**UNIVERSIDADE DE SOROCABA- UNISO**

**ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

JOÃO VICTOR OLIVEIRA SOARES

LUCAS GABRIEL DE PROENÇA SUZUKI

WESLEY DE PONTES BATISTA MARIANO

WESLEY DOS SANTOS RODRIGUES

**POLÍTICAS DE SEGURANÇA LÓGICA**

**NO SISTEMA SERMAIS**

Sorocaba

2023

JOÃO VICTOR OLIVEIRA SOARES

LUCAS GABRIEL DE PROENÇA SUZUKI

WESLEY DE PONTES BATISTA MARIANO

WESLEY DOS SANTOS RODRIGUES

**POLÍTICAS DE SEGURANÇA LÓGICA**

**NO SISTEMA SERMAIS**

Trabalho de Segurança de Sistemas apresentado à Universidade de Sorocaba - UNISO

Sorocaba

2023

JOÃO VICTOR OLIVEIRA SOARES

LUCAS GABRIEL DE PROENÇA SUZUKI

WESLEY DE PONTES BATISTA MARIANO

WESLEY DOS SANTOS RODRIGUES

**POLÍTICAS DE SEGURANÇA LÓGICA**

**NO SISTEMA SERMAIS**

Trabalho de Segurança de Sistemas apresentado à Universidade de Sorocaba - UNISO

Banca Examinadora:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome do Professor

**RESUMO**

Este trabalho acadêmico apresenta um estudo de caso sobre a implementação de políticas de segurança lógica no sistema SerMais, abordando diretamente os conceitos que complementam o que realmente é uma política de segurança lógica, citando processos que fazem parte dessa política e demosntrando a maneira de implementação no sistema SerMais. Por fim é demonstrado a importância em ter uma política de segurança lógica em um sistema e porque ele deve ser aplicado e seguido, também a criação de um plano de contingência em controle de acesso e gestão de identidade demonstrando os processos que a empresa SerMais deverá seguir internamento para caso ocorra algum problema dentro de controle de acesso e gestão de identidade.

**Palavras-chave:** segurança, lógica, gestão

**ABSTRACT**

This academic work presents a case study of how security logic policies were implemented in the SerMais system, addressing directly the concepts that supplement what is actually a security logic policy, citing processes that make up this policy, and demonstrating how it was implemented there. Finally, it is demonstrated the significance of having a logical security policy in a system and why it must be implemented and followed, as well as the development of a contingency plan for access control and identity management that demonstrates the internal procedures that SerMais must employ in the event that a problem arises with access control and identity management.

**Key-words:** security, logic, and management

**SUMÁRIO**

[1INTRODUÇÃO 6](#_Toc2028524851)

[1.1 JUSTIFICATIVA 7](#_Toc197517065)

[1.2 OBJETIVOS 7](#_Toc2079042057)

[2 FUNDAMENTAÇÃO BIBLIOGRÁFICA 7](#_Toc2110445)

[2.1 O NOSSO SISTEMA 8](#_Toc2044419195)

[2.2 A IMPORTÂNCIA DE UM SISTEMA SEGURO 8](#_Toc653133812)

[2.3 O QUE É INFORMAÇÃO 9](#_Toc1881266532)

[2.4 O QUE É SEGURANÇA 9](#_Toc1055773172)

[2.5 SEGURANÇA DA INFORMAÇÃO 10](#_Toc1897145606)

[2.6 SEGURANÇA LÓGICA 11](#_Toc2129020766)

[2.7 A IMPORTÂNCIA DA SEGURANÇA LÓGICA NA FERRAMENTA 12](#_Toc459048421)

[2.8 AUTENTICAÇÃO DE USUÁRIOS 13](#_Toc1736139464)

[2.9 GESTÃO DE IDENTIDADE 14](#_Toc334234209)

[2.10 CRIPTOGRAFIA 15](#_Toc1750031089)

[2.11 USO DE FIREWALLS 15](#_Toc619275344)

[2.12 MONITORAMENTO 15](#_Toc571580287)

[2.13 BACKUP 16](#_Toc531261595)

[2.14 PLANO DE CONTIGÊNCIA – PROGRAMAÇÃO 17](#_Toc351746835)

[2.15 CONCLUSÃO 18](#_Toc851787648)

[3 CONSIDERAÇÕES FINAIS 18](#_Toc457297895)

[4 REFERÊNCIAS 19](#_Toc62464776)

[APÊNDICE A 21](#_Toc800013011)

[5 PLANO DE CONTIGÊNCIA - CONTROLE DE ACESSO E GERENCIAMENTO DE IDENTIDADE 22](#_Toc1429480540)

[5.1 INTRODUÇÃO 22](#_Toc308128828)

[5.2 OBJETIVOS 22](#_Toc1056617239)

[5.3 ESTRUTURA DO PLANO 23](#_Toc1722909229)

[5.4 PROCEDIMENTOS E RESPONSABILIDADES 24](#_Toc1883025672)

[5.5 COMUNICAÇÃO EM CASOS DE INCIDENTES 25](#_Toc328653762)

[5.6 TESTES E REVISÕES PERIÓDICAS 27](#_Toc1821098954)

# 1 INTRODUÇÃO

Atualmente vemos que a política de segurança lógica vem sendo um marco importante dentro das organizações e empresas, com a importância dos dados e informações para as empresas e o número de ameaças cibernéticas e ransomware vem aumentando, é muito importante que essas organizações tenham procedimentos e práticas para garantir a integridade de suas informações.

As políticas de segurança lógica são um conjunto de diretrizes e práticas que buscam garantir a integridade, confidencialidade e disponibilidade das informações, essas políticas definem medidas técnicas de segurança que ajudam a organização a se proteger e se prevenir contra ameaças cibernéticas, e além disso inclui procedimentos de gestão de riscos e incidentes de segurança.

## JUSTIFICATIVA

Como as políticas de segurança lógicas é algo importante em uma organização, ainda mais em uma empresa que está começando agora, é válido afirmar que definir procedimentos e práticas que visam utilizar diretrizes para uma boa segurança lógica é importante para essa organização. Com ênfase nisso e na criação da SerMais, visamos aplicar essas políticas de segurança lógicas nesta empresa, a fim de se assegurar que ela iniciará seguindo esses procedimentos e práticas com o intuito de proteger essa organização contra futuras ameaças cibernéticas, e a segurança da integridade de seus dados.

## OBJETIVOS

Definir procedimentos que envolvam práticas de segurança da informação e de sistemas, a fim de manter esse sistema e informações seguras seguindo os procedimentos estabelecidos. Abordaremos todas essas práticas com base na empresa SerMais, visando abordar passo a passo a importância de cada procedimento e como ela será aplicada. E por fim, criar essa política de segurança lógica, demonstrando os procedimentos criados e a sua importância em uma organização.

# FUNDAMENTAÇÃO BIBLIOGRÁFICA

## O NOSSO SISTEMA

Nos dias atuais, um site ou um sistema web é uma marca muito importante para um pequeno, médio ou grande negócio. É essencial ter essa marca digital e expor a credibilidade do negócio na internet. A partir dessa importância, nos aprofundamos em uma outra camada onde buscamos achar a necessidade, a tal que vimos no mundo da psicologia, onde muitos profissionais que acabam de se formar e outros que já atuam na área seguem no ramo com uma consultoria própria ou parceira. E com isso observamos que muitos utilizam portfólios online e divulgações em redes sociais de seus serviços, mas criar esse portifólio na internet e também divulgações nas redes sociais demanda tempo e um investimento inicial, onde muitos acabam não tendo logo de início.

Foi vendo esse aspecto que criamos a SerMais, uma ferramenta web, com o foco em criação de portfólios para psicólogos, essa ferramenta permite que psicólogos possam criar uma conta na plataforma e gerenciar uma aba (página) com o seu portfólio, podendo ser divulgado nas redes sociais. A plataforma também contará com um sistema de agendamento de consultas, onde o profissional cadastrado poderá utilizar por meio de um agendamento online, um sistema de consultas para seus clientes ou novos clientes. A plataforma altamente acessível e com ótima usabilidade, permitirá qualquer pessoa, com o mínimo de conhecimento em criação de portfólios, possa configurar a sua página de maneira intuitiva e prática.

## A IMPORTÂNCIA DE UM SISTEMA SEGURO

A partir da necessidade em se criar esse sistema, vimos que a segurança e o controle da informação são altamente importantes para o desenvolvimento. E para que esse sistema tenha uma boa segurança será aplicado uma política de segurança lógica, onde a partir do escopo do projeto definir um conjunto de regras e ações a serem tomadas, para que os usuários não precisem se preocupar com a segurança da plataforma e de seus dados.

Mas antes de entrar diretamente na criação dessa política, precisamos entender alguns conceitos que modulará os processos a serem criados.

## O QUE É INFORMAÇÃO

Primeiramente precisamos entender o que é a informação e como ela vai ser utilizada na ferramenta.

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. (ABNT, 2005, p. x).

Dado o conceito de informação, podemos especificar alguns dos tipos de informações em que a plataforma deve se assegurar em mantê-las protegidas.

* Informações pessoais;
* Informações de segurança;

Com esses dois tipos de informações, deverá ser criado uma política de segurança lógica onde envolverá a segurança e o tratamento correto desses dados.

Mas afinal, o que é segurança? E porque ela deve ser levada a sério quando se trata das informações citadas acima.

## O QUE É SEGURANÇA

De forma geral, segurança pode ser definida como um conjunto de medidas e precauções tomadas para prevenir ou minimizar riscos, perigos ou danos a pessoas, bens ou informações. Assim, a segurança no meio digital convém a assegurar que dados pessoais, informações financeiras de uma organização ou de um usuário, por exemplo, possam ser protegidas para prevenção de riscos.

A segurança é um conjunto de medidas que visam proteger pessoas, bens e informações contra ameaças internas e externas. Essas ameaças podem incluir a violência, o crime, as catástrofes naturais, as fraudes, os ataques cibernéticos, entre outros eventos que podem comprometer a integridade, a confidencialidade e a disponibilidade dos recursos e das informações. (GOMES, L. A, 2018).

Porém, é importante destacar que a segurança não é uma garantia absoluta, pois sempre haverá novas ameaças e vulnerabilidades que surgem com o avanço da tecnologia e da criatividade dos cibercriminosos.

A segurança é um processo contínuo que requer um comprometimento constante com a atualização e a melhoria das medidas de segurança. (WHITMAN, M. E.; MATTORD, H. J., 2016)

Portanto, é fundamental que as empresas e indivíduos invistam em medidas de segurança para proteger seus recursos e informações, mitigar os riscos de ataques e minimizar os prejuízos em caso de incidentes de segurança. Isso exige uma abordagem integrada e estratégica para a segurança, envolvendo a conscientização dos usuários, o uso de tecnologias e ferramentas adequadas e a adoção de políticas de segurança claras e bem definidas.

## SEGURANÇA DA INFORMAÇÃO

No contexto da segurança da informação, as principais ameaças incluem a ação de hackers, crackers, vírus, malware, phishing, ransomware e outras técnicas utilizadas por cibercriminosos para acessar, manipular ou roubar informações. Para combater essas ameaças, são necessárias medidas de segurança que abrangem aspectos técnicos, organizacionais e humanos.

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade de negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. [...] A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. (ABNT, 2005, p. x).

Entre as principais técnicas de segurança da informação, podem-se citar a criptografia, o controle de acesso, a autenticação, o monitoramento de atividades, a gestão de riscos, a política de segurança, entre outras. Cada uma dessas técnicas tem um papel específico na proteção das informações e deve ser implementada de acordo com as necessidades e o perfil da organização.

## SEGURANÇA LÓGICA

A segurança lógica em um site ou sistema web pode ser visto como uma medida de segurança para proteger o sistema de informação contra ameaças virtuais, como por exemplo ataques cibernéticos, roubos de dados e invasão de sistemas.

A segurança lógica é um conjunto de ações que visam à proteção das informações em meio eletrônico, garantindo que elas estejam disponíveis somente para as pessoas autorizadas a acessá-las. (BARCELLOS, R. B, 2014).

Referente a citação acima o autor ainda destaca que as medidas de segurança lógica devem ser planejadas e implementadas de forma integrada, abrangendo não apenas aspectos técnicos, mas também organizacionais e humanos.

Entre as principais técnicas de segurança lógica, pode-se citar a criptografia, que consiste na transformação dos dados em códigos indecifráveis sem uma chave de descriptografia o controle de acesso, que determina quem pode acessar determinados recursos e em que nível de permissão; e a autenticação, que verifica se o usuário é realmente quem diz ser por meio de senhas, tokens ou biometria.

Além disso, é importante destacar que a segurança lógica não é um processo estático e deve ser constantemente atualizada e revisada para acompanhar as mudanças tecnológicas e as novas ameaças que surgem.

A segurança lógica não é apenas um problema técnico, mas um problema de gestão de riscos que requer uma abordagem abrangente e holística. (KIM, D.; SOLOMON, M. G, 2014).

Portanto, é fundamental que as empresas e organizações invistam em medidas de segurança lógica para proteger suas informações e evitar prejuízos financeiros, legais e reputacionais. Isso exige um planejamento cuidadoso, a adoção de tecnologias e ferramentas de segurança adequadas e a conscientização dos usuários sobre a importância da segurança da informação.

## A IMPORTÂNCIA DA SEGURANÇA LÓGICA NA FERRAMENTA

Com base nas informações que temos sobre o sistema de criação de portfólios para psicólogos, podemos definir alguns conceitos importantes sobre a segurança da informação e a criação de uma política lógica para esse sistema.

Partindo do princípio, a segurança lógica é extremamente importante para um site quando o assunto é proteção de dados contra ameaças virtuais. Com a crescente quantidade de informações que são armazenadas e compartilhadas pela internet, tornou-se cada vez mais necessário garantir a integridade, a confidencialidade e a disponibilidade dos dados, evitando o acesso não autorizado, o roubo de informações sensíveis e outras formas de violação da privacidade dos usuários.

Para isso, é preciso adotar medidas de segurança lógica que englobam desde a proteção do sistema operacional e dos aplicativos até a implementação de políticas de segurança que envolvem os usuários e os processos internos da empresa. Entre as principais técnicas de segurança lógica, podem-se citar a criptografia, o uso de firewalls, o monitoramento de tráfego, a autenticação de usuários, a gestão de identidade, entre outras.

Além disso, é fundamental estar sempre atualizado sobre as novas ameaças e vulnerabilidades que surgem no ambiente digital, buscando constantemente aprimorar as medidas de segurança e promovendo uma cultura de segurança entre todos os usuários do site.

A segurança lógica é um processo contínuo que envolve uma abordagem holística para a proteção dos dados e exige a colaboração de todos os envolvidos. (CHANG; LIN, 2015).

Dessa forma, ao adotar medidas de segurança lógica eficientes, é possível garantir a proteção dos dados e a confiança dos usuários em relação ao site, contribuindo para o sucesso da empresa e para a segurança do ambiente digital como um todo.

Os tópicos abaixo, abrangerão medidas de segurança lógicas, que engloba todo o sistema do SerMais.

## AUTENTICAÇÃO DE USUÁRIOS

É importante que uma plataforma web, onde um sistema percorre por trás, tenha algumas regras para validação e autenticação dos usuários e seus acessos ao site, ou determinado recurso.

O impedimento de uso não autorizado de um recurso (ou seja, esse serviço controla quem pode ter acesso a um recurso, sob que condições o acesso pode ocorrer e o que é permitido para aqueles que acessam o recurso). (STALLINGSS, WILLIAM, p. 9).

O sistema web da SerMais terá alguns níveis de acesso, então essa hierarquia e controle de acesso a páginas específicas partirá de um login.

Terão 3 níveis de usuários, são eles:

* **Administrador:** Gerencia e valida os cadastros dos profissionais, e outras informações importantes do sistema.
* **Profissional (Psicólogo):** É o tipo de usuário que poderá se cadastrar no sistema, e criar seu portfólio. Podendo usufruir da ferramenta como o sistema de agendamento por exemplo.
* **Usuário comum (cliente):** É o usuário que poderá escolher um profissional e agendar uma consulta, esse usuário não terá muitas funções na plataforma, o intuito dele é acessar/ou criar sua conta de login, escolher um profissional e realizar um agendamento de uma consulta.

Esses 3 tipos de usuário não podem ter acessos as mesmas informações, um login específico para cada um é exigido para que possamos especificar seu nível de acesso e autenticidade.

## GESTÃO DE IDENTIDADE

Na gestão de identidade podemos ir um pouco além da autenticidade, dita no tópico anterior, onde aqui devemos impor os procedimentos que o software irá compor para o gerenciamento dessas informações de identidade e permissões de acesso, garantindo que apenas as pessoas certas tenham acesso as informações respectivas a seu nível hierárquico.

Gerenciamento de identidade significa gerenciar várias identidades parciais (geralmente denotadas por pseudônimos) de uma pessoa individual, ou seja, administração de atributos de identidade, incluindo o desenvolvimento e escolha da identidade parcial e do pseudônimo a serem (re)utilizados em um contexto ou função. (PFITZMANN; HANSEN, 2010, p.33).

No caso do sistema SerMais, não terá diversas identidades parciais, cada usuário terá um acesso único e seu acesso dependerá o seu nível de usuário na hierarquia.

Há vários processos que podemos seguir e aplicar dentro da gestão de identidade, o que abordaremos aqui, será:

* **Sistema de autenticação:** Os acessos desses usuários serão validados por meio de uma página de login, contendo credencias, como e-mail, senha e token de autenticação.
* **Sistema de autorização:** A partir em que o usuário acessa o site colocando seus dados de login, o software o redireciona para a página respectiva com seu nível de usuário, validado na página de login, de acordo com as informações que consta no banco referente a esse usuário e seu acesso.
* **Provisionamento:** Apenas usuários administradores possuem esse poder, a partir das políticas que a plataforma segue quaisquer dos usuários que não a respeitarem, poderão ter sua conta suspensa ou desativada da plataforma, não podendo ter mais acesso.
* **Administração de senhas:** É definido uma política de senhas, onde nessa política há padrões e formas que o usuário precisa adotar na criação de sua senha pessoal, envolvendo autenticação de dois fatores, complexidade da senha, recuperação da senha e alteração da senha.

## CRIPTOGRAFIA

No sistema SerMais, senhas de usuários precisarão ter uma criptografia. Para as senhas, assim que um usuário criar sua conta no site da SerMais, sua senha será armazenada na base de dados sendo criptografada, há vários padrões de criptografia, mas não entraremos muito nesse detalhe de qual será o escolhido, pois isso dependerá do nível de segurança e outros fatores do servidor.

A criptografia é importante, quando devemos dificultar o acesso a tal informação ou dado.

Algoritmos criptográficos basicamente objetivam “esconder” informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia. (TERADA, ROUTO, 2008, p. 18).

## USO DE FIREWALLS

É essencial citar a importância do firewall e seu papel no sistema SerMais, os fiewalls são uma barreira de defesa entre uma rede e a internet, contra invasões e ataques cibernéticos. Além disso o firewall te ajuda a monitorar e filtrar todo o tráfego de rede garantindo que apenas os tráfegos seguros (legítimos) passem.

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre uma rede e a Internet ou entre redes distintas. Seu objetivo é permitir somente a transmissão e a recepção de fluxos de dados autorizados. (LOPES, EDMO. 2008, p. 52).

Na SerMais a proteção das informações contra invasores e ataques cibernéticos é muito importante, pois a empresa tratará de dados pessoais de clientes, além de outras informações internas da empresa. Por isso é essencial se adequar e utilizar um bom firewall. Há diversos dispositivos de segurança no mercado que ajudam/ ou fazem o controle de firewall dando um leque de opções para a empresa escolher conforme sua necessidade.

## MONITORAMENTO

Há diversas práticas de monitoramento de firewall que podem ser utilizadas para garantira segurança da rede e das informações que nela trafegam, abaixo uma lista que o site SerMais adotará como práticas de monitoramento.

* **Registro de logs**: O firewall faz o registro de todas as informações sobre as tentativas de conexão que ocorrem na rede.
* **Alertas em tempo real**: O firewall pode ser configurado para enviar alertas em tempo real para os administradores do sistema sempre que uma atividade suspeita é detectada.
* **Análise de tráfego**: O firewall pode ser usado para analisar o tráfego de rede em tempo real.
* **Bloqueio de tráfego suspenso**: O firewall pode ser configurado para bloquear automaticamente o tráfego suspeito.
* **Monitoramento de aplicativos**: O firewall pode ser usado para monitorar o uso de aplicativos na rede.
* **Testes de penetração**: Os testes de penetração são usados para testar a segurança da rede e do firewall.

No mercado existe diversas ferramentas que fazem o monitoramento de firewall e da segurança da informação. A SerMais utilizará a ferramenta Firewall Analyzer.

Apresentamos o Firewall Analyzer, um software de gerenciamento de configuração e análise de log sem agente que ajuda os administradores de rede a entender como a largura de banda está sendo usada em sua rede. O Firewall Analyzer é independente do fornecedor e suporta quase todos os firewalls de rede comerciais e de código aberto, como Check Point, Cisco, Juniper, Fortinet, Palo Alto e muito mais. (FIREWALL ANALYZER, 2023).

A ferramenta suporta diversos tipos de firewalls que estão no mercado, assim o leque na escolha de qual firewall a SerMais irá utilizar fica mais fácil. Além disso o plano varia dependendo da quantidade de informações que a plataforma gerencia.

## BACKUP

Não é de hoje que a importância do armazenamento e o backup das informações são relevantes e importantíssimas para uma organização. Guardar os dados não é só importante, como é uma medida de segurança contra possíveis riscos e ameaças que podem ser causadas.

No âmbito da informática esta palavra ganhou significado particular sendo definida como cópia de segurança dos dados de determinado dispositivo de armazenamento que pode ser espelhado em outro dispositivo de forma a garantir a estabilidade dos arquivos e afastar a possibilidade de surpresas como a perda desses dados [...] muitos fabricantes de software oferecem uma solução de backup para cópia de sistemas completos, neste caso em geral são criados pontos de restauração para recuperar o sistema de possíveis interrupções. (CARDOSO, C.; TRINDADE, J.; LAROCA, M.; GOMES, M. 2012, p. 2).

Há alguns tipos de procedimentos de cópia de dados, o que parece ser mais essencial para a SerMais pelo sistema interagir diariamente com os seus usuários é o procedimento Incremental em conjunto com um backup completo.

O backup completo trata-se de copiar todos os arquivos para a sua mídia apropriada, onde é definida pela empresa. O problema de um backup completo, é que se nenhum dos arquivos mudam, o novo backup será igual ao anterior. Já o incremental, é inverso ao backup completo, pois ele verifica se o horário de um arquivo é mais recente do que o último backup feito, e caso o horário de modificação de um arquivo seja mais recente, o backup é realizado.

Então, para que possamos ter uma boa eficiência e facilidade na recuperação de algum dado, dados ou informação devemos utilizar esses dois procedimentos juntos – backup completo e backup incremental.

## PLANO DE CONTIGÊNCIA – PROGRAMAÇÃO

Entende-se de plano de contingência ser um documento que busca estabelecer e formalizar os procedimentos que uma equipe deve seguir caso haja alguma paralisação de sistema, ou outro problema qualquer que venha impactar diretamente no negócio da organização.

Na SerMais por ter uma ferramenta online onde seus clientes necessitam de acesso e disponibilidade do sistema por 24 por dias e 7 dias na semana, dá a se observar que caso a internet da empresa venha a oscilar ou a ficar fora do ar, independente do tempo, pode vir a trazer desconforto para os seus clientes pela indisponibilidade do sistema independente do tempo. Esse é um impacto enorme, pois envolve pessoas. Mas para garantir que isso não ocorra, é importante definir um documento buscando criar procedimentos que amenizem esses impactos caso um dia chegue a ocorrer.

Um plano de contingência pode ser considerado um conjunto de diretrizes e ações pré-determinadas que uma organização estabelece para lidar com situações de emergência/crises ou algum evento adverso que possa afetar o funcionamento normal da organização. E tem como objetivo permitir que a organização responda de forma eficaz e eficiente a essas situações, podendo minimizar os danos, protegendo os funcionários, clientes, ativos e garantindo que a continuidade das operações críticas. (PLANO DE CONTINGÊNCIA EM APÊNDICE A) no final do documento.

## CONCLUSÃO

Por meio deste trabalho, onde buscamos explorar e expor conceitos de políticas de segurança lógicas no projeto SerMais (uma ferramenta web, com o foco em criação de portfólios para psicólogos) e que também pudemos apresentar a importância da segurança das informações de uma empresa. Podemos concluir que de fato se importar em seguir procedimentos de uma política pode ajudar a empresa estar um passo à frente dos riscos que possam surgir. Não há como sumir com 100% dos riscos que uma empresa pode ter, mas pode ser minimizado o máximo, se as regras forem seguidas por todos.

Por fim, encorajamos os leitores a considerarem que independente do sistema que há de ser criados, ou até mesmo aqueles que já existem no mercado, necessitam de uma política de segurança lógica e que ela deve ser levada a sério, não esquecendo também em ter um plano de contingência, que busca solucionar algum risco caso ele venha a ser real na empresa.

# CONSIDERAÇÕES FINAIS

Ao longo da pesquisa, foi possível demonstrar que a importância da criação de uma política de segurança lógica em uma empresa oferece vantagens para a empresa, trazendo segurança e outros benefícios internos para a empresa.

Foi citado diversos conceitos, onde deu aos leitores a clareza de entender que a política de segurança criada em (APÊNDICE A) vem a ser muito importância, ela não é só um exemplo de como uma política lógica deve ser, mas sim um exemplo do que realmente devemos nos preocupar na criação de uma política e seus processos.

Também não esquecendo de toda a segurança que essa política trás, e que esses processos, envolvem um plano de contingência, também criado e exibido em (APÊNDICE A) no final deste documento. Que demonstrará o que fazer caso um risco ou problema venha acontecer na empresa, e como contorná-lo e resolvê-lo.

# REFERÊNCIAS

ABNT. NBR ISO/IEC 27002: **tecnologia da informação - técnicas de segurança - código de prática para a gestão de segurança da informação**. Rio de Janeiro: ABNT, 2013. Disponível em: https://profjefer.files.wordpress.com/2013/10/nbr\_iso\_27002-para-impressc3a3o.pdf. Acesso em: 10 mar. 2023.

BARCELLOS, R. B. **Segurança da Informação: Como garantir a confidencialidade, integridade e disponibilidade das informações em sua empresa.** São Paulo: Brasport, 2014.

Acesso em: 15 abr. 2023.

CARDOSO, C.; TRINDADE, J.; LAROCA, M.; GOMES, M. **BACKUP. RTA**

**Nº. 06 - X Semana de Extensão - XIV Jornada de Iniciação Científica - 2012**. Disponível em: http://revista.universo.edu.br/index.php?journal=1reta2&page=article&op=view&path%5B%5D=1155&path%5B%5D=862

Acesso em: 23 abr. 2023.

CHANG, V.; LIN, J. **Cyber-security technology and the protection of intellectual property.** In: INTERNATIONAL CONFERENCE ON ELECTRONIC BUSINESS (ICEB), 2015, Hong Kong. Proceedings... Hong Kong: ICEB, 2015. p. 1-6.

Acesso em: 15 abr. 2023.

FIREWALL ANALYZER. **Software de análise de logs e gerenciamento de configuração para dispositivos de segurança de rede.** 2023. Disponível em: https://www.manageengine.com/products/firewall/

Acesso em: 23 abr. 2023.

GOMES, L. A. **Segurança Pública: Conceitos, Sistemas e Gestão.** 3. ed. Rio de Janeiro: Forense, 2018.

Acesso em: 15 abr. 2023.

KIM, D.; SOLOMON, M. G. **Fundamentals of Information Systems Security.** 3. ed. Boston: Jones & Bartlett Learning, 2014.

Acesso em: 15 abr. 2023.

LOPES, EDMO. **ARQUITETURA DE ALTA DISPONIBILIDADE PARA FIREWALL E IPS BASEADA EM SCTP.** 2008. Disponível em: https://repositorio.ufu.br/bitstream/123456789/12466/1/Edmo.pdf

Acesso em: 23 abr. 2023.

PFITZMANN, A.; HANSEN, M. A. **terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.** August 2010. V0.34. Disponível em: http://dud.inf.tu-dresden.de/literatur/Anon\_Terminology\_v0.34.pdf.

Acesso em: 22 abr. 2023.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes: princípios e práticas.** São Paulo: Pearson Education do Brasil, 2014.

Acesso em: 10 mar. 2023.

TERADA, ROUTO. **Segurança de dados: criptografia em rede de computador**. 2008. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=lIe6DwAAQBAJ&oi=fnd&pg=PA15&dq=criptografia&ots=wIp\_SY9kMG&sig=1ck\_Wfr6flqVgloyGAJm6p4wILY&redir\_esc=y#v=onepage&q=criptografia&f=falseAcesso em: 23 abr. 2023.

WHITMAN, M. E.; MATTORD, H. J. **Management of Information Security**. 5. ed. Boston: Cengage Learning, 2016.

Acesso em: 15 abr. 2023.

# **APÊNDICE A**

# PLANO DE CONTIGÊNCIA - CONTROLE DE ACESSO E GERENCIAMENTO DE IDENTIDADE

Na gestão de identidade devemos impor os procedimentos que o software irá compor para o gerenciamento dessas informações de identidade e permissões de acesso, garantindo que apenas as pessoas certas tenham acesso as informações respectivas a seu nível hierárquico.

## INTRODUÇÃO

Este documento apresenta conceitos e ações para o plano de contingência a empresa SerMais.

Partindo do princípio, a segurança lógica é extremamente importante para um site quando o assunto é proteção de dados contra ameaças virtuais. Com a crescente quantidade de informações que são armazenadas e compartilhadas pela internet, tornou-se cada vez mais necessário garantir a integridade, a confidencialidade e a disponibilidade dos dados, evitando o acesso não autorizado, o roubo de informações sensíveis e outras formas de violação da privacidade dos usuários.

Além disso, é fundamental estar sempre atualizado sobre as novas ameaças e vulnerabilidades que surgem no ambiente digital, buscando constantemente aprimorar as medidas de segurança e promovendo uma cultura de segurança entre todos os usuários do site.

## OBJETIVOS

Garantir que o controle de acesso e o gerenciamento de identidade no sistema da SerMais seja totalmente seguro, seguindo procedimentos quem impõe importância na segurança das informações. Esses processos definidos em tópicos abordarão um passo a passo que destinará em um plano final caso venha ocorrer algum problema com o controle de acesso e o gerenciamento de identidade.

Isso garantirá que o acesso adequado a recursos, a prevenção de acessos não autorizados e a minimização dos ricos de violação de segurança sejam abordados e definidos.

Esse plano envolve os processos internos da empresa, sem vínculo com o cliente final, esses processos são com os funcionários da empresa SerMais.

## ESTRUTURA DO PLANO

* **Sistema de autenticação**: Define que os acessos desses usuários serão validados por meio de uma página de login, contendo credencias, como e-mail e senha criptografada.
* **Sistema de autorização**: No momento que o usuário acessa o site colocando seus dados de login, o software o redireciona para a página respectiva com seu nível de usuário, validado na página de login, de acordo com as informações que consta no banco referente a esse usuário e seu acesso.
* **Administração de senhas**: É definido uma política de senhas, onde nessa política há padrões e formas que o usuário precisa adotar na criação de sua senha pessoal, envolvendo autenticação de dois fatores, complexidade da senha, recuperação da senha e alteração da senha.
* **Provisionamento de contas**: Estabelece procedimentos para criação, remoção e exclusão de contas de usuários, e dar a garantia que a criação ou exclusão de constas sejam realizadas de maneira adequada e de acordo com outras políticas estabelecidas;
* **Gerenciamento de privilégios**: Consta em ter a implementação de política de privilégio mínimo, onde os usuários têm acesso apenas as informações e recursos necessários para realizar suas atividades. ￼
* **Auditoria e monitoramento**: Realizar a implementação de ferramentas e práticas de auditoria, para monitorar e registrar as atividades dos usuários, realizando a identificação de possíveis violações de políticas lógicas, e também a análise de logs para identificar comportamentos suspeitos e tomar medidas corretivas quando necessário.
* **Educação e conscientização**: Realização de treinamentos e programas de conscientização para usuários sobre a importância das políticas de controle de acesso e gerenciamento de identidade, e também incentivar o usuário a reportarem atividades suspeitas.

## PROCEDIMENTOS E RESPONSABILIDADES

**Sistema de autenticação:**

* Os usuários devem criar uma conta fornecendo informações precisas, como nome, e-mail e dados de contato.
* Para garantir a segurança das informações, o sistema irá verificar as credenciais do usuário por meio de uma página de login segura, protegendo-as com criptografia.
* Orientações serão fornecidas aos usuários para criar senhas fortes, seguindo as diretrizes estabelecidas na política de senhas.
* A equipe de TI será responsável por monitorar e auditar regularmente o sistema de autenticação, visando identificar possíveis vulnerabilidades ou tentativas de acesso não autorizado.

**Sistema de autorização:**

* Após o login bem-sucedido, o sistema irá redirecionar o usuário para as páginas ou recursos adequados ao seu nível de acesso.
* A equipe de desenvolvimento será responsável por implementar as regras de autorização no sistema, garantindo que cada usuário tenha acesso apenas às informações e recursos permitidos.
* A equipe de segurança irá monitorar as permissões de acesso e revisar regularmente os privilégios dos usuários para evitar concessões excessivas.

**Administração de senhas:**

* Os usuários devem seguir as diretrizes estabelecidas na política de senhas, que incluem requisitos de complexidade, uso de autenticação em dois fatores e práticas de recuperação e alteração de senhas.
* A equipe de suporte ao usuário será responsável por orientar os usuários sobre a criação e o gerenciamento adequados de senhas.
* Serão realizadas auditorias periódicas nas senhas dos usuários pela equipe de segurança, visando identificar senhas fracas ou violações das políticas estabelecidas.

**Provisionamento de contas:**

* A equipe de Recursos Humanos fornecerá informações precisas e atualizadas sobre os funcionários contratados, transferidos ou desligados, garantindo a criação, remoção ou exclusão adequada das contas de usuário.
* A equipe de TI será responsável por implementar os procedimentos de provisionamento de contas de acordo com as políticas estabelecidas, assegurando que as contas sejam criadas e removidas de forma oportuna e precisa.
* A equipe de auditoria realizará verificações regulares para garantir que todas as contas de usuário estejam devidamente provisionadas e em conformidade com as políticas da organização.

**Gerenciamento de privilégios:**

* A equipe de TI definirá os privilégios mínimos necessários para cada função ou cargo dentro da organização.
* Os administradores do sistema serão responsáveis por atribuir os privilégios adequados aos usuários, garantindo que tenham acesso somente às informações e recursos necessários para realizar suas atividades.
* A equipe de segurança realizará auditorias periódicas nos privilégios dos usuários, identificando e corrigindo possíveis violações de privacidade ou acesso indevido.

## COMUNICAÇÃO EM CASOS DE INCIDENTES

**Notificação interna**: Quando um problema de segurança é detectado, a equipe responsável pela segurança ou pelo gerenciamento de incidentes deve ser informada imediatamente. Isso pode ser feito através de um sistema de comunicação interno, como um sistema de tickets, e-mail ou ferramenta de chat.

*(Exemplo: Um membro da equipe de suporte técnico percebe uma atividade suspeita em um servidor e avisa imediatamente a equipe de segurança usando um sistema de tickets.)*

**Avaliação inicial e classificação do incidente**: Depois de receber o aviso, a equipe de segurança analisa a situação para entender a gravidade e o possível impacto do incidente. O incidente é classificado com base em uma escala pré-definida, como "baixo", "médio" ou "alto" usando uma matriz de risco.

*(Exemplo: A equipe de segurança avalia o incidente e o classifica como "médio", indicando que pode ter um impacto moderado nas operações da empresa.)*

**Notificação à alta administração**: Se o incidente for considerado significativo, a equipe de segurança deve informar a alta administração ou as pessoas chave na organização. Essa comunicação deve incluir informações sobre a natureza do incidente, o possível impacto e as medidas tomadas até o momento.

*(Exemplo: A equipe de segurança informa o diretor de TI e o diretor executivo sobre o incidente, fornecendo detalhes sobre as ações tomadas até o momento e os riscos potenciais associados.)*

**Comunicação externa, se necessário**: Em alguns casos, pode ser necessário comunicar o incidente a partes externas, como fornecedores, clientes ou autoridades reguladoras. Essa comunicação deve ser feita de acordo com as políticas e regulamentações aplicáveis, garantindo a proteção adequada das informações sensíveis.

*(Exemplo: A equipe de segurança identifica que o incidente pode ter afetado os dados dos clientes e, portanto, notifica a autoridade de proteção de dados, seguindo os procedimentos estabelecidos.)*

**Comunicação contínua e atualizações**: Durante o gerenciamento do incidente, é importante manter todas as partes relevantes informadas sobre o progresso, as medidas tomadas e os próximos passos. Isso pode ser feito através de atualizações regulares por e-mail, reuniões de acompanhamento ou qualquer outra forma de comunicação apropriada.

*(Exemplo: A equipe de segurança envia atualizações diárias por e-mail para a alta administração, fornecendo informações sobre o progresso da investigação, as medidas de mitigação implementadas e quaisquer novos desenvolvimentos relevantes.)*

## TESTES E REVISÕES PERIÓDICAS

Revisão constante das políticas de controle de acesso e gerenciamento de identidade para garantir a sua eficácia e conformidade com as mudanças nas necessidades e regulamentações de segurança.