Relatório do trabalho da disciplina de Cibersegurança

Plano de Segurança: Farmácia Ideal

Lucas Braga Mendonça - 17870

Sérgio Ribeiro - 18858

José Esteves - 16960

Engenharia de Sistemas Informáticos - PL

Janeiro de 2022

ESCOLA SUPERIOR DE TECNOLOGIA IPCA

Afirmo por minha honra que não recebi qualquer apoio não autorizado na realização deste trabalho prático. Afirmo igualmente que não copiei qualquer material de livro, artigo, documento web ou de qualquer outra fonte exceto onde a origem estiver expressamente citada.

Lucas Braga Mendonça - 17870

Sérgio Ribeiro – 18858

José Esteves - 16960

Índice

Lista de Tabelas

Lista de Figuras

1. Introdução

Este relatório é baseado no trabalho prático da unidade curricular Cibersegurança, inserida no plano de estudos do curso LESI (Engenharia de Sistemas Informáticos), tendo como objetivo elaborar um plano de segurança de uma determinada instituição ou organização na área da saúde ou industrial.

O grupo decidiu optar pela área da saúde e criou a Farmácia Ideal onde iremos abordar tecnologias e estratégias para implementar na elaboração do Plano de Segurança. Pretendemos então aplicar os conhecimentos adquiridos nas aulas que iremos usar para a elaboração deste.

Nesta farmácia, o cliente pode comparecer na farmácia diretamente e indicar o que pretende, pode pedir ajuda profissional para que os farmacêuticos o consigam atender e ajudar devidamente, ou até mesmo trazer uma receita em papel ou por mensagem dada por um médico.

Os dados de cada compra são guardados na base de dados. Como cada vez que chega um novo stock de remédios à farmácia, também é necessário guardar na base de dados e atualizar o inventário do estabelecimento.

1.1 Contactos

Tabela 1. Tabela de contactos

Tipo Contacto	Telefone	Email
Apoio	217111111	apoio@famarciaideal.pt
Encomendas	217222222	encomendas@famarciaideal.pt

Pagamentos	217333333	cobrancas@famarciaideal.pt
Protocolos	217444444	encomendas@famarciaideal.pt

Morada
Rua Rosa Ramalho Barcelos, nº33 4750-ZZZ

1.2 Funções e Responsabilidades

Há duas funções distintas, o gerente do sistema e os funcionários gerais. Passo a citar as responsabilidades de cada um:

- Gerente do Sistema: O gerente do sistema é responsável por gerir as pessoas dentro de sua equipa, neste caso os funcionários, gerir e priorizar os projetos de TI, desenvolver novas estratégias assim como analisar novas tecnologias e por fim garantir a segurança de informações.
- Funcionários Gerais: Os funcionários gerais são responsáveis por conhecer o negócio, usar correctamente o sistema consoante as normas de segurança abordadas no início da formação, otimizar a utilização de recursos, reportar incidentes e garantir a segurança da informação como não divulgar o funcionamento dos sistemas nem os conhecimentos que tenham sobre o plano de segurança a pessoas fora da empresa.

2. Caracterização do Sistema de Informação

2.1. Políticas de Segurança

O sistema desenvolvido a partir do plano de segurança irá respeitar os seguintes objetivos:

- Confidencialidade: a confidencialidade é a propriedade da informação que não estará disponível ou divulgada a indivíduos não autorizados, o que quer dizer que a extração de dados não autorizada poderá afetar negativamente a segurança do sistema.
- Integridade: a integridade é a proteção contra a modificação ou destruição de informação inadequada sendo que os dados guardados no sistema permanecerão inalterados até que uma ordem contrária seja apresentada.
- Disponibilidade: a disponibilidade garante o acesso oportuno e viável e uso de informação. É importante que o acesso à informação esteja constantemente disponível e que este seja feito com facilidade e com agilidade.

2.2. Descrição Geral da Farmácia

O processo iniciou-se no contacto de um potencial cliente com um farmacêutico, através de um balcão da própria farmácia ou de outra entidade que o represente, designado por agente medidor. Este agente pode ser um balcão de um hospital ou uma pessoa em particular, sendo que todas as entidades precisam de um parecer legal para exercer tal atividade. O interesse do potencial cliente retém-se com o objetivo de pretender comprar um produto com diferentes afins como tratar da sua saúde, tratar da saúde de outrem, etc.

Esse interesse traduz-se numa proposta que, em termos gerais, é um produto que o cliente usa para melhorar e estabelecer a sua saúde física ou mental. O cliente tem várias escolhas de atendimento que passo a citar: o cliente pode comparecer

na farmácia diretamente e indicar o que pretende, pode pedir ajuda profissional para que os farmacêuticos o consigam atender e ajudar devidamente, ou até mesmo trazer uma receita em papel ou por mensagem dada por um médico.

O farmacêutico irá dar ajuda profissional caso seja solicitado ou necessário assim como arranjar o produto pretendido registrando os dados da compra no software (data de compra, nome do produto, etc).

Os dados de cada compra são guardados na base de dados. Como cada vez que chega um novo stock de remédios à farmácia, também é necessário guardar na base de dados e atualizar o inventário do estabelecimento.

Após o cliente mostrar a receita ao farmacêutico este irá primeiro ver se o/os produto/os encontram-se e stock. Caso não se encontrem em stock poderá ver que outras farmácias têm e comunicar ao cliente. Se no caso tiverem o produto, o farmacêutico irá assinalar o mesmo no software o que vai fazer com que a sua quantidade no stock diminuía e todas as farmácias consigam ter acesso a essa informação.

Os clientes podem ter as receitas como forma de mensagem no telemóvel que irão ter de ser validadas vendo se a mensagem vem de alguma organização de saúde.

O gestor do estabelecimento tem acesso à saída e entrada de todo o stock de medicamentos, bem como todas receitas recebidas e dadas. Não tem acesso a todas informações de cada funcionário, mas tem acesso a cada receita dada por cada funcionário e a cada login feito (hora e dia feito, e medicamentos dados pela mesma).

2.3. Ambiente e Interconexão de Informação do sistema

O sistema da Farmácia Ideal é composto por uma rede interna de computadores que se encontram em constante comunicação com o servidor local. Este também está interligado à Rede de Informação da Saúde que é uma rede privada multimédia do Ministério da Saúde que interliga as redes locais dos seus organismos e serviços.

2.4. Dependências do Sistema

Visto que um sistema necessita de um conjunto de dependências de recursos para a análise de transporte, processamento ou armazenamento de dados, foram identificadas as seguintes mesmas:

- Ligação à internet;
- Firewall;
- VPN;
- Ambientes de execução dedicados;
- Análise antivírus;
- Interligação à Rede de informação Nacional de Saúde;
- Cartões eletrónicos de funcionários;
- Access Lists pré-configuradas nos dispositivos de rede local de modo a filtrar tipo de tráfego de entrada e saída;
- Servidores criptografados.

2.4.1. Programas e Aplicações Suportadas

O sistema suporta a utilização dos seguintes programas:

- Sistema de informação da farmácia;
- Sistema de vendas;
- Correio eletrónico (Email);
- Sistema de base de dados.

3. Controlos de Gestão do Sistema

3.1. Certificação, Acreditação e Avaliações de Segurança

3.1.1. Certificação, Acreditação e Avaliações de Segurança e Procedimentos

Primeiramente temos de tomar uma decisão, isto é, decidir que queremos obter uma certificação, sendo que neste trabalho preparatório temos de estabelecer os objetivos, decidir quais os recursos e elaborar um plano de ação e selecionar a empresa consultora.

Após decidir a empresa consultora esta deverá realizar avaliações de segurança e políticas de certificação apresentando então, os objetivos estabelecidos, papéis de responsabilidade, compromisso de gestão e conformidade com a Farmácia Ideal.

3.1.2. Avaliações de segurança

A empresa consultora deve fazer uma análise detalhada e minuciosa para minimizar os riscos que determinadas ações podem gerar. Deverá fazer uma análise qualitativa onde irá, a partir de uma check list, registar onde estão os riscos e qual o grau destes. Deverá também fazer uma análise quantitativa para avaliar a quantidade de riscos presentes. Com estas observações pode-se criar ações de segurança.

3.1.3. Certificação de segurança

O referencial ISSO 27001 fornece uma estrutura para implementar um SGSI, salvaguardando os seus ativos de informação e, ao mesmo tempo, facilitar a gestão, a avaliação e a melhoria do processo. Esta norma irá ajudar-nos a abordar as três dimensões da segurança da informação anteriormente vistas: Confidencialidade, Integridade e Disponibilidade.

3.1.4. Plano de ações e metas

O primeiro passo para montar o plano de ação e metas é considerar o planejamento estratégico da empresa. De seguida temos de criar metas mensuráveis e listar as tarefas a serem executadas. Após as ações anteriores realizadas dividiremos as grandes tarefas em partes menores e gerenciáveis para que seja mais fácil atingir todas as metas. É bastante importante também criar prazos para as entregas pois vai ser mais fácil planear a execução das atividades priorizando as metas mais importantes. Por fim, basta acompanhar as ações com frequência para ajudar a equipa a completar o máximo número de metas possível.

3.1.5. Monitorização

O bloco de construção irá suportar:

- Autorização e verificação de software a ser instalado;
- Lista de permissões de execução de software;
- Manutenção do inventário de software instalado;
- Controle de acesso à rede baseado no inventário do software.

3.2 Planeamento de segurança do sistema

O plano de segurança do sistema pode ser definido como o conjunto de avaliações e decisões a serem tomadas em âmbito intermediário da organização, com objetivo de suportar o sistema de gestão da segurança.

Objetivos:

- Identificar e unificar objetivos de segurança;
- Avaliar e controlar os riscos potenciais;
- Implementar normas, procedimentos, ações e atividades;
- Minimizar os riscos e maximizar os pontos fortes do sistema.

Critérios:

- Manter o software de diagnóstico no local;
- Procura por falhas no sistema;
- Monitorização do login;
- Atualizações dos dispositivos ligados à rede;
- Criar backups.

O sistema irá possuir firewalls que restringem o acesso a serviços menos aqueles que necessitam de permanecer executados.

Cada funcionário irá possuir um cartão pessoal que será necessário usar para iniciar a sua estação de trabalho assim como colocar a sua palavra-passe.

As palavras-passe deverão ser:

- 14 ou mais caracteres de comprimento;
- Combinação de letras maiúsculas, minúsculas, números e símbolos;
- Diferente de palavras-passe já usadas em outras aplicações;
- Ex: A9*sQi%&Mak,y/

O sistema também terá o uso de um VPN para disfarçar o tráfego de dados online e proteger de acesso externo. Ao trabalhar remotamente, podemos precisar de acessar arquivos importantes na rede da empresa, então, com o uso do VPN, fica mais seguro completar esta ação.

Por fim temos uma lista de requisitos de segurança que devem ser citados:

- O software de antivírus deverá ser atualizado frequentemente;
- Toda a infraestrutura de rede do sistema deverá estar identificada e protegida;
- Videovigilância;
- O acesso ao hardware deve ser controlado e registrado eletronicamente;
- O acesso a salas específicas deverá ter um papel para que cada pessoa que lá entre possa assinar a que hora entrou e saiu;
- Access Lists para controle e filtragem de tráfego.

3.3. Avaliação de Risco

3.3.1. Objetivos de Segurança

Existem três objetivos de segurança, que por sua vez já foram citados anteriormente, que são:

- Confidencialidade: assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é restrito a utilizadores considerados legítimos.
- Integridade: garantir a veracidade, autenticidade, e exatidão da informação, bem como os seus métodos de processamento ao longo de todo o processo, garantindo que o conteúdo não seja adulterado.
- Disponibilidade: assegurar o acesso à informação, a quem se encontre devidamente credenciado e legitimamente autorizado. A informação está acessível quando se revelar necessária.
- Legitimidade: a recolha de informação é feita nos estritos limites da lei que é aplicável ao objeto de recolha.

3.3.2. Avaliação de Risco

A abordagem da avaliação de riscos vai ser dividida em 5 etapas.

1ª Etapa: Identificação dos perigos à análise dos aspectos do trabalho que podem causar riscos;

2ª Etapa: Avaliação e priorização dos riscos à Apreciação dos riscos existentes e classificação dos mesmos;

3ª Etapa: Decisão sobre medidas preventivas à Identificação de medidas adequadas para eliminar ou controlar os riscos;

4ª Etapa: Adoção de medidas de prevenção e proteção à Uso de um plano de prioridades;

5ª Etapa: Acompanhamento e revisão à avaliação deve ser revista regularmente para assegurar que se mantenha atualizada.

3.3.3. Procura de vulnerabilidades

Tabela 2. Tabela de vulnerabilidades

Vulnerabilidades	Nivel de Risco Baixo	Nivel de Risco médio	Nivel de Risco Alto
Falha de equipamentos		**X**	
Erros de Software		**X**	
Falha de Eletricidade		**X**	
Exposição de software malicioso			**X**
Ataques cibernéticos			**X**
Incêndios		**X**	

3.4. Aquisição de Sistemas e Serviços

3.4.1 Aquisições

O sistema informático trata da aquisição e gestão do hardware de todos os serviços centrais e administrativos onde se incluem:

- Equipamento – computadores, monitores, impressoras, etc;
- Componentes – memórias, placas de rede, discos rigidos, etc;
- Dispositivos de redes – switches, hubs e routers;
- Servidores;
- Software.

3.4.2 Restrições do uso de software

Os softwares disponíveis aos funcionários e utilizadores estão devidamente licenciados e registrados, sendo que qualquer cópia destes poderá ser penalizada por lei.

4. Controles Operacionais

4.1 Consciencialização e Formação

4.1.1 Consciencialização da segurança

São aplicáveis políticas de conduta aos utilizadores do sistema de modo a respeitar as normas de utilização.

4.1.2 Formação sobre Segurança

A própria Farmácia irá oferecer formação de consciencialização de segurança básica para todos os utilizadores do sistema de informação, de maneira que estes o possam utilizar de forma mais correta e segura a sua infraestrutura tecnológica de forma geral.

4.2 Gestão da Configuração

4.2.1 Configuração Base

O sistema de informação da Farmácia Ideal apresenta uma configuração baseada num servidor local que se encontra configurado tanto para suportar o sistema de vendas e a base de dados acerca do inventário da farmácia, como também para poder comunicar diretamente com o Ministério da Saúde, através de uma rede privada.

A restante infraestrutura de equipamentos baseia-se em terminais de trabalho para os funcionários da Farmácia que estão conectados diretamente com o servidor.

4.2.2 Controlo de modificações na configuração

Qualquer modificação na configuração do sistema terá de ser previamente aprovado e efetuado pelo Gerente dos Sistemas Informáticos e claro, com o consentimento e conhecimento da equipa dos Funcionários da Farmácia.

Isto através de um processo organizacional que irá então anunciar todas as modificações às configurações do sistema, como sistemas operativos, bases de dados, infraestrutura e dispositivos de rede, e medidas de segurança e efetuar então as tais alterações.

4.2.3 Monitorização das Modificações na Configuração

Qualquer modificação no sistema de informação irá ser testada antes ser posta numa situação real na Farmácia, para não dificultar os encargos dos Funcionários da Farmácia. Após uma série de testes realizados pelo Gerente dos Sistemas de Informação, aí sim, é feita a tal modificação.

4.2.4 Restrições de Acesso para Modificações

Somente pessoal especializado ao serviço, como o Gerente dos Sistemas, poderá ter acesso para isso. No caso de ser necessário uma mudança mais rebusca, poderá então ser necessário contratar uma equipa para auxiliar na tal atualização/modificação do sistema.

4.2.5 Inventário de Componentes do Sistema

Tabela 1. Componentes do sistema

Componente	Marca/Modelo
Servidor	HP ProLiant 2500
Desktop	HP 800 G2 TORRE
Router	Cisco Router 2500
Switch	Cisco Switch 1800

4.3 Plano de Contingência

4.3.1 Plano de Contingência

Em caso de falha do sistema ou qualquer catástrofe, o sistema detém um plano de contingência de modo a minimizar os danos e recuperar dos mesmos que vai ser descrito agora.

4.3.2 Formação de Contingência

É dada formação aos funcionários da Farmácia de modo a possuírem conhecimentos de como agir em caso de catástrofe natural ou qualquer outra situação de inoperabilidadedo sistema. Esta formação terá que ser dada por uma empresa do ramo da segurança dos sistemas de informação, de maneira a obterem um conhecimento mais fidedigno e correto acerca do tema.

4.3.3 Exercícios de Teste ao Plano de Contingência

O plano de contingência é sujeito a uma série de testes regulares de forma a garantir que a Farmácia detém os devidos meios para combater determinadas eventualidades.

4.3.4 Atualização do Plano de Contingência

No decorrer de análises contínuas ao plano de contingência, em caso de deteção de novas variáveis, possíveis eventualidades e falhas no plano, este é atualizado de acordo com os novos dados recolhidos pela empresa que realizou a análise e encontrou a tal falha, por exemplo, numa auditoria feita por uma empresa local que se realiza trimestralmente ao ano.

4.3.5 Local Alternativo de Armazenamento

O local alternativo de armazenamento de dados e backups físico foi definido para as instalações da Checkmarx. Este local disponibiliza claro, instalações prontas para armazenar dados acerta dos clientes da Farmácia Ideal, das vendas e do inventário das instalações.

4.3.6 Serviços de Telecomunicações

Em caso de falha técnica, os serviços de telecomunicação alternativos serão garantidos pela empresa NOS, que garantiu um plano de comunicações na ocorrência destes casos.

4.3.7 Cópia de Segurança do Sistema

O sistema de informação da Farmácia possui uma cópia de segurança na Checkmarx, para além do já mencionado local alternativo de armazenamento.

4.3.8 Recuperação e Reconstituição do Sistema

O sistema de informação da Farmácia possui mecanismos de reconstituição das funcionalidades, dados e estado do sistema anterior ao incidente através das cópias de segurança armazenadas nos locais já referidos.

4.4 Resposta a Incidentes

4.4.1 Formação de Resposta a Incidentes

A Farmácia Ideal nas suas várias formações acerca de Segurança dos Sistemas Informáticos, contêm também este tema.

4.4.2 Exercícios de Teste à Resposta a Incidentes

Duas vezes ao ano é necessário efetuar testes do género, efetuados e supervisionados pelo Gerente dos Sistemas, de maneira a garantir, numa situação real, uma resposta adequada ao acontecimento em causa.

4.4.3 Monitorização de Incidentes

A monotorização dos incidentes e as suas soluções é efetuada por uma empresa local, a SafeWork, empresa especializada em resolver e acompanhar empresas de média e pequena escala neste tipo de situações.

4.4.4 Notificação de Incidentes

A notificação de um incidente é efectuada pelo Gerente de Sistemas à empresa SafeWork, que tratara de acompanhar o acontecimento.

No caso de o incidente atrapalhar gravemente a organização normal da Farmácia, também irá ser comunicado ao Ministério de Saúde o acontecido.

4.4.5 Assistência a Resposta a Incidentes

Para além da tal monotorização que já foi mencionada em cima, a empresa SafeWork disponibiliza também os seus serviços para assistir a Farmácia Ideal na ocorrência de um incidente.

4.5 Manutenção

4.5.1 Manutenção Controlada

A farmácia possui acordos de verificação e manutenção periódicos para com a SafeWork, de modo a garantir o bom funcionamento e integridade do sistema.

4.5.2 Ferramentas de Manutenção

O sistema de informação da Farmácia Ideal possui algumas ferramentas de manutenção e de notificação automáticas que alertam o Gerente de Sistemas de incidentes que possam ocorrer no sistema de forma a agir o mais rápido possível na sua resolução. Alguns incidentes são autossolucionáveis com o uso de ferramentas de gestão. No caso de isso não acontecer, então é comunicado com à SafeWork o sucedido.

4.5.3 Responsáveis pela Manutenção

A entidade principal responsável pela manutenção do sistema é a SafeWork. No caso da mesma não conseguir lidar com algum problema ou inconveniente, é reportado ao Gerente de Sistemas e então encaminhado para uma organização mais especializada na manutenção do que em segurança.

4.6 Proteção de Meios de Armazenamento Digital de Dados

4.6.1 Acesso

O acesso de armazenamento digital de informação da Farmácia é restrito ao Gestor dos Sistemas.

4.6.2 Rotulagem

A rotulagem deve ser efetuada através de um procedimento sequencial, ou seja, com o dia da sua rotulação e o nome do responsável que o fez. Mais uma vez, apenas o Gestor dos Sistemas tem acesso para o fazer. Os outros funcionários apenas podem realizar ações de consulta ou pesquisa.

4.6.3 Armazenamento

As cópias de segurança dos dados estão armazenadas na Checkmarx.

4.6.4 Transporte

Caso exista necessidade de transporte de drives para um outro local exterior à Farmácia, tal deve ser feito por funcionários destacados para o efeito ou pela empresa de segurança.

4.6.5 Destruição

No caso de haver a necessidade de destruição de informação, de forma a garantir a confidencialidade da informação existente no seu interior, ou algum inconveniente que comprometa a segurança da informação armazenada, tal deverá ser assegurado pelo Gestor de Sistemas e pela a empresa que acompanha e ajuda na questão da base de dados, a Checkmarx.

4.7 Proteção Física

4.7.1 Autorizações de Acesso Físico

A Farmácia Ideal realiza testes mensais, de maneira a verificar se todos os requisitos funcionais, de segurança e ecológicos estão dentro das normais e políticas formais que definem os mesmos requisitos.

A publicação “NIST SP 800-12” fornece orientação sobre políticas e procedimentos de segurança.

4.7.2 Controlo de Acesso Físico

A Farmácia Ideal garante acesso físico aos Desktops a todos os funcionários. Switch e Rooter também. O Servidor por sua vez apenas pode ser acedido pelo Gestor de Sistemas, devido à importância e fragilidade do componente.

O controlo de acesso físico pode passar por chaves ou leitor de cartões.

4.7.3 Controlo de Acesso a Meios de Transmissão de Dados

A Farmácia Ideal tem uma política muito rígida acerca da transmissão de qualquer tipo de transmissão de dados. Para ter permissão para tal, no caso de ser apenas um Funcionário, é necessário efetuar login com as suas credencias pessoais, informar o Gestor de Sistemas e só após a confirmação do mesmo, é que poderá proceder à transmissão dos dados.

4.7.4 Controlo de Acesso a Meios de Exibição de Dados

A Farmácia também controla o acesso físico aos dispositivos de informação do sistema que exibem informações para impedir a entrada de pessoas não autorizadas.

4.7.5 Monitorização de Acessos Físicos

O Gestor de Sistemas monitoriza o acesso físico ao sistema de informações para detetar e responder a incidentes de segurança física, analisando periodicamente os Logs de acesso físico e investigando aparentes violações de segurança ou atividades suspeitas de acesso físico.

4.7.6 Equipamento e Cablagens Elétricas

A Farmácia Ideal protege equipamentos de energia e cablagens de energia para o sistema de informações de danos e destruição.

4.7.7 Corte de Energia (Emergência)

A Farmácia Ideal fornece, para locais específicos, a capacidade de desligar a alimentação de qualquer componente do sistema de informações que podem não estar a funcionar corretamente ou ameaçados, sem colocar em perigo os funcionários.

Os Funcionários durante a sua formação na Farmácia serão devidamente ensinados como proceder neste tipo de incidentes e claro, onde se situam estes locais em que se realiza o corte de energia.

4.7.8. Eletricidade de Emergência

A Farmácia Ideal fornece um curto prazo de fornecimento de energia ininterrupta para facilitar o desligamento ordenado do sistema de informação em caso de uma perda da principal fonte de alimentação, isto através de uma fonte de energia secundária, idealizada para este tipo de situações.

4.7.9. Iluminação de Emergência

A Farmácia também fornece iluminação de emergência automática que ativa em caso de falta de energia que cobre as saídas de emergência e rotas de evacuação.

4.7.10 Proteção Contra Incêndios

A Farmácia fornece, em caso de incêndio, extintores e dispositivos de deteção que podem ser ativados em caso de emergência, como, sistemas de aspersão, mangueiras, e detetores de fumo.

4.7.11 Fornecimento e Remoção

A Farmácia Ideal controla os itens relacionados com o sistema que entram e saem da instalação e mantem registos apropriados. Isto porque o controlo do inventário é extremamente importante neste caso.

4.7.12. Localização dos Componentes do Sistema de Informação

A Farmácia posiciona os componentes de sistemas de informação dentro das instalações para minimizar os danos potenciais de riscos físicos e ambientais e minimizar a possibilidade de acesso não autorizado.

4.8 Integridade do Sistema e da Informação

4.8.1 Recuperação de Falhas

A Farmácia identifica e relata os componentes afetados, que contem software danificado. Após esse relato, é comunicado à empresa SafeWork o acontecimento e a mesma irá proceder para solucionar o problema.

4.8.2 Proteção Contra Código Malicioso

O sistema de informação implementa proteção contra código malicioso, utilizando mecanismos de proteção nas entradas de informação críticas do sistema e pontos de saída (firewall).

A publicação “NIST SP 800-83” fornece orientação sobre a implementação de proteção de código malicioso.

Em casos mais graves, o Gestor de Sistemas decidirá como proceder e se é necessário comunicar com alguma organização para solucionar o problema

4.8.3 Ferramentas e Técnicas de Monitorização do Sistema de Informação

A Farmácia usa ferramentas e técnicas para monitorizar eventos no sistema de informação, detetar ataques, e fornecer a identificação de uso não autorizado do sistema, utilizando sistemas de deteção e prevenção de intrusão ou software de monitoramento de rede.

4.8.4 Verificação de Funcionalidades de Segurança

O próprio sistema de informação verifica o correto funcionamento das funções de segurança, notifica o Gestor de Sistemas de Imformação.

4.8.5 Integridade do Software e da Informação

O sistema de informação deteta e protege contra alterações não autorizadas de software e outras informações.

4.8.6 Proteção Anti-Spam

O sistema de informação implementa proteção contra spam nos pontos críticos do sistema de entrada (firewall) e em estações de trabalho ou dispositivos que estejam ligados na rede.

A publicação “NIST SP 800-45” fornece orientação sobre a segurança de correio eletrónico.

4.8.7 Restrições de Inserção de Informação no Sistema

Só é permitido inserir novos dados, quer seja de novos funcionários, ou de novos medicamentos, acedendo com as credencias pessoais de cada funcionário. No caso do movimento em causa seja duvidoso (por exemplo, remoção inesperada de um medicamento), a operação é parada e é notificado o Gestor de Sistemas.

4.8.8 Gestão de Erros

O sistema de informação identifica e trata as condições de erro de forma autónoma. À medida em que o sistema de informação é incapaz de o fazer, o Gestor de Sistemas irá analisar a situação e se necessário, encaminhar o processo para uma organização solucionar o problema.

5. Controle Técnico

Neste capítulo serão enunciadas mais detalhadamente as ferramentas e normas para um controle técnico na gestão de riscos no contexto de *cibersegurança*. Aqui serão abordados os principais pontos que podem fazer do sistema farmacêutico em questão mais seguro e confiável. Assim como devem ser instruídas as pessoas que estejam inseridas neste ambiente, nomeadamente funcionários e farmacêuticos da empresa.

5.1. Controlo de acesso

Sendo o principal objetivo de o controlo de acesso minimizar o risco de que pessoas não autorizadas tenham acesso a material sensível, como é o caso dos medicamentos de uma farmácia, ou até mesmo de acesso a informações privilegiadas, foi estruturada uma arquitetura de acesso que garante o sigilo e integridade dos dados e bens materiais. Dividem-se em dois grupos:

a) **Controle de acesso físico**: permite a proteção de espaços físicos, como o próprio nome já diz. Como por exemplo em nosso caso, às instalações da farmácia com acesso restrito aos seus funcionários. Para esses espaços mais restritos dentro da própria farmácia, será utilizado a biometria por reconhecimento facial e a entrada da farmácia será aberta (na primeira vez) através de um cartão RFID que é um método de identificação automática através de sinais de rádio.

Figura 1. Acesso com tecnlogia RFID

b) **Controle de acesso lógico**: tem a função de proteger os bens digitais, limitando o acesso ao sistema farmacêutico, de forma a proteger os dados e informações confidenciais, assim como impedindo a atualização e consequente integridade dos dados nele contidos. A ideia seria dividir os utilizadores em grupos de segurança, como é no caso do sistema operacional Windows. Os direitos de usuário são atribuídos automaticamente a alguns grupos de segurança quando o Active Directory é instalado para ajudar os administradores a definir a função administrativa de uma pessoa no domínio. Depois de ter restringido o acesso a nível de sistema operacional, no acesso a nível de Sistema de Gestão Farmacêutico, os funcionários usariam credenciais móveis com o *app Microsoft Authenticator*, onde os utilizadores podem iniciar sua sessão através da notificação para o seu telemóvel,

correspondendo um número exibido no ecrã ao do telemóvel e, em seguida, utilizando o seu biométrico (toque ou rosto) ou PIN para confirmar, como uma camada de proteção adicional de logon. O acesso ao sistema é exclusivo de Desktops devidamente configurados para tal acesso e não pode ser efetuado por outros tipos de dispositivos.

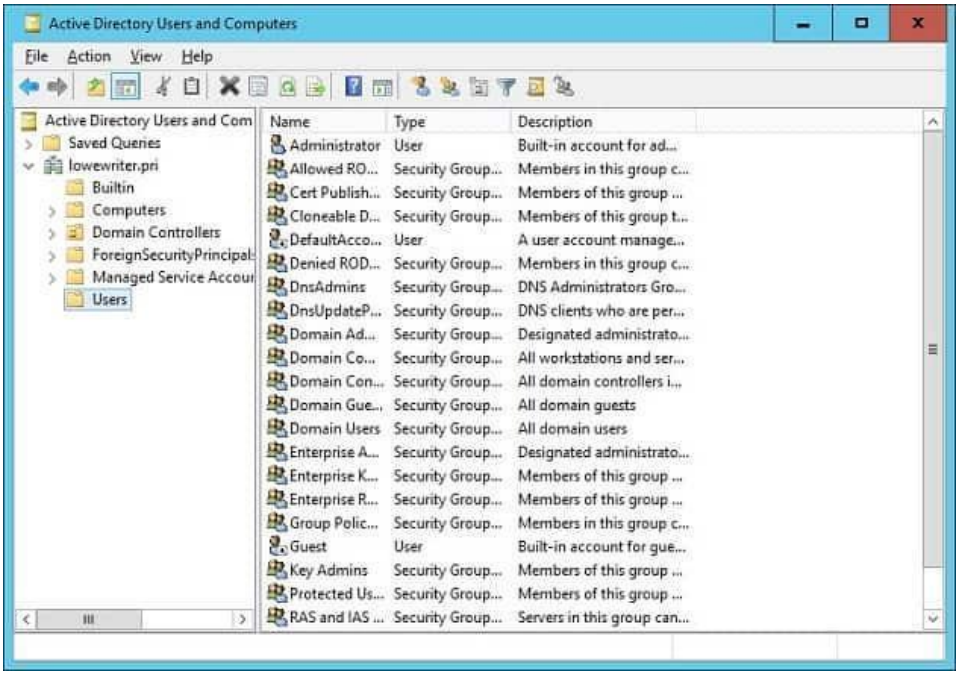

Figura 2. Active Directory do Windows

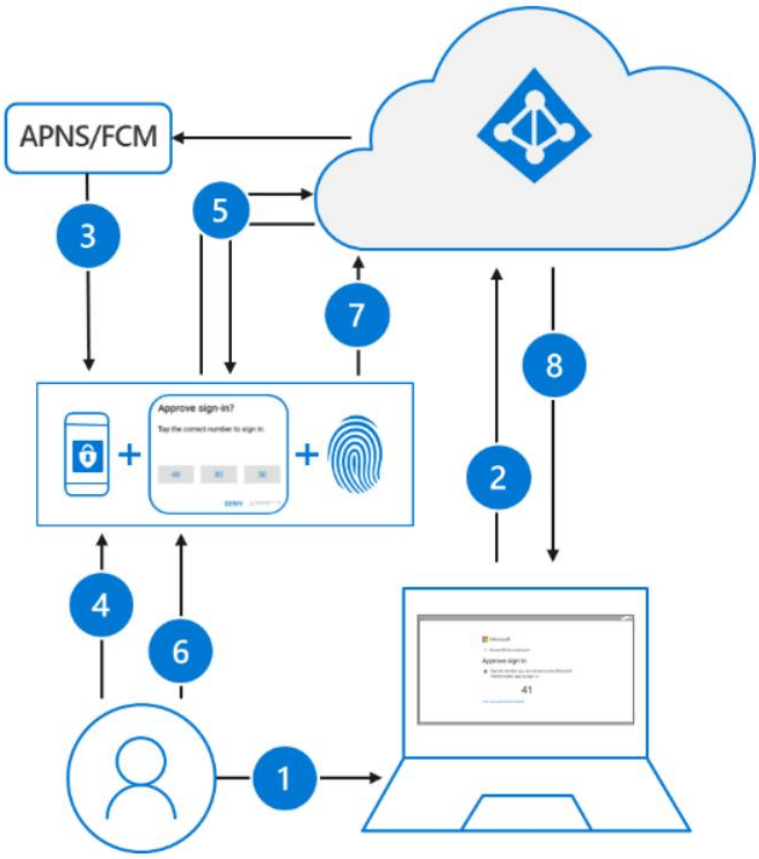

Figura 3. Autenticação adicional com o Microsoft Authenticator

Em ambos os casos, o sistema interno irá fornecer e registrar informações detalhadas com a produção de alguns relatórios em casos de análise em incidentes de segurança. É preciso ainda, ter controle e informação real sobre o número de pessoas que se encontram dentro da instalação, o que é extremamente relevante em tempos de pandemia e caso haja uma emergência em que seja preciso controlar a capacidade máxima de uma área. Além disso, pode ser necessário um acesso remoto ao sistema, que deve ser feito através de VPN, com um login e senha de segurança, normalmente de posse do administrador da farmácia para que bloqueios e restrições de acesso possam ser feitos à distância, numa eventualidade de algum risco iminente, assim como o bloqueio a determinados espaços, também de maneira online.

A publicação “NIST SP 800-63” e a “NIST SP 800-77” fornecem, respectivamente, orientações sobre autenticações remotas e IPsec baseados em VPNs.

5.1.1. Processo automatizado de acesso e controlo a medicamentos

O processo automatizado que permite a melhor utilização do espaço, além de acomodar e acondicionar mais os medicamentos na região do estoque, otimizando o processo, é feito por um sistema robotizado. Este sistema guarda os medicamentos, possibilita a gestão de estoque de forma automática e faz os demais registros sem a intervenção humana.

Figura 4. Automação por sistema robotizado

Com a implantação deste robô é feito um controle de estoque maior e sem riscos de intervenção humana e ainda auxilia na administração de remédios aos pacientes. Para acessar tal equipamento, deve ser feita a leitura biométrica do profissional, assim acarretando menores riscos de serem expostos medicamentos de forma irregular. O sistema também emite avisos de reposição de medicamentos, além de corrigir o farmacêutico caso este assinale um medicamento errado, baseado na receita ou no histórico do paciente. É possível suspender de forma automática também todos os medicamentos fora da validade.

5.2. Conformidade do Sistema com a LGPD

Torna-se necessário que o sistema da Farmácia Ideal faça o registro de operações e tratamentos de dados pessoais de seus clientes, dispondo que este saiba de forma clara e acessível, todas as informações que seus dados terão e para que fins foram coletados. Ainda, é preciso haver um termo de consentimento por parte do cliente.

Com relação aos dados em si, estes devem ser criptografados. A ISO 27001 recomenda que seja desenvolvida e implementada uma Política de Criptografia para proteção da informação, garantindo assim, a conformidade com a norma e requisitos legais, bem como a manutenção segura das informações no transporte, armazenamento e com a devida restrição de acesso. O nosso foco é conseguir transferir a responsabilidade da criptografia desses dados para um *SECaaS* (Security as a Service), ou seja, um negócio com modelo de subscrição em que um provedor de serviços web é integrado com os dados que estão em sistema e os mantém seguros. Podem incluir a detecção de intrusos e o fornecimento de ferramentas de antivírus. Esse *SECaaS* pode ser o da própria Azure (já que iremos utilizar alguns serviços deles como o de autenticação), como o de terceiros (dependendo do preço de mercado).

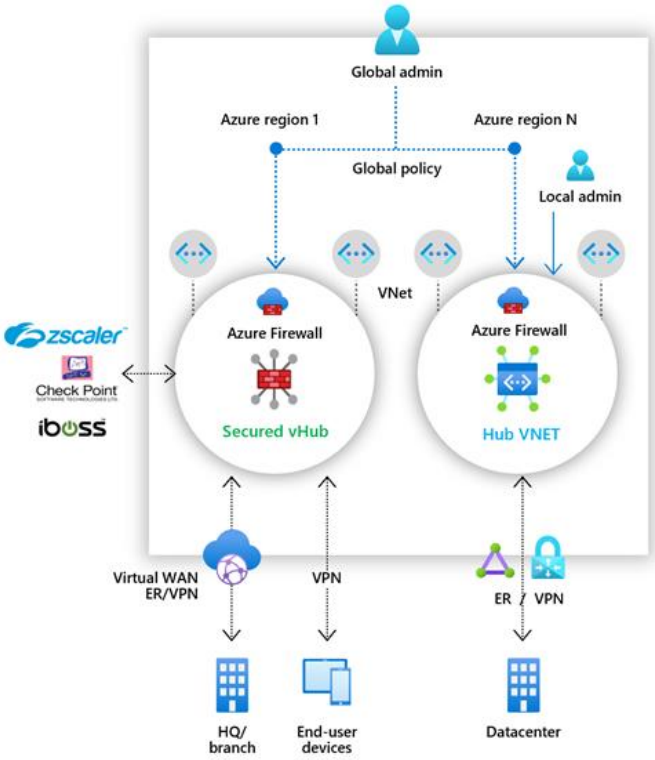

Figura 5. Arquitetura com criptografia e segurança dos dados

“Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.” Artigo 42 da Lei nº 13.709 de 14 de Agosto de 2018.

5.3. Monitoramente de tráfego da rede

É importante salientar o uso de uma ferramenta de diagnóstico e monitoramento de rede e para isso, escolhemos usar o *CloudStats* que é um software gratuito e nos permite saber o que trafega em cada ponto da rede interna ou do servidor, no caso da contratação de serviços, em tempo real. Essa ferramenta é uma ferramenta interna da farmácia que auxilia no controle à riscos, além da manutenção habitual da empresa externa SafeWork.

Permite identificar qual é o volume de tráfego na rede, quais protocolos que o compõe, qual aplicações são consumidas em maior parte facilitando mensurar sua utilizaçao e verificar possíveis subutilizações de recursos ou até mesmo prever incidentes na rede e servidor. É importante que haja um funcionamento contínuo do sistema para garantir que a rede não caia em momentos inoportunos.

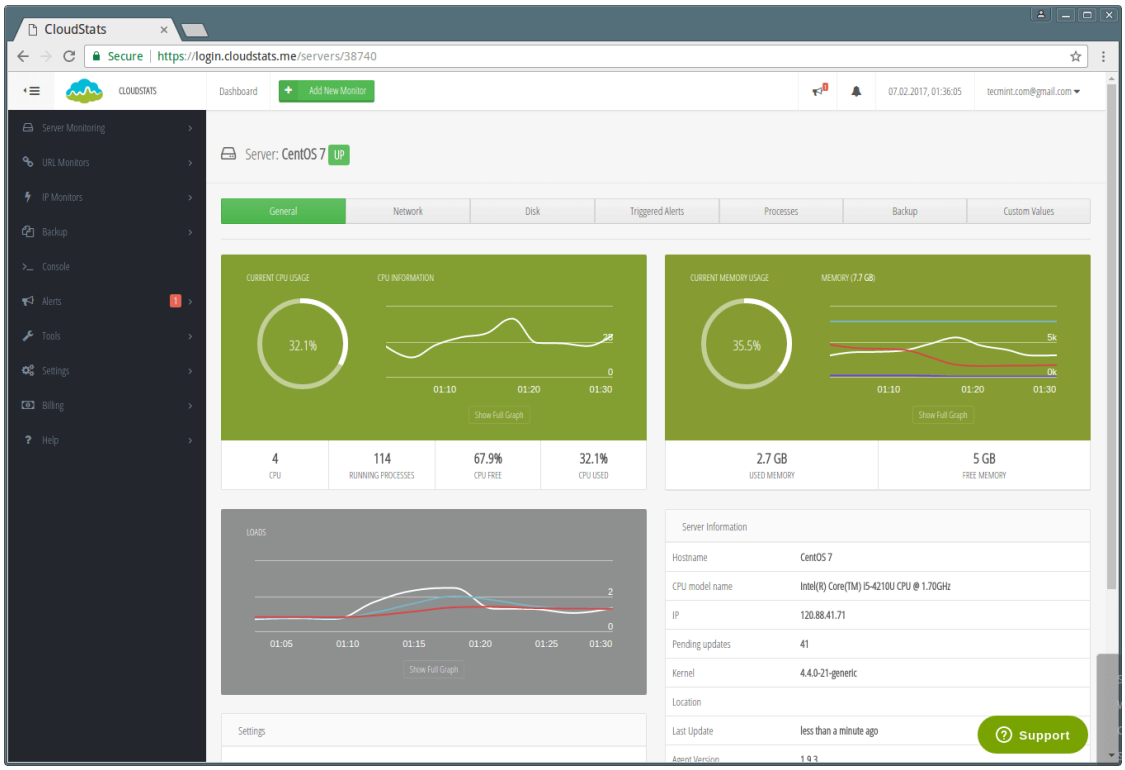

Figura 6. Overview do servidor com CloudStats

5.4. Normas e recomendações gerais

Assim como o tratamento do utente depende da administração correta dos seus medicamentos e do bom atendimento efetuado nas mais diversas farmácias, também faz parte do funcionário proteger estes mesmos utentes da exposição dos seus dados pessoais a terceiros, assim como acesso indevido, alterações e até mesmo destruição de informação sigilosa.

As principais recomendações para uso do sistema proposto, não só por nós fabricantes do software em questão, mas também pela ordem dos farmacêuticos são:

1. Confirmar que não existe nenhuma atualização a ser feita no sistema ou alguma mensagem que seja suspeita por validar;

2. Ter plena noção que todos os dias surgem novo vírus e por isso devemos ter os sistemas atualizados;

3. Utilizar apenas minha credencial ao acessar os sistemas e não a de outros colegas;

4. Não instalar nada no PC de trabalho que comprometa as informações que estão presentes no mesmo;

5. Não clicar em hiperligações de origem desconhecida.

Além disso, é importante ressaltar a importância de inclusão dos funcionários em cursos de cibersegurança, para que descuidos como estes enumerados ocorram cada vez menos.

5.5. Auditoria e Responsabilização

De forma a tentar proteger as informações confidenciais no sistema farmacêutico, é necessário o monitoramento de alterações e as tentativas de acesso não autorizado a dados sensíveis. O sistema de informação deve ser capaz de produzir registros de auditoria que contém informações necessárias para garantir a averiguação de um determinado incidente, tal como data e hora, utilizador (desconhecido ou não), tipo do incidente e a consequência da ação. Sendo assim, devem ficar registrados todos os logs de segurança e logs adicionais para monitoramento usual do sistema como um todo. Além disso, o nosso sistema farmacêutico deve estar em conformidade com a norma de segurança internacional HIPAA.

5.5.1. Conformidade com HIPAA

A norma HIPAA exige que as organizações abrangidas implementem alguns tipos de proteção para as Informações Eletrônicas Protegidas de Saúde (ePHI), onde é

feito uma referência específica à criptografia dos dados, a controlo de acesso, gerenciamento das chaves de criptografia, gestão do risco, auditoria e monitoramento de informações sigilosas. O módulo criptográfico usado para assinar digitalmente os elementos têm de ser, no mínimo, FIPS 140-2 Nível 1 validado e que a chave privada do aplicativo farmacêutico deva ser armazenada criptografada.

O Windows 10 e o Windows Server podem ser configurados para serem executados em um modo de operação aprovado pelo FIPS 140-2, comumente chamado de "modo FIPS". Para o sistema da Farmácia Ideal é garantido que todos os serviços do Azure usem algoritmos aprovados pelo FIPS 140 para segurança de dados porque o sistema operacional baseado em nuvem usa algoritmos aprovados pelo FIPS 140 enquanto opera em uma nuvem de hiperescala.

5.6. Respostas a *ciberataques*

Neste e em outros diversos tipos de sistema, ataques do tipo *ransomware* são comuns, onde códigos maliciosos bloqueiam o acesso a sistemas ou mesmo criptografam informações da vítima. Por isso, no sistema da Farmácia Ideal será constantemente atualizado para evitar esse tipo de invasão e o controle de *phishing* será constante também na ferramenta de e-mail utilizada. Todos os colaboradores serão instruídos da melhor maneira. E em uma área como essa, a saúde, um ataque como esses pode ter consequências gravíssimas. Torna-se preciso um sistema mais seguro e apto a alertar o utilizador caso ocorra algo suspeito, como por exemplo no recebimento de um e-mail.

Além disso, é importante um plano para manter a integridade dos dados através de backups regulares que podem ser automáticos ou manuais. Os manuais são ainda mais importantes, porque pode haver situações em que haja falha no sistema na inicialização de um backup. Por isso, é importante validar este backup que é feito com o uso da ferramenta da empresa Checkmarx. Caso um ataque desses ocorra e a informação seja perdida, a opção mais viável seria a de recuperação dos dados em backup.

Por isso, o sistema da Farmácia Ideal inclui backups regulares automáticos e manuais que geralmente são feitos ao fim do dia. Todos os seus funcionários passam por cursos que incentivam o tratamento e uso correto dos sistemas de gestão internos, tentando garantir a melhor segurança e evitando que o pior aconteça.

6. Bibliografia

6.1. Links

- https://www.kimaldi.com/pt-pt/blog-pt-pt/controlo_de_acessos_e_presenca/controlo_de_acessos/
- https://docs.microsoft.com/pt-br/windows/security/identity-protection/access-control/active-directory-security-groups
- https://docs.microsoft.com/pt-pt/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys
- https://ictq.com.br/varejo-farmaceutico/765-robos-em-portugal-amentam-a-empregabilidade-de-farmaceuticos-nas-farmacias
- https://www.ordemfarmaceuticos.pt/fotos/editor2/2019/WWW/noticias/ManualFarmaceutico_VF.pdf
- https://www.entrust.com/pt/digital-security/hsm/solutions/industry/retail/pharmacies
- https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo/
- https://csrc.nist.gov/Projects/Continuous-Monitoring
- https://www.siteware.com.br/projetos/como-criar-um-plano-de-acao/
- https://www.intertek.pt/servicos/certificacao-iso-27001/
- https://templum.pt/passo-a-passo-para-a-certificacao-de-um-sistema-de-gestao/
- https://support.microsoft.com/pt-pt/windows/criar-e-utilizar-palavras-passe-seguras-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
- https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn
- https://www.hbarcelos.min-saude.pt/wp-content/uploads/sites/11/2019/11/PoliticaSegurancaInformacao.pdf
- https://oiraproject.eu/pt/how-carry-out-risk-assessment