxiliar o Postfix a adquirir essas características. Todavia, o último pilar da segurança da informação será tratado mais profundamente nessa seção por meio de configurações finas do SMTP.

Antes de iniciar a configuração do Postfix, é primordial fazer a atualização deste software segundo visto no Quadro 26.

Quadro 26: Atualizando o Postfix

```
yum update postfix
```

Através do comando acima, o servidor o qual o MTA está instalado irá verificar, nos repositórios configurados, a última versão do Postfix e o atualizará caso o software instalado seja mais antigo. A utilização de repositórios estáveis deve ser configurada na máquina do Postfix com a finalidade de se evitar falhas e erros encontrados em versões betas e imaturas.

Após isso, um software antivírus deverá estar instalado com intuito de realizar a checagem das mensagens trafegadas no servidor de e-mail. Além disso, a atualização

periódica da base de assinaturas do antivírus é uma política desejável de se implantar na corporação. No ambiente proposto e também nesta monografia, o software antivírus não está enquadrado no escopo, porém a sua importância é crucial no provimento seguro de correio eletrônico.

As configurações de restrição do SMTP serão realizadas todas no arquivo /etc/postfix/main.cf, pois tratam a respeito do envio de mensagens eletrônicas.

A geração, configuração e inspeção do arquivo de logs do serviço de e-mail é outro aspecto fundamental que deverá ser adotado. Por meio deste arquivo acompanhamento tentativas não autorizadas, problemas de configurações e demais eventos relevantes a segurança podem ser encontrados nesse arquivo. Por convenção, o Postfix utiliza o *syslog* para registrar os eventos relativos à mensageiria eletrônica. Sendo assim, basta configurar o nível de detalhamento dos logs gerados. Isso pode ser conferido por meio da linha do Quadro 27.

Quadro 27: Nível de registramento de *logs*

```
debug_peer_level = 2
```

O valor atribuído para o nível de *debug* do MTA deverá conter um valor compatível com o grau de detalhamento da informação que a empresa necessita. O número exibido acima traduz um valor mínimo para que as informações sejam proveitosas na inspeção dos *logs* do serviço.

A implantação de um programa analisador de *logs* para geração de gráficos estatísticos é fundamental para metrificar e analisar os eventos ocorridos no ambiente de correio eletrônico. Além disso, o acompanhamento dos processos e desempenho do servidor também é essencial para realizar a gestão da segurança da informação, pois uma vez que não se mensura não é possível gerir algo.

Outra prática importante para garantir a disponibilidade do serviço provido é realização periódica de *backups* dos dados sensíveis da máquina de correio eletrônico. Arquivos de configuração, e-mails das caixas postais, *scripts* administrativos e demais arquivos constituintes do serviço de e-mail devem ser contemplados na execução de um *backup*. Outro ponto que deve ser observado é a retenção do *backup* e o local onde será residida as mídias detentoras dos dados.

A retenção dos e-mails dos usuários deverá atender os aspectos legais levando em consideração que, mesmo após alguns meses do desligamento de um funcionário, ele tem direito de requisitar dados de sua conta de e-mail.

No tocante da fita de armazenamento, esta deve ser confinada em um local seguro sendo de preferência cofres com segredo situados em locais diferentes do ambiente de produção do correio eletrônico.

O bloqueio de remetentes e destinatários desconhecidos é interessante implantado no servidor de correio. Tal requisito é aplicado por meio da ativação dos parâmetros *smtpd_reject_unlisted_sender* e *smtpd_reject_unlisted_recipient* sendo este último já vem habilitado por padrão (não precisa da desta linha no arquivo de configuração). Desta forma, o servidor estará mais protegido de vírus e spam que enviam e-mails com remetentes e destinatários que não estão listados na tabela virtual ou canonical.

Quadro 28: Refinamentos do servidor Postfix

```
1. smtpd_reject_unlisted_sender = yes
2. smtpd_reject_unlisted_recipient = yes
3. smtpd_client_restrictions = reject_multi_recipient_bounce,
permit_mynetworks, reject
4. smtpd_data_restrictions = reject_unauth_pipelining
5. smptd_helo_required = yes
6. smtpd_helo_restrictions = reject_non_fqdn_helo_hostname,
reject_unknown_helo_hostname, reject_invalid_helo_hostname
7. smtpd_sender_restrictions = reject_non_fqdn_sender,
reject_unknown_sender_domain, reject_unverified_sender,
reject_unlisted_sender
8. smtpd_recipient_restrictions = reject_non_fqdn_recipient,
reject_unknown_recipient_domain, reject_unauth_destination
permit_mynetworks
9. smtpd_etrn_restrictions = permit_mynetworks, reject
10. smtpd_banner = Servidor de e-mail da empresa.br
11. message_size_limit = 5242880
```

Os clientes que acessam o serviço de e-mail devem ser restringidos no servidor, podendo somente aqueles que estiverem no intervalo de rede configurado na variável *mynetworks* segundo exibido na configuração do primeiro ambiente. Além disso, quando um envelope contiver endereço de remetente vazio e o campo destinatário possuírem diversos e-mails é um cenário que deverá ser barrado com o argumento *reject_multi_recipient_bounce*. As situações descritas podem ser acompanhadas por meio da linha 3 do Quadro 28.

A linha 4 limita, na abrangência do comando DATA, que usuários usem os comandos do SMTP for de ordem e também que ele envie outros comandos sem que o servidor envie sua resposta. Tal prática restringe bastante a incidência de *worms* e *spams* no servidor de correio.

Em versões mais recentes que a 2.3 do Postfix, a linha 5 habilita é obrigatória caso exista a necessidade de qualquer tipo de filtragem no comando HELO ou EHLO.

A linha 6 controla as repostas do cliente no contexto HELO ou EHLO. Nela, por meio do argumento *reject_non_fqdn_helo_hostname*, os *hosts* que requisitam conexão com o servidor SMTP devem especificar o seu nome no formato FQDN conforme especificado pela RFC. O outro parâmetro citado foi o *reject_unknown_helo_hostname* cuja função é rejeitar o nome dos *hosts* que não possuem um registro A ou MX no servidor DNS. E, fechando a linha 6, o valor *reject_invalid_helo_hostname* nega os nomes de *hosts* fornecidos com a sintaxe inválida. No ambiente em questão, como não houve registro do domínio e nem uso de um servidor DNS, a aplicação dos argumentos *reject_non_fqdn_helo_hostname* e *reject_unknown_helo_hostname* foi desconsiderada. Entretanto, vale ressaltar que estes filtros são essenciais para mitigar a incidência de *spams* em ambientes de produção porque evitam que servidores sem registros MX em DNS ou com seu domínio cadastrado de maneira incorreta tenham capacidade de enviar e-mails para o MTA configurado. Normalmente um *spammer* usufrui dessa ausência de checagem para disparar diversos e-mails sem sequer possuir esses requisitos citados.

Os filtros realizados no escopo MAIL FROM está contidos na linha 7. Os valores fornecidos no parâmetro *smtpd_sender_restrictions* devem ser colocados conjuntamente com os atributos informados na autenticação do SMTP, caso tenha sido aplicado alguma *sender restriction*, pois na existência de duas linhas desse parâmetro ele é sobrescrito pela ultima linha dessa configuração. Os argumentos providos no filtro do remetente podem ser explanados da seguinte maneira:

- *reject_non_fqdn_sender*: Rejeita remetentes que possuem o endereço de e-mail que não estão no formato FQDN requisitado pela RFC
- *reject_unknown_sender_domain*: Bloqueia mensagens de remetentes os quais os seus domínios não possuem um registro A ou MX do host ou o registro MX não está atribuído ou configurado corretamente no domínio do remetente. Nesta etapa do experimento esse argumento esse controle não foi implementado porque na elaboração da estrutura desse ambiente não se utilizou um servidor DNS e também não houve registro do domínio “empresa.br”. Customizações no arquivo de *hosts* do cliente foram executadas para resolução de nomes.
- *reject_unverified_sender*: Nega mensagens quando o endereço do remetente não está alcançável. Isso ocorre quando o serviço de verificação não retorna um resultado.
- *reject_unlisted_sender*: Rejeita conexões SMTP quando o endereço de origem do e-mail não está listado como um endereço de origem válido.

As customizações no âmbito do comando RCTO TO estão apresentados na linha 8. Consoante explicado no contexto do MAIL FROM, caso existam linhas duplicadas dessa restrição, prevalecerá a ultima linha. O significado de cada parâmetro está exposto abaixo:

- *reject_non_fqdn_recipient*: Nega recebimento de mensagens as quais o destinatário não exibe seu endereço no padrão FQDN solicitado pela RFC.
- *reject_unknown_recipient_domain*: Rejeita e-mails cujo domínio do destinatário não contém um registro A ou MX do *host* ou o registro MX do domínio em questão não está configurado de maneira correta. Este controle não foi levado em questão no experimento porque um servidor DNS não foi usado para resoluções de nome.
- *reject_unauth_destination*: Bloqueia e-mails onde o destinatário não é encontrado nos arquivos de pesquisa local ou quando não são localizados no domínio *relay* configurado no Postfix. Este parâmetro foi ignorado no experimento, pois o Postfix ao verificar o domínio do destinatário consulta servidores DNS. E, no caso de uma entrega local, o servidor nega envios de e-mails uma vez que não consegue validar o domínio.

Conexões intermitentes são tratadas pelo postfix via comando ETRN. Neste âmbito, a configuração almejada é liberar apenas a rede confiável de utilizar o servidor SMTP segundo exibido na linha 9.

Outro fator a ser observado está associado com o vazamento das informações de versão do servidor SMTP. Por padrão, o servidor Postfix exibe a sua versão por meio do parâmetro *smtpd_banner*. Tal variável deve ser alterada para uma breve apresentação saudação da empresa segundo visto na linha 10 do Quadro 28.

Outro ponto crucial a ser citado é relativo ao tamanho máximo das mensagens eletrônicas aceitas pelo servidor de e-mail. Isso pode ser modificado conforme a linha 11 do Quadro 28.

O limite dos e-mails estipulado foi de 5 MB. Este controle é importante, pois máquinas *spammers* que enviam e-mails com conteúdos enormes podem causar queda de performance do serviço ou até mesmo indisponibilidade deste. Além disso, liberar e-mails com tamanho enorme pode causar insuficiência de espaço no servidor de caixas postais, uma vez que o atacante se aproveita deste artifício para enviar diversas mensagens eletrônicas, ocorrendo, assim, parada no serviço provido.

Por fim, uma documentação contemplando todas as configurações aplicadas e seus detalhamentos deverão ser realizados para que, em caso de troca de equipe ou mesmo treinamento de servidores, esse documento sirva como orientador. Aliado a isso, quando

ocorre uma queda no serviço provido, as informações contidas no documento são importantes para o rápido restabelecimento do serviço ofertado.

7. CONSIDERAÇÕES FINAIS

7.1. IMPLEMENTAÇÕES

Em tempos anteriores, os serviços disponibilizados sob a internet tinham como princípio básico o funcionamento destes. Porém, com a explosão e a disseminação da rede mundial de computadores, esse requisito funcional passou a necessitar de um complemento conhecido como segurança. Os ambientes deste experimento vieram simular esse paradoxo. A facilidade de dispor um serviço é muito simplória uma vez que se tem uma enorme quantidade de guias na Internet. Entretanto, esses guias, em sua maioria, costumam apresentar um teor de conhecimento raso sobre o assunto, pois o enfoque está voltado para a questão prática. Dentre as consequências causadas por isso, aspectos relacionados à segurança geralmente são os mais afetados e normalmente são colocados em segundo plano.

Foi observado que um ambiente de mensageiria eletrônica corporativo, impreterivelmente, carece de uma configuração robusta no tocante a segurança da informação.

Mecanismos técnicos e procedimentos norteados por normas de segurança foram apresentados neste documento objetivando agregar maior segurança e confiabilidade do serviço de e-mail.

Para solidificar os conceitos, práticas e procedimentos sugeridos, máquinas virtuais foram exibidas de modo a exemplificar as entidades governamentais as quais não aplicam as boas práticas de configuração no âmbito de mensageiria eletrônica. Outras máquinas foram elaboradas conferindo mecanismos e configurações desejáveis para reduzir a incidência de ataques no ambiente de e-mail.

7.2. ANALOGIA ENTRE AMBIENTES

Os resultados dos experimentos propostos denotam que a aderência ao mecanismo de autenticação do SMTP associado com a utilização de algoritmos criptográficos confere uma maior segurança no serviço de e-mail. Ataques do tipo *man-in-the-middle*, *sniffing*, *DoS*,

DDoS e outras mais podem ter sua probabilidade de sucesso reduzida segundo observado no experimento.

Visto isto, seria de grande valia instituições governamentais buscarem incorporar tais mecanismos, pois o grau de relevância ocupado por estas organizações é indubitavelmente crucial na estratégia política do país. Logo, os benefícios decorridos do segundo ambiente do experimento podem conduzir uma melhor gestão de gastos dos órgãos governamentais bem como uma tramitação de informações por e-mail mais segura, confiável e com menos interrupções, o que pode melhorar a imagem desta instituição.

Ficou nítido que o segundo ambiente apresentado explorou diversos conteúdos e se mostrou muito mais complexo de se manipular em relação ao primeiro ambiente. O ganho adquirido pela implementação exibida pela segunda estrutura torna o mesmo programa, Postfix, mais confiável, robusto e seguro.

O primeiro ambiente contém vulnerabilidades conhecidas no âmbito de segurança e podem ser facilmente exploradas. Um ataque *man in the middle* terá grandes chances de capturar informações sensíveis deste ambiente como consequência da ausência da camada de criptografia. Em se tratando de instituições governamentais, o prejuízo causado pelo vazamento da informação pode alcançar valores na casa dos milhões, o que dependerá do teor do dado contido nessas mensagens eletrônicas.

Além disso, como a primeira estrutura não apresenta autenticação no protocolo SMTP, um usuário pode se disfarçar por outro e enviar e-mails. Tal procedimento, além de causar perda de confiança no serviço ofertado, afeta diretamente o princípio da integridade dos dados. Neste caso pode-se imaginar um usuário solicitando uma expiração de senha de outro usuário por meio de uma configuração maliciosa de e-mail, ou seja, se passando por outro usuário para adquirir sua senha. Isso seria devastador no esquema de segurança de informação e perda de credibilidade da imagem do corpo integrante da TI.

A disponibilidade 24 horas por 7 dias no ambiente de mensageiria é uma realidade encontrada em diversas empresas. Portanto, a parada deste serviço por um longo período se torna inaceitável. Para isso, refinamentos de configurações devem ser feitos a fim de se proteger de ataques do tipo DoS, DDoS e outros mais que visam interromper o fornecimento do correio eletrônico. Acredita-se que o ambiente 1 está mais suscetível a esses ataques, pois apresenta menos barreiras e configurações que restrinjam o acesso do atacante.

7.3. TRABALHOS FUTUROS

Os controles apresentados no ambiente 2 do experimento podem não traduzir uma segurança satisfatória no contexto de correio eletrônico de uma empresa. Cada instituição contém requisitos e gradações diferentes de aceitabilidade em relação a falhas e ataques ocorridos. Portanto, mecanismos, métodos, programas e técnicas que visam reduzir a incidência de *spams* como programas *chalange response*, *sender policy framework* (SPF) e programas que usem *greylists* aliado a *softwares* de contenção de *malwares* e outros tipos de ataques também devem ser considerados nestas entidades. O foco selecionado nessa monografia não priorizou estes elementos citados anteriormente e, que podem vir a ser explorados e discutidos mais detalhadamente em trabalhos futuros, pois são de grande importância no assunto tratado nesta monografia.

8. BIBLIOGRAFIA

[1] KUROSE, JAMES F.; ROSS, KEITH W. *Computer networking: A top-down approach featuring the Internet.* 5. ed. *Boston*: *Pearson Education*, Março de 2009.

[2] TANENBAUM, ANDREW S. *Computer Networks.* 4. ed. *Amsterdam*: *Prentice Hall*, Novembro de 2002.

[3] DENT, KYLE D. *Postfix: The Definitive Guide.* 1. ed. *Sebastopol: O'Reilly*, Dezembro de 2003.

[4] OLIVEIRA, WILDSON DE MACEDO. Postfix: Servidor de E-mail – Guia prático. 1. Ed: Ciência Moderna, Janeiro de 2011.

[5] MYERS, J.; MELLON, CARNEGIE; ROSE, M.; DOVER BEACH CONSULTING, INC. RFC 1939 – *Post Office Protocol – Version 3*. Disponível em: <http://www.rfc-editor.org/rfc/rfc1939.txt>. Acesso em: 03 abr. 2012.

[6] FREED, N.; INNOSOFT; BORENSTEIN, N. RFC 2045 – *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. Disponível em: <http://www.rfc-editor.org/rfc/rfc2045.txt>. Acesso em: 03 abr. 2012.

[7] FREED, N.; INNOSOFT; BORENSTEIN, N. RFC 2049 – *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples*. Disponível em: <http://www.rfc-editor.org/rfc/rfc2049.txt>. Acesso em: 03 abr. 2012.

[8] CRISPIN, M. RFC 3501 – *Internet Message Access Protocol – Version 4rev1*. Disponível em: <http://www.rfc-editor.org/rfc/rfc3501.txt>. Acesso em: 03 abr. 2012.

[9] A. MELNIKOV, ED; ISODE LIMITED; K. ZEILENGA, ED.; OPENLDAP FOUNDATION. RFC 4422 – *Simple Authentication and Security Layer* (SASL). Disponível em: <http://www.rfc-editor.org/rfc/rfc4422.txt>. Acesso em: 03 abr. 2012.

[10] JOSEFSSON, S. RFC 4648 – *The Base 16, Base 32 and Base 64 Data Encodings*. Disponível em: <http://www.rfc-editor.org/rfc/rfc4648.txt>. Acesso em: 03 abr. 2012.

[11] R. SIEMBORSKI, ED.; GOOGLE, INC; A. MELNIKOV, ED. RFC 4954 – SMTP *Service Extension for Authentication*. Disponível em: <http://www.rfc-editor.org/rfc/rfc4954.txt>. Acesso em: 03 abr. 2012.

[12] KLENSIN, J. RFC 5321 – *Simple Mail Transfer Protocol*. Disponível em: <http://www.rfc-editor.org/rfc/rfc5321.txt>. Acesso em: 03 abr. 2012.

[13] P. RESNICK, ED; QUALCOMM INCORPORATED. RFC 5322 – *Internet Message Format*. Disponível em: <http://www.rfc-editor.org/rfc/rfc5322.txt>. Acesso em: 03 abr. 2012.

[14] RAMSDELL, B.; BRUTE SQUAD LABS; TURNER, S. RFC 5751 – *Secure / Multipurpose Internet Mail Extensions (S/MIME) – Version 3.2 Message Specification*. Disponível em: <http://www.rfc-editor.org/rfc/rfc5751.txt>. Acesso em: 03 abr. 2012.

[15] ESTATÍSTICAS de notificações de spam reportadas ao CERT.BR. Disponível em: <http://www.cert.br/stats/spam/>. Acesso em: 03 abr. 2012.

[16] LEMOS, RONALDO; DONEDA, DANILO MAGANHOTO; DE SOUZA, CARLOS AFFONSO PEREIRA; ROSSINI, CAROLINA ALMEIDA A. Estudo

sobre a regulamentação jurídica do spam no Brasil. Disponível em: <http://www.cgi.br/publicacoes/documentacao/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 03 abr. 2012.
[17] ABNT. Associação Brasileira de Normas Técnicas. Disponível em: <http://www.abnt.org.br/>. Acesso em: 03 abr. 2012.
[18] CERT.BR. Cartilha de segurança para Internet. Disponível em: <http://cartilha.cert.br>. Acesso em: 03 abr. 2012.
[19] KLEBER. Servidor Postfix Total. Disponível em: <http://www.vivaolinux.com.br/artigo/Servidor-Postfix-Total>. Acesso em: 03 abr. 2012.
[20] ALECRIM, EMERSON. Entendendo a certificação digital. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 03 abr. 2012.
[21] ALECRIM, EMERSON. Criptografia. Disponível em: <http://www.infowester.com/criptografia.php>. Acesso em: 03 abr. 2012.
[22] SILVA, ALEXANDRE REIS E; STANTON, MICHAEL A. Processamento dinâmico de caminhos de certificação em ambientes distribuídos de grande porte. Disponível em: <http://www.rnp.br/newsgen/0203/processamento_dinamico.html>. Acesso em: 03 abr. 2012.
[23] KOSUTIC, DEJAN. Quatro benefícios fundamentais da implementação da ISO 27001. Disponível em: <http://blog.iso27001standard.com/pt-br/2010/12/19/quatro-beneficios-fundamentais-da-implementacao-da-iso-27001/>. Acesso em: 03 abr. 2012.
[24] INTERNATIONAL ISMS REGISTER. *Certificate Search Page*. Disponível em: <http://www.iso27001certificates.com/Taxonomy/CertificateSearch.htm>. Acesso em: 03 abr. 2012.
[25] KOSUTIC, DEJAN. Lista de verificação para implementação da ISO 27001. Disponível em: <http://blog.iso27001standard.com/pt-br/tag/procedimentos-obrigatorios/>. Acesso em: 03 abr. 2012.
[26] DEFINIÇÃO de critérios de risco. Disponível em: <http://www.iso31000qsp.org/2010/12/definicao-dos-criterios-de-risco.html>. Acesso em: 03 abr. 2012.
[27] POLÍTICA de uso do e-mail corporativo. Disponível em: <http://www.smartunion.com.br/download_artigos/Politica_Email_Smart_Union_Versao_Simples.htm>. Acesso em: 03 abr. 2012.
[28] KOSUTIC, DEJAN. Problemas com definição de escopo da norma ISO 27001. Disponível em: <http://blog.iso27001standard.com/pt-br/tag/sgsi-pt-br/>. Acesso em: 03 abr. 2012.
[29] GNU. *Various licenses and comments about them*. Disponível em: <http://www.gnu.org/licenses/license-list.html>. Acesso em: 03 abr. 2012.
[30] BERNSTEIN, D. J. *QMQP: Quick Mail Queueing Protocol*. Disponível em: <http://cr.yp.to/proto/qmqp.html>. Acesso em: 03 abr. 2012.
[31] PATTERSON, DAVID A.; GIBSON, GARTH; KATZ, RANDY H. *A case for redundant array of inexpensive disks (RAID)*. Disponível em: <http://www.cs.cmu.edu/~garth/RAIDpaper/Patterson88.pdf>. Acesso em: 03 abr. 2012.
[32] LAYTON, JEFFREY B. *Introduction to RAID*. Disponível em: <http://www.linux-mag.com/id/7924/>. Acesso em: 03 abr. 2012.
[33] *BYTE PILE. RAID Types – Classifications*. Disponível em: <http://www.bytepile.com/raid_class.php>. Acesso em: 03 abr. 2012.

[34] DE SANTANA, JOÃO LUCAS. Uma introdução ao Linux-PAM. Disponível em: <http://www.vivaolinux.com.br/artigo/Uma-introducao-ao-LinuxPAM>. Acesso em: 03 abr. 2012.
[35] BRAMSCHER, PAUL. *Creating authorities and self-signed SSL certificates*. Disponível em: <http://www.tc.umn.edu/~brams006/selfsign.html>. Acesso em: 03 abr. 2012.
[36] LEVITTE, RICHARD. *HOWTO certificates*. Disponível em: <http://www.openssl.org/docs/HOWTO/certificates.txt>. Acesso em: 03 abr. 2012.
[37] LEVITTE, RICHARD. *HOWTO keys*. Disponível em: <http://www.openssl.org/docs/HOWTO/keys.txt>. Acesso em: 03 abr. 2012.
[38] HEINLEIN, PAUL. *OpenSSL command-line HOWTO*. Disponível em: <http://www.madboa.com/geek/openssl/>. Acesso em: 03 abr. 2012.
[39] *DOVECOT – Secure IMAP Sever*. Disponível em: <http://www.dovecot.org/>. Acesso em: 03 abr. 2012.
[40] CONCEITOS de certificação digital. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/CertificadoConceitos>. Acesso em: 03 abr. 2012.
[41] LACEY, PETER. *Secure Virtual Mailserver HOWTO*. Disponível em: <http://wanderingbarque.com/howtos/mailserver/mailserver.html>. Acesso em: 03 abr. 2012.
[42] *POSTFIX documentation*. Disponível em: <http://www.postfix.org/documentation.html>. Acesso em: 03 abr. 2012.
[43] GRAND, MARK. *MIME Overview*. Disponível em: <http://mgrand.home.mindspring.com/mime.html>. Acesso em: 03 abr. 2012.
[44] BRODKIN, JON. *The MIME guys: How two internet gurus changed e-mail forever*. Disponível em: <http://www.networkworld.com/news/2011/020111-mime-internet-email.html?page=3>. Acesso em: 03 abr. 2012.
[45] IANA. *Simple Authentication and Security Layer (SASL) Mechanisms*. Disponível em: <http://www.iana.org/assignments/sasl-mechanisms/sasl-mechanisms.xml>. Acesso em: 03 abr. 2012.
[46] VINFO. Tutorial Part One: Email Basics. Disponível em: <http://www.tekguard.com/Content/Software/Tutorials/EMailTutorial_P1.htm>. Acesso em: 03/04/2012.
[47] MAR, WILSON. *Information Security Threats and Vulnerabilities*. Disponível em: <www.wilsonmar.com/1secvul.htm>. Acesso em: 03 abr. 2012.
[48] FERRAMENTA de Análise de Risco em Processos de Software. Disponível em: <http://www.maxwell.lambda.ele.puc-rio.br/10205/10205_5.PDF>. Acesso em: 03 abr. 2012.
[49] GESTÃO de pessoas. Como elaborar um plano diretor de treinamento. Disponível em: <http://www.rh.com.br/Portal/Desenvolvimento/Materia/5245/como-elaborar-um-plano-diretor-de-treinamento.html>. Acesso em: 03 abr. 2012.
[50] DALL'AGNOL, AMÉLIO. A importância do agronegócio para o Brasil. Disponível em: <http://www.agrolink.com.br/culturas/milho/noticia/a-importancia-do-agronegocio-para-o-brasil_119909.html>. Acesso em: 03 abr. 2012.