Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

1. Sumário

2. INTRODUÇÃO 1
3. OBJETIVO 2
4. ABRANGÊNCIA 2
5. COMPOSIÇÃO 2
6. ACESSO AO DOCUMENTO 3
7. DEFINIÇÕES 3
8. DIRETRIZES 8
9. CONTROLE ORGANIZACIONAIS 8
10. CONTROLE DE PESSOAS 32
11. CONTROLES FÍSICOS 36
12. CONTROLES TECNOLÓGICOS 50
13. CONSCIENTIZAÇÃO 134
14. PLANO DE CONTINUIDADE DE NEGÓCIOS 135
15. MESA LIMPA E TELA LIMPA 135
16. RESPONSABILIDADES 136
17. SANÇÕES 138
18. AUDITORIA 138
19. DISPOSIÇÕES GERAIS 139
20. ATUALIZAÇÃO 140
21. DIVULGAÇÃO 140
22. VIGÊNCIA 140
23. HISTÓRICO DE ALTERAÇÕES 141
24. REFERÊNCIAS 141

2. INTRODUÇÃO

Elaboração	Análise crítica	Classificação da Informação	Aprovação
Brunno Eduardo Vilela Batista	Murilo Morais De Oliveira	Pública	Dra. Rosane Abramo Dr. Raphael Gonçalves de Oliveira
Data: 12/01/2026	Data: 16/01/2026		

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

Esta Política tem como finalidade estabelecer os conceitos e diretrizes de segurança da informação, visando a proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.

A Política de Segurança da Informação ("PSI") deve adotar critérios técnicos e administrativos aptos a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, ou qualquer forma de tratamento inadequado, conforme previsão do art. 46 da Lei nº 13.709/2018 (LGPD).

3. OBJETIVO

Esta PSI é um documento estratégico, que estabelece os conceitos e diretrizes para promover a utilização segura dos ativos de informação de todos os colaboradores da Unimed Ituiutaba – que deve implementar soluções de natureza multidisciplinar, com observância do descrito na ISO 27001, preservando a confidencialidade, a integridade e a disponibilidade das informações para resolução de incidentes e deliberação de procedimentos a serem adotados para a tomada de decisão.

4. ABRANGÊNCIA

Esta política se aplica a todos os Diretores, Gestores, Clientes, Parceiros, Colaboradores e demais partes interessadas que se relacionem com a Unimed Ituiutaba, em todas suas áreas de atendimento.

5. COMPOSIÇÃO

Elaboração	Análise crítica	Classificação da Informação	Aprovação
Brunno Eduardo Vilela Batista	Murilo Morais De Oliveira	Pública	Dra. Rosane Abramo Dr. Raphael Gonçalves de Oliveira
Data: 12/01/2026	Data: 16/01/2026		

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

A estrutura da PSI é composta por um conjunto de documentos hierarquicamente descritos a seguir, na ordem de importância e de prevalência:

Política de Segurança da Informação: constituída por este documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação. A aprovação deste documento é dada pela Diretoria, e a sua revisão deverá ser anual e, quando necessário;

Procedimentos de Segurança da Informação: visam a instrumentalizar o disposto na PSI. Cabe aos gestores das Tecnologia utilizadas elaborarem e implementarem os procedimentos de segurança adotados, devendo este documento ser revisto anualmente.

6. ACESSO AO DOCUMENTO

A presente Política e demais documentos a ela associados estarão disponíveis no site da Unimed Ituiutaba para os colaboradores, e para os parceiros, clientes e demais partes interessadas estará disponível, no link: https://www.unimed.coop.br/site/web/ituiutaba/politica-de-privacidade .

7. DEFINIÇÕES

7.1. Ativos/Recursos:

Além da própria informação, o ativo está incluído em qualquer elemento, seja ele humano, tecnológico, software, com valor financeiro e de repercussão direta para o funcionamento no dia a dia da Unimed Ituiutaba.

7.2. Auditoria em Segurança da Informação:

Processo de avaliação da situação atual dos controles de segurança da informação implementados.

7.3. Autenticidade:

Consiste na certeza absoluta da veracidade e originalidade de algo. A autenticidade é necessária por uma **questão de segurança**, para garantir que informações, por exemplo, sejam transmitidas para pessoas ou entidades que não devem ter acesso a estes dados. Já a **autenticidade de documentos** é usada para garantir que estes são legítimos. Por outro lado, também ajuda a diminuir a aplicação de fraudes e golpes contra terceiros.

7.4. BYOD (Bring Your Own Device):

Conceito de infraestrutura em TI que consiste na utilização dos aparelhos dos próprios funcionários para desempenhar as atividades empresariais.

7.5. CGPSI (Comitê Gestor de Privacidade de Dados e Segurança da Informação):

É uma instância organizacional responsável por supervisionar, implementar e monitorar políticas, diretrizes e estratégias relacionadas à privacidade de dados e à segurança da informação. Ele atua como um órgão consultivo e deliberativo, alinhado às normas legais, regulamentações e boas práticas de mercado, como a LGPD (Lei Geral de Proteção de Dados).

7.6. Confidencialidade:

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

Princípio de segurança da informação pelo qual se garante que o acesso à informação seja obtido somente por pessoas autorizadas.

7.7. Criticidade:

Grau de importância da informação para a continuidade dos negócios e processos da Unimed Ituiutaba.

7.8. Dado Pessoal:

Qualquer dado que possa permitir identificar uma pessoa.

7.9. Disponibilidade:

Princípio de segurança da informação pelo qual se estabelece que os ativos/recursos estarão disponíveis sempre que necessário.

7.10. Disponibilidade:

Princípio de segurança da informação pelo qual se estabelece que os ativos/recursos estarão disponíveis sempre que necessário.

7.11. Incidente de Segurança da Informação:

Um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação (PSI).

7.12. Informação:

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

A informação é um ativo/recurso tão importante quanto qualquer outro, podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos mostrada em filmes ou falada em conversas.

7.13. Integridade:

Princípio de segurança da informação por meio do qual é garantido que a informação não será alterada sem a devida autorização.

7.14. Gestão de Mudanças (GMUD):

A GMUD é o processo de solicitação, determinação da viabilidade, planejamento, implementação e avaliação de mudanças em um sistema. Tem dois objetivos principais: dar suporte ao processo de mudança organizacional e permitir um acompanhamento das alterações. As operações empresariais e os ecossistemas de TI estão se tornando mais complexos, com mais dependências e mudanças frequentes.

7.15. Usuário:

Quaisquer pessoas que utilizem de forma autorizada ativos/recursos da Unimed Ituiutaba.

7.16. LGPD:

Lei Geral de Proteção de Dados Pessoais - Lei n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

7.17. Norma:

Elaboração	Análise crítica	Classificação da Informação	Aprovação
Brunno Eduardo Vilela Batista	Murilo Morais De Oliveira	Pública	Dra. Rosane Abramo Dr. Raphael Gonçalves de Oliveira
Data: 12/01/2026	Data: 16/01/2026		

Documento que contém regras a serem seguidas.

7.18. Online:

(Estar disponível ao vivo): no contexto da Internet significa estar disponível para acesso imediato, em tempo real.

7.19. Procedimento Operacional Padrão (POP):

Documento que formaliza a descrição das atividades envolvidas no fluxo do processo de trabalho da Unimed Ituiutaba, relacionando-os com os responsáveis, os recursos utilizados e a identificação dos dados de "quem", "o quê" e "quando" são realizadas em cada etapa das operações.

7.20. Recursos Tecnológicos:

Todo e qualquer recurso que possibilita o acesso, processamento, armazenamento e/ou transmissão de informações; como sistemas de informação, servidores físicos ou em Nuvem, estações de trabalho, computadores portáteis (notebooks), impressoras, dispositivos portáteis como Tablets, celulares e IOT's, link de internet, Wi-Fi, servidores de rede e equipamentos de conectividade.

7.21. Risco:

Combinação da probabilidade de ocorrência de um evento e de suas consequências.

7.22. SI:

Segurança da Informação.

7.23. TIC:

Tecnologia da Informação e Comunicação.

7.24. TI:

Tecnologia da Informação.

8. DIRETRIZES

A Unimed Ituiutaba é comprometida com a observância dos regulamentos em vigor aplicáveis, bem como com o seu Código de Conduta e Ética. Para a condução de suas atividades administrativas, sociais, treinamentos, é necessário o estabelecimento de uma Política de Segurança da Informação estruturada e clara, que possibilite aderência e conformidade a partir da implementação de uma série de controles, que podem ser: tecnológicos, físicos ou administrativos.

9. CONTROLE ORGANIZACIONAIS

9.1. Papéis e responsabilidades pela Segurança da Informação:

Os papéis e responsabilidades pela segurança da informação serão definidos e atribuídos de forma clara, garantindo que todos os colaboradores compreendam suas atribuições. A Unimed Ituiutaba estabelecerá os seguintes papéis principais:

Responsável pela Segurança da Informação (RSI): Supervisionar a implementação das políticas de segurança da informação e garantir o cumprimento das normas estabelecidas.

- **Equipe de TI:** Implementar e manter soluções tecnológicas alinhadas às diretrizes de segurança.
- **Colaboradores:** Cumprir as políticas e procedimentos relacionados à segurança da informação.
- **Auditores Internos:** Monitorar e avaliar a conformidade das práticas de segurança.

9.2. Segregação de funções:

A Unimed Ituiutaba implementará a segregação de funções para minimizar o risco de acessos indevidos ou erros. As funções conflitantes serão identificadas e documentadas. Exemplos de medidas incluem:

- Separar funções de desenvolvimento, operações e controle.
- Restringir acessos administrativos apenas a funções críticas e devidamente autorizadas.
- Implementar revisões regulares para evitar a acumulação de responsabilidades conflitantes.

9.3. Responsabilidades da direção:

A direção é responsável por:

- Garantir que todos os colaboradores apliquem a segurança da informação em conformidade com as políticas e procedimentos organizacionais.
- Promover treinamentos e campanhas de conscientização periódicas.
- Monitorar e avaliar continuamente os riscos e controles associados à segurança da informação.

9.4. Contato com autoridade:

A Unimed Ituiutaba estabelecerá canais formais de comunicação com autoridades relevantes, incluindo:

- Agências reguladoras do setor.
- Forças de segurança, em caso de incidentes de segurança cibernética ou quebras de conformidade.
- Escritórios jurídicos especializados em proteção de dados e privacidade.

9.5. Contato com grupos de interesse especial:

Para manter-se atualizada e alinhada com boas práticas, a Unimed Ituiutaba participará de:

- Associações profissionais de segurança da informação.
- Grupos de inteligência de ameaças.
- Fóruns de discussão sobre cibersegurança.

9.6. Inteligência de ameaças:

As informações relacionadas às ameaças à segurança da informação serão coletadas, analisadas e transformadas em ações preventivas. Exemplos incluem:

- Monitoramento de fontes de ameaças.
- Atualização contínua de antivírus e firewall.
- Participação em grupos de compartilhamento de informações sobre ameaças cibernéticas.

Segurança da informação no gerenciamento de Projetos:

A segurança da informação será integrada ao gerenciamento de projetos desde a sua concepção até o encerramento. As diretrizes incluem:

- Realizar análises de riscos de segurança no início de cada projeto.
- Garantir que os requisitos de segurança estejam alinhados aos objetivos do projeto.
- Realizar revisões regulares para garantir a conformidade com as normas de segurança estabelecidas

9.7. Gestão de Ativos:

Os ativos associados com informação e com os recursos de processamento da informação são identificados por meio da plataforma HP Smart Device Services Manager Simpress, Workforce Experience Platform HP(Simpress) e planilha de ativos próprios, incluindo o inventário destes ativos.

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

Ativo é qualquer elemento que tenha valor para a Unimed Ituiutaba e que precise de proteção:

- **Hardware:** Servidores, computadores desktop, notebooks, celulares.
- **Informação:** arquivos em PDF, mídias eletrônicas, HD´s externos ,banco de dados.
- **Infraestrutura:** Internet dedicada redundante, eletricidade, geradores, ar-condicionado e ar-condicionado redundante.

Os colaboradores e partes externas que usam ou têm acesso aos ativos da Unimed Ituiutaba são conscientes dos requisitos de segurança da informação dos ativos da Unimed Ituiutaba, presentes nesta política.

Eles são responsáveis pelo uso de qualquer recurso de processamento da informação e tal uso é realizado sob sua responsabilidade.

a) comportamentos esperados e inaceitáveis dos colaboradores do ponto de vista de segurança da informação:

- Proibida a utilização da internet para uso pessoal;
- Proibida a utilização de redes sociais pessoais;

b) uso permitido e proibido de informações e outros ativos associados.

Proibida a utilização de informação de negócio para uso pessoal;

Proibida a transferências de informações de negócios por canais não homologados pela Unimed Ituiutaba;

c) atividades de monitoramento que estão são realizadas pela Unimed Ituiutaba:

software de monitoramento de acessos: acessos por VPN são monitorados por firewall, Google Workspace para monitoramento de usabilidade;

Todos os colaboradores e partes externas devem devolver todos os ativos da Unimed Ituiutaba que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

Realizando a entrega imediatamente ao departamento de tecnologia da informação. Com todos os acessórios.

9.8. Classificação e Tratamentos de Informações:

A informação recebe um nível adequado de proteção, de acordo com a sua importância para a Unimed Ituiutaba. A responsabilidade de classificação é do proprietário do ativo. Os níveis de classificação são:

- **Público:** quando sua divulgação não causa nenhum dano;
- **Uso Interno:** quando a divulgação causa constrangimento ou inconveniência operacional;
- **Confidencial:** quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da Unimed Ituiutaba em risco.

Informações devem ser identificadas com etiquetas claras (físicas ou digitais) indicando sua classificação.

Exemplos: "Confidencial", "Uso Interno", ou "Público" visivelmente marcados em documentos, sistemas ou e-mails.

Os procedimentos de operação são documentados e disponibilizados a todos os usuários que necessitem deles, por meio de file server.

9.9. Transferência de Informações:

A Unimed Ituiutaba possui as seguintes regras para realizar transferência de informações dentro da Unimed Ituiutaba e entre a Unimed Ituiutaba e outras partes:

- Quando possível a informação deve ser transferida utilizando recursos de criptografia;

Os serviços de transferências considerados confiáveis são:

- **Gerenciador de e-mail:** Google workspace;
- **Plataformas de comunicação:** Google workspace;
- **Plataforma de armazenamento e transferência:** Google workspace;
- **Mídia de transferência física:** Fibra, Hd's, fitas magnéticas;
- **Informação física:** Correios AR ;

Diretrizes de retenção e descarte para todos os registros de negócios.

Acordos de transferências específicos com partes externas: registrados via contrato ou informação documentada equivalente;

Seguir quaisquer requisitos legais, estatutários, regulamentares e contratuais relevantes nas transferências de informações.

9.10. Controle e Direitos de Acessos:

A Unimed Ituiutaba utiliza a plataforma Google Workspace para controlar informações (e-mail, documentos, entre outros), a plataforma Smart Device Services Manager Simpress, Workforce Experience Platform HP(Simpress) e planilha de ativos para registrar os ativos físicos.

Estas adotam as seguintes regras de acesso físico e lógico às informações e a outros ativos associados:

- A determinação de quais entidades possuem acesso às informações e outros ativos está registrada nas plataformas citadas.
- A Unimed Ituiutaba deve considerar requisitos de negócios, risco da informação, legislação pertinente e conflitos de interesses para controlar seu acesso.
- As plataformas citadas devem ser atualizadas quando houver a inserção ou retirada de uma entidade na Unimed Ituiutaba.

- O conteúdo das plataformas citadas deve ser revisado com periodicidade mínima anualmente com a finalidade de revisar os acessos a quais as entidades possuem direitos e ajustando conforme necessidade.
- O processo de provisionamento e revogação de direito de acesso é realizado por meio de abertura de ticket.

9.11. Gestão de Identidade:

A gestão do ciclo de vida das identidades deve ser realizada de forma estruturada e consistente, abrangendo as seguintes etapas principais:

- **Criação e registro de identidades:**
  - Definir processos para a criação de identidades digitais, garantindo que apenas usuários autorizados possam acessar sistemas e recursos.
  - Coletar as informações necessárias para identificar o usuário de forma única.
- **Gerenciamento de acessos:**
  - Assegurar que os acessos sejam concedidos de acordo com o princípio de privilégio mínimo, baseado em papéis e responsabilidades definidos para cada identidade.
  - Implementar controles para revisão periódica de acessos, garantindo que as permissões permaneçam alinhadas às necessidades do usuário e às políticas organizacionais.

- **Manutenção e atualização:**
  - Revisar regularmente as identidades e atualizar informações conforme mudanças de função, transferências ou outras alterações organizacionais.

- **Revogação e exclusão:**
  - Garantir a desativação ou exclusão imediata das identidades em caso de desligamento ou término do relacionamento com a Unimed Ituiutaba.
  - Manter registros auditáveis sobre os processos de revogação e exclusão.

9.12. Informações de autenticação:

A alocação e a gestão de informações de autenticação devem ser conduzidas com base em boas práticas de segurança, incluindo:

- **Geração de informações de autenticação:**
  - Implementar requisitos para senhas fortes e outros fatores de autenticação (ex.: biometria, tokens de segurança).
  - Utilizar geradores automáticos para criação de credenciais, minimizando erros humanos.
- **Distribuição segura:**
  - Garantir que credenciais sejam entregues ao usuário de forma segura e confidencial.
  - Evitar o compartilhamento de informações de autenticação por canais inseguros.
- **Manuseio e armazenamento:**
  - Educar os funcionários sobre as melhores práticas para proteger informações de autenticação, como não anotar senhas em locais acessíveis.
  - Utilizar criptografia para armazenar credenciais em sistemas organizacionais.
- **Revisão e renovação:**
  - Exigir mudanças periódicas de senhas e o uso de novos fatores de autenticação, quando aplicável.
- **Revogação e resposta a incidentes:**
  - Desenvolver processos para desativação imediata de credenciais comprometidas.

- Estabelecer um plano de resposta para violações relacionadas à autenticação.

9.13. Segurança da Informação nas relações com fornecedores:

Para garantir a segurança da informação nas relações com fornecedores, a Unimed Ituiutaba deve implementar os seguintes processos e procedimentos:

- **Avaliação inicial:**
  - Realizar análise de riscos antes de estabelecer relação com fornecedores, avaliando a segurança de seus produtos e serviços.
  - Verificar a aderência dos fornecedores às políticas de segurança da Unimed Ituiutaba.
- **Gestão contratual:**
  - Incluir cláusulas contratuais claras sobre segurança da informação e conformidade regulatória.
  - Garantir que os fornecedores se comprometam a proteger informações confidenciais.
- **Monitoramento e auditoria:**
  - Realizar monitoramentos periódicos e auditorias nos fornecedores para verificar o cumprimento dos requisitos de segurança.
  - Solicitar relatórios de conformidade e testes de vulnerabilidade realizados pelos fornecedores.
- **Plano de contingência:**
  - Estabelecer planos de continuidade e contingência para mitigar riscos associados a falhas ou incidentes com fornecedores.

9.14. Abordagem da Segurança da Informação nos contratos de fornecedores:

Os requisitos de segurança da informação nos contratos de fornecedores devem ser detalhados e adaptados ao tipo de relação estabelecida. Estes requisitos incluem:

- **Definição de responsabilidades:**

- Estabelecer responsabilidades claras para o fornecedor no que tange à proteção de dados e sistemas da Unimed Ituiutaba.

- **Proteção de dados:**
  - Incluir cláusulas que definam como os dados serão armazenados, processados e protegidos.
  - Exigir que os dados sejam tratados em conformidade com as leis aplicáveis, como a LGPD (Lei Geral de Proteção de Dados).
- **Requisitos de conformidade:**
  - Garantir que os fornecedores sigam padrões de mercado, como ISO 27001 ou outros certificados relevantes.
- **Notificação de incidentes:**
  - Determinar prazos e procedimentos para notificação de incidentes de segurança por parte do fornecedor.
- **Auditoria e revisão:**
  - Permitir que a Unimed Ituiutaba realize auditorias regulares para verificar a conformidade com os requisitos de segurança.
- **Término de contrato:**
  - Especificar procedimentos para a devolução ou eliminação segura de dados ao final do contrato.

9.15. Gestão da segurança da informação na cadeia de fornecimento de TIC:

Os processos e procedimentos para gerenciar os riscos da segurança da informação associados à cadeia de fornecimento de produtos e serviços de TIC devem incluir:

- **Identificação de Riscos:** Mapear os riscos de segurança associados a cada fornecedor ou serviço na cadeia de fornecimento, considerando o impacto potencial na Unimed Ituiutaba.

- **Seleção de Fornecedores:** Avaliar os fornecedores quanto à conformidade com os requisitos de segurança da informação da Unimed Ituiutaba antes da contratação, utilizando critérios claros e padrões de conformidade (como ISO/IEC 27001 ou equivalentes).
- **Acordos Contratuais:** Incluir cláusulas específicas relacionadas à segurança da informação nos contratos, como obrigações de confidencialidade, políticas de acesso a dados, e notificações de incidentes.
- **Monitoramento Contínuo:** Estabelecer mecanismos regulares para avaliar o desempenho dos fornecedores quanto às práticas de segurança, por meio de auditorias, revisões e relatórios de conformidade.
- **Planos de Resposta:** Definir planos de resposta a incidentes relacionados a falhas de segurança na cadeia de fornecimento, incluindo comunicação, mitigação de impacto e resolução.

9.16. Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores:

A Unimed Ituiutaba deve implementar processos para monitorar, avaliar e gerenciar mudanças nos serviços de fornecedores e práticas de segurança da seguinte forma:

- **Monitoramento Contínuo:** Estabelecer métricas e indicadores de desempenho para acompanhar os serviços prestados pelos fornecedores em tempo real ou em intervalos regulares.
- **Auditorias Periódicas:** Realizar auditorias regulares nos fornecedores para garantir que práticas de segurança continuem alinhadas às exigências contratuais e regulamentares.
- **Gestão de Mudanças:** Criar um processo estruturado para avaliar os impactos de alterações nos serviços ou práticas de segurança do fornecedor, como mudanças em infraestrutura, políticas ou equipe.

- **Revisões Regulares:** Realizar análises críticas e revisões formais da prestação de serviços, documentando quaisquer desvios ou lacunas identificadas, bem como ações corretivas necessárias.
- **Comunicação Eficaz:** Manter uma comunicação ativa e transparente com os fornecedores, assegurando que mudanças relevantes sejam notificadas e aprovadas antes de sua implementação.

9.17. Segurança da informação para uso de serviços em nuvem:

Os processos para aquisição, uso, gestão e saída de serviços em nuvem devem ser definidos considerando os seguintes pontos:

- **Avaliação de Fornecedores de Nuvem:** Garantir que os provedores de serviços em nuvem atendam aos requisitos de segurança da informação da Unimed Ituiutaba, com certificações reconhecidas (como ISO 27017, SOC 2) e políticas robustas de proteção de dados.
- **Contrato de Serviço:** Formalizar acordos claros de nível de serviço (SLAs) com cláusulas específicas relacionadas à segurança da informação, como localização de dados, backups, gerenciamento de incidentes e término do contrato.
- **Gestão de Acessos:** Implementar controles rigorosos de autenticação e autorização para usuários e sistemas que acessam os serviços em nuvem, incluindo práticas como autenticação multifator.
- **Monitoramento e Auditoria:** Utilizar ferramentas de monitoramento para acompanhar a utilização de recursos em nuvem e identificar possíveis vulnerabilidades ou incidentes de segurança.
- **Plano de Continuidade e Recuperação:** Garantir que haja um plano robusto para continuidade de negócios e recuperação de dados em caso de falhas, bem como a capacidade de migração segura para outro fornecedor em caso de término do contrato.

- **Saída de Serviços:** Definir um processo claro para a saída de serviços em nuvem, incluindo a exclusão segura de dados, transferência de informações e encerramento de acessos, garantindo a integridade e a confidencialidade das informações da Unimed Ituiutaba.

9.18. Gestão de Incidentes de Segurança da Informação:

Os colaboradores e partes externas que usam os sistemas e serviços de informação da Unimed Ituiutaba, devem registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços por meio de e-mail, telefone, ticket ou e-mail anonimizado. A notificação é recebida pela equipe de Segurança da Informação e posteriormente segue para avaliação.

Os eventos de segurança da informação são avaliados e é decidido se eles são classificados como incidentes de segurança da informação. Se classificado como incidente é realizado um processo estruturado que visa identificar, responder, mitigar e documentar incidentes relacionados à segurança. Ele pode ser descrito em etapas principais, conforme abaixo:

9.18.1. Detecção e Registro

- Identificar o incidente por meio de sistemas de monitoramento, alertas ou denúncias.
- Registrar o evento em um sistema de gerenciamento de incidentes, documentando:
  - Data e hora do ocorrido.
  - Fonte de detecção.
  - Descrição inicial do incidente.

9.18.2. Análise e Classificação

- Analisar a natureza do incidente para determinar:

- O escopo (quais sistemas, dados ou usuários foram afetados).
- A criticidade (impacto potencial no negócio, confidencialidade, integridade e disponibilidade).
- A causa provável (ataques externos, erros internos, falhas técnicas, etc.).

- Classificar o incidente conforme a gravidade e urgência, definindo prioridades de tratamento.

9.18.3. Contenção

- Contenção Imediata:
  - Medidas para evitar a propagação ou agravamento do impacto (ex.: desconectar sistemas comprometidos da rede, bloquear acessos não autorizados).
- Contenção de Longo Prazo:
  - Implementar ações mais completas para estabilizar o ambiente, como aplicar correções ou atualizar sistemas.

9.18.4. Erradicação

- Identificar e remover a causa raiz do incidente (ex.: remoção de malware, correção de vulnerabilidades, atualização de patches).
- Verificar se o ambiente está seguro antes de retomar as operações.

9.18.5. Recuperação

- Restaurar sistemas e dados ao estado normal, garantindo que estejam livres de vulnerabilidades.
- Monitorar o ambiente após a recuperação para verificar se o incidente foi completamente resolvido.

9.18.6. Documentação e Comunicação

- Documentar todas as etapas do tratamento, incluindo:
  - Ações realizadas.
  - Decisões tomadas.
  - Resultados obtidos.
- Comunicar as partes interessadas, conforme apropriado:
  - Equipes internas.
  - Clientes ou fornecedores impactados.
  - Autoridades regulatórias, se exigido.

9.18.7. Aprendizado e Melhoria Contínua

- Realizar uma análise pós-incidente (Post-Mortem) para identificar lições aprendidas:
  - O que funcionou bem.
  - O que poderia ser melhorado.
- Atualizar políticas, processos, ferramentas e treinamentos com base no incidente ocorrido.

Esse processo, quando bem definido e executado, ajuda a minimizar impactos e previne a recorrência de incidentes similares.

Os incidentes de segurança da informação são reportados para pessoas relevantes da Unimed Ituiutaba, ou ainda, partes externas.

Convém que a notificação, quando possível, inclua os seguintes itens:

- Contenção, se as consequências do incidente podem se espalhar, dos sistemas afetados pelo incidente;

- Coleta de evidências o mais rápido possível após a ocorrência;
- Escalonamento, conforme necessário, incluindo atividades de gestão de crises e possivelmente invocação de planos de continuidade de negócios;
- Garantia de que todas as atividades de resposta envolvidas sejam devidamente registradas para análise posterior;
- Comunicação da existência do incidente de segurança da informação ou quaisquer detalhes relevantes deles a todas as partes interessadas internas e externas relevantes seguindo o princípio da necessidade de conhecer;
- Coordenação com partes internas e externas, como autoridades, grupos de interesse externo e fóruns, fornecedores e clientes para melhorar a eficácia da resposta e ajudar a minimizar as consequências para outras organizações;
- Uma vez que o incidente foi tratado com sucesso, formalmente fechá-lo e registrá-lo;
- Análise forense de segurança da informação, conforme necessário;
- Análise pós-incidente para identificar a causa-raiz. Assegurar que seja documentada e comunicada de acordo com os procedimentos definidos;
- Identificação e gestão de vulnerabilidades e fragilidades de segurança da informação, incluindo aquelas relacionadas com os controles que causaram, contribuíram ou falharam em prevenir o incidente.

A Unimed Ituiutaba utilizará o conhecimento adquirido com incidentes de segurança da informação para fortalecer e melhorar os controles, identificando incidentes recorrentes ou graves e suas causas para atualizar o processo de avaliação de risco de segurança da informação e determinar e implementar controles adicionais necessários para reduzir a probabilidade ou as consequências de futuros incidentes semelhantes.

A coleta de evidências deve considerar:

- A cadeia de custódia;

- A segurança da evidência;
- A segurança das pessoas;
- Papéis e responsabilidades das pessoas envolvidas;
- Competência do pessoal;
- Documentação;
- Resumo do incidente.
- Os registros estão completos e não foram adulterados de forma alguma.
- As cópias de evidências eletrônicas são idênticas aos originais.
- Qualquer sistema de informação a partir do qual as evidências foram coletadas estava operando corretamente no momento em que a evidência foi registrada.

9.19. Segurança da informação durante a disrupção:

A Unimed Ituiutaba deve estabelecer um plano robusto para assegurar que a segurança da informação seja mantida em níveis apropriados durante períodos de disrupção. Isso inclui a identificação de riscos específicos relacionados à segurança da informação em cenários de interrupção, a implementação de controles compensatórios e a manutenção de uma comunicação clara e segura com todas as partes interessadas. Os processos críticos devem estar respaldados por soluções que garantam confidencialidade, integridade e disponibilidade das informações, mesmo em condições adversas. O planejamento deve prever procedimentos de resposta a incidentes, autenticação reforçada e acesso controlado para minimizar impactos durante situações de crise.

9.20. Prontidão de TIC para continuidade de negócios:

9.20.1. Planejamento

9.20.1.1. Análise de Impacto nos Negócios (BIA - Business Impact Analysis):

- Identificar os sistemas e serviços de TIC críticos para os processos de negócios.
- Estimar o impacto financeiro, operacional e reputacional de possíveis interrupções.
- Determinar os requisitos de tempo de recuperação (RTO - Recovery Time Objective) e os objetivos de ponto de recuperação (RPO - Recovery Point Objective).

9.20.1.2. Gestão de Riscos de TIC:

- Realizar uma avaliação de riscos para identificar vulnerabilidades e ameaças aos sistemas de TIC.
- Desenvolver estratégias para mitigar os riscos, como redundância, backups, segurança cibernética e sistemas de failover.

9.20.1.3. Definição de Políticas e Diretrizes:

- Estabelecer políticas claras de continuidade de TIC alinhadas aos objetivos gerais da Unimed Ituiutaba.
- Documentar planos de continuidade específicos para a infraestrutura e os serviços críticos de TIC.

9.20.2. Implementação

9.20.2.1. Infraestrutura Resiliente:

- Implantar sistemas redundantes e de alta disponibilidade, como clusters de servidores, redes alternativas e armazenamento em nuvem.
- Configure backups regulares e offsite para proteger dados críticos.

9.20.2.2. Automação de Processos:

- Utilizar soluções de automação para monitorar e gerenciar incidentes.
- Implemente ferramentas de monitoramento em tempo real para detectar falhas e ameaças rapidamente.

9.20.2.3. Segurança de TIC:

- Adotar práticas robustas de segurança cibernética, incluindo firewalls, criptografia, controles de acesso e monitoramento contínuo.

9.20.2.4. Treinamento e Capacitação:

- Capacitar a equipe de TIC em resposta a incidentes e em práticas de continuidade de negócios.
- Realizar campanhas de conscientização sobre segurança cibernética para todos os colaboradores.

9.20.3. Manutenção

9.20.3.1. Monitoramento Contínuo:

- Estabelecer processos de monitoramento proativo para identificar e corrigir problemas antes que eles escalem.

9.20.3.2. Atualizações e Melhorias:

- Atualizar regularmente sistemas, softwares e hardware para garantir compatibilidade e segurança.
- Revisar e ajuste os planos de continuidade de TIC conforme as necessidades da Unimed Ituiutaba e o ambiente tecnológico evoluem.

9.20.3.3. Gestão de Fornecedores:

- Garantir que fornecedores e parceiros de TIC estejam alinhados aos padrões de continuidade exigidos pela Unimed Ituiutaba.
- Negociar contratos que incluam SLAs (Service Level Agreements) específicos para continuidade de negócios.

9.20.4. Testes

9.20.4.1. Simulações e Exercícios:

- Realizar testes regulares, como simulações de falhas de TIC e exercícios de recuperação.
- Avaliar o desempenho da equipe e a eficácia dos planos durante os testes.

9.20.4.2. Testes de Backups e Restauração:

- Validar a integridade e a funcionalidade dos backups executando testes de recuperação periódicos.

9.20.4.3. Testes de Desempenho:

- Verificar a capacidade de resposta e resiliência da infraestrutura de TIC em condições de estresse, como picos de demanda ou ataques cibernéticos.

9.20.4.4. Avaliação Pós-Teste:

- Documentar os resultados dos testes e identifique áreas de melhoria.
- Atualizar os planos e procedimentos com base nos aprendizados obtidos.

9.21. Requisitos legais, estatutários, regulamentares e contratuais:

A prontidão de TIC deve ser planejada, implementada e mantida de forma a suportar os objetivos de continuidade de negócios, assegurando que os serviços essenciais possam ser restabelecidos de

maneira rápida e eficaz. Isso inclui a realização de uma análise de impacto nos negócios, a definição de requisitos de recuperação e o desenvolvimento de planos de recuperação de desastres. Testes regulares devem ser conduzidos para validar a eficácia das medidas implementadas, e atualizações periódicas são necessárias para incorporar mudanças tecnológicas ou organizacionais. A integração com os objetivos estratégicos e operacionais da Unimed Ituiutaba é fundamental para garantir a resiliência e a continuidade dos serviços de TIC.

9.22. Direitos de propriedade intelectual:

A Unimed Ituiutaba implementa os seguintes procedimentos para proteger os direitos de propriedade intelectual:

- Adquirir software somente por meio de fontes conhecidas e confiáveis, para assegurar que os direitos autorais não sejam violados;
- Manter registros apropriados de ativos e identificar todos os ativos com requisitos de proteção de direitos de propriedade intelectual;
- Manter provas e evidências de propriedade de licenças, manuais etc.;
- Assegurar que qualquer número máximo de usuários ou recursos (por exemplo, CPU) permitidos dentro da licença não seja excedido;
- Realizar análises críticas para assegurar que apenas softwares autorizados e produtos licenciados sejam instalados;
- Manter o compliance dos termos e condições de software e informações obtidas de redes públicas e fontes externas;
- Não duplicar, converter para outro formato ou extrair de gravações comerciais (vídeo, áudio) outro além do permitido pela lei de direitos autorais e as licenças aplicáveis;

- Não copiar, total ou parcialmente, normas (por exemplo, normas internacionais ISO/IEC), livros, artigos, relatórios ou outros documentos, além do permitido pela lei de direitos autorais e as licenças aplicáveis.

9.23. Proteção de registros:

A Unimed Ituiutaba deve implementar um plano abrangente para proteger registros contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada. Esse plano deve incluir medidas como:

- Criação de backups regulares armazenados em locais seguros;
- Controle rigoroso de acesso com autenticação baseada em níveis de permissão;
- Uso de criptografia para proteção de dados confidenciais em trânsito e em repouso;
- Monitoramento contínuo para detecção de tentativas de acesso não autorizado;
- Definição de um plano de recuperação para restaurar registros em caso de falhas ou incidentes.

Além disso, deve-se garantir que os registros sejam gerenciados de acordo com o ciclo de vida definido e em conformidade com leis e regulamentações aplicáveis.

9.24. Privacidade e proteção de DP:

A Unimed Ituiutaba deve identificar e atender aos requisitos relacionados à privacidade e proteção de dados pessoais em conformidade com as leis e regulamentos aplicáveis, como a LGPD (Lei Geral de Proteção de Dados) no Brasil, o GDPR na Europa ou outros marcos regulatórios relevantes. As ações incluem:

- Realizar mapeamento de dados pessoais para identificar quais dados são coletados, processados, armazenados e compartilhados;

- Estabelecer políticas e procedimentos claros para a coleta, uso, retenção e descarte de dados pessoais;
- Garantir o consentimento explícito dos titulares de dados, quando necessário;
- Implementar controles técnicos e organizacionais para proteger os dados pessoais contra acessos e violações não autorizados;
- Conduzir treinamentos regulares para conscientizar os colaboradores sobre a proteção de dados pessoais;
- Realizar auditorias periódicas para assegurar conformidade com os requisitos legais e contratuais.

9.25. Análise crítica independente da segurança da informação:

A abordagem da Unimed Ituiutaba para gerenciar a segurança da informação será baseada em uma combinação de pessoas, processos e tecnologias, alinhada a um Sistema de Gestão de Segurança da Informação (SGSI). Para garantir a eficácia, será realizada uma análise crítica independente, a intervalos planejados ou após mudanças significativas, incluindo:

- Auditorias conduzidas por terceiros qualificados e imparciais para avaliar a conformidade com políticas internas, padrões de mercado (como ISO 27001) e requisitos legais;
- Revisões internas conduzidas por equipes que não estejam diretamente envolvidas na implementação dos controles;
- Identificação de não conformidades e riscos emergentes, seguidos por planos de ação corretivos e preventivos;
- Apresentação dos resultados para a alta administração, garantindo que ajustes estratégicos sejam realizados conforme necessário;

Garantia de que as análises críticas considerem incidentes de segurança, mudanças no ambiente tecnológico e as melhores práticas do setor.

9.26. Compliance com políticas, regras e normas para segurança da informação:

A Unimed Ituiutaba deve garantir que sua política de segurança da informação, assim como políticas, regras e normas específicas relacionadas a temas como gestão de acesso, proteção de dados, continuidade de negócios e segurança de TIC, sejam implementadas, monitoradas e revisadas regularmente para assegurar o compliance.

As ações incluem:

- Estabelecer um processo de auditoria regular para avaliar a conformidade com as políticas internas e normas externas aplicáveis (como ISO 27001, LGPD, GDPR, entre outras);
- Promover treinamentos regulares e campanhas de conscientização para todos os colaboradores sobre as políticas e normas de segurança da informação;
- Monitorar a aplicação e eficácia dos controles através de ferramentas de monitoramento e indicadores de desempenho (KPIs);
- Conduzir revisões periódicas por equipes internas e/ou externas para identificar desvios ou não conformidades;
- Elaborar relatórios de conformidade e apresentá-los para a alta direção, que deve assegurar a implementação de ações corretivas e melhorias contínuas;
- Garantir que qualquer nova política ou mudança nas normas seja comunicada de forma clara e integrada aos processos organizacionais.

9.27. Documentação dos procedimentos de operação:

Os procedimentos operacionais relacionados aos recursos de tratamento da informação devem ser documentados de maneira clara e acessível, garantindo sua disponibilização apenas para o pessoal autorizado e que necessite deles.

Para isso, a Unimed Ituiutaba deve:

- Criar manuais detalhados descrevendo as etapas operacionais necessárias para a gestão de sistemas e recursos de informação, incluindo backups, recuperação de desastres, gestão de acesso e manutenção de infraestrutura;
- Armazenar a documentação em repositórios seguros e centralizados, com controle de versões para garantir que sempre esteja atualizada;
- Garantir que o acesso à documentação seja restrito a indivíduos que desempenhem funções específicas relacionadas à operação dos recursos de tratamento da informação;
- Realizar revisões periódicas da documentação para assegurar que esteja alinhada a mudanças nos processos, tecnologias ou requisitos regulatórios;
- Disponibilizar a documentação em formatos que facilitem sua utilização no dia a dia, como guias digitais interativos ou checklists operacionais.

10.CONTROLE DE PESSOAS

10.1. Seleção:

A Unimed Ituiutaba deve realizar verificações de antecedentes de todos os candidatos antes de sua contratação. Essas verificações devem ser conduzidas de forma ética e em conformidade com as leis e regulamentações aplicáveis, como a LGPD, garantindo que sejam proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos. O processo pode incluir:

- Consulta a referências profissionais;
- Verificação de qualificações acadêmicas e certificações;
- Pesquisa de histórico criminal, conforme permitido pelas leis locais;
- Avaliação contínua, quando aplicável, para funções críticas relacionadas à segurança da informação.

10.2. Termos e condições de contratação:

Os contratos de trabalho devem incluir cláusulas específicas que estabeleçam as responsabilidades do colaborador e da Unimed Ituiutaba em relação à segurança da informação. Essas cláusulas devem:

- Informar sobre as políticas de segurança da Unimed Ituiutaba;
- Definir responsabilidades de confidencialidade e proteção de informações sensíveis;
- Incluir penalidades em caso de violações de segurança;
- Descrever os direitos e obrigações do colaborador no uso de sistemas e recursos da Unimed Ituiutaba.

10.3. Conscientização, educação e treinamento em segurança da informação:

Todos os colaboradores e partes interessadas relevantes devem receber treinamento inicial e contínuo sobre segurança da informação. Esse treinamento deve incluir:

- Política de segurança da informação da Unimed Ituiutaba;
- Procedimentos específicos por função ou tema, como proteção de dados e gestão de incidentes;
- Atualizações regulares sobre novas ameaças e melhores práticas;
- Simulações e treinamentos práticos, como resposta a phishing.

O objetivo é garantir que todos compreendam suas responsabilidades na proteção das informações da Unimed Ituiutaba.

10.4. Processo disciplinar:

O processo disciplinar da Unimed Ituiutaba deve ser formalizado e comunicado a todos os colaboradores e partes interessadas relevantes. Ele deve prever:

- Investigação de incidentes de violação das políticas de segurança;
- Aplicação de ações proporcionais, desde advertências até demissões, dependendo da gravidade da violação;
- Garantia de conformidade com leis trabalhistas e regulamentos aplicáveis.

10.5. Responsabilidades após encerramento ou mudança da contratação:

As responsabilidades de segurança da informação que permanecem válidas após o término ou mudança da contratação devem ser definidas e comunicadas. Elas incluem:

- Devolução de equipamentos e materiais da Unimed Ituiutaba;
- Revogação de acessos a sistemas e informações;
- Continuidade de obrigações de confidencialidade e não divulgação;
- Exclusão de dados corporativos armazenados em dispositivos pessoais.

10.6. Acordos de confidencialidade ou não divulgação:

Os acordos de confidencialidade ou não divulgação (NDAs) devem ser identificados, documentados, revisados regularmente e assinados por colaboradores e partes interessadas relevantes. Esses acordos devem abordar:

- Proteção de informações sensíveis e proprietárias;
- Proibições de divulgação não autorizada;
- Penalidades para violações contratuais.

10.7. Trabalho remoto:

As seguintes medidas de segurança devem ser implementadas para proteger informações acessadas, tratadas ou armazenadas durante o trabalho remoto:

- Uso de VPNs e autenticação multifator para acesso remoto;

- Dispositivos corporativos com criptografia e software de segurança atualizados;
- Proibição de acesso a informações sensíveis em redes públicas ou não seguras;
- Treinamento sobre boas práticas de segurança em home office.

10.8. Relatos de eventos de Segurança da Informação:

A Unimed Ituiutaba deve oferecer mecanismos seguros e acessíveis para que todos relatem eventos de segurança observados ou suspeitos. Esses mecanismos devem incluir:

- Um canal dedicado, como e-mail ou hotline de segurança;
- Opção de relatos anônimos, quando aplicável;
- Garantia de resposta rápida e investigação dos relatos;
- Comunicação de retorno para o relator, se necessário.

10.9. Informação documentada:

A informação documentada relacionada ao controle de pessoas está formalizada na plataforma Unimed Ituiutaba. Os documentos incluem:

- Política de Compliance;
- Política de Benefícios;
- Código de Ética e Conduta;
- Política de Trabalho Remoto;
- Política de Treinamento em Segurança da Informação;
- Termos de Confidencialidade e Não Divulgação (NDAs);
- Manual do Colaborador.

11.CONTROLES FÍSICOS

11.1. Segurança Física e o Ambiente:

11.1.1. Perímetros de segurança física:

Os perímetros de segurança onde há manipulação de informações são definidos e usados para proteger tanto as áreas que contenham informação e outros ativos associados.

Para evitar acesso físico não autorizado, a Unimed Ituiutaba dispõe de:

- Câmera;
- Alarme;
- Portas protegidas contra acesso não autorizado;
- Janelas protegidas contra acesso não autorizado;
- Barreiras.
- Fechaduras;

11.1.2. Entrada física:

As áreas seguras são protegidas por controles de entradas por meio de:

- Fechaduras;
- Registro de entrada e saída para visitantes;
- Registro de entrada e saída para colaboradores;

Visitantes devem ser supervisionados, a menos que uma exceção documentada seja concedida.

11.1.3. Segurança de escritórios, salas e instalações:

Os escritórios, salas e instalações são protegidas por meio de:

- Salas com design discreto, projetado para minimizar a identificação de atividades relacionadas ao tratamento de informações.;
- Não divulgar ramais internos e mapas online;

11.1.4. Monitoramento de segurança física:

Para detectar e impedir o acesso físico não autorizado o monitoramento inclui:

- Vídeo monitoramento;
- Alarme de intrusos;
- Detectores de movimento;
- Sensores infravermelho;

11.1.5. Proteção contra ameaças físicas e ambientais:

São projetadas e aplicadas proteção física contra desastres naturais, ameaças físicas intencionais ou não intencionais por meio de proteções prevista:

- Auto de Vistoria do Corpo de Bombeiros (AVCB);
- Proteção de sobrecarga elétrica (para-raios);

11.1.6. Trabalho em áreas seguras:

As salas da direção são consideradas áreas seguras não sendo monitoradas por câmeras e não é permitido a utilização de dispositivos de gravação de áudio e imagem por pessoas externas.

11.1.7. Localização e proteção de equipamentos:

Os equipamentos de gravação e monitoramento de vídeo estão localizados no datacenter da Unimed Ituiutaba, que conta com câmeras estrategicamente posicionadas em postos-chave, incluindo as entradas do local.

11.1.8. Serviços de Infraestrutura:

- **Fontes de Energia Redundantes**: como nobreaks e gerador a diesel.
- **Manutenção Preventiva**: Realizar inspeções regulares e manutenção dos equipamentos elétricos, como painéis de distribuição, baterias de UPS e geradores.
- **Monitoramento Contínuo**: Implementar sistemas de monitoramento para identificar problemas elétricos antes que eles se tornem críticos.
- **Climatização Adequada**: Garantir sistemas de refrigeração eficientes para prevenir superaquecimento de equipamentos.
- **Planejamento de Recuperação de Desastres**: Estabelecer e testar regularmente um plano de recuperação para minimizar os impactos de falhas.
- **Segurança Física e Acesso Restrito**: Garantir que apenas pessoal autorizado tenha acesso às áreas críticas para reduzir o risco de danos acidentais ou intencionais.

11.1.9. Segurança do cabeamento:

Encaminhamento Seguro:

- Instalar os cabos em dutos ou canaletas protegidas, preferencialmente subterrâneas ou em locais de difícil acesso.
- Evitar trajetos expostos ou áreas de alto risco, como próximas a maquinários pesados ou zonas de tráfego intenso.

Blindagem:

- Utilizar cabos blindados para reduzir a interferência eletromagnética (EMI) e proteger contra acessos não autorizados.
- Implementar proteção adicional contra surtos elétricos e descargas atmosféricas.

Segurança Física:

- Proteger os dutos e canaletas com estruturas resistentes a impactos, como aço ou materiais reforçados.
- Monitorar fisicamente os pontos de entrada e saída de cabos com sensores ou câmeras.

Controle de Acesso:

- Restringir o acesso a áreas onde os cabos estão instalados, permitindo a entrada apenas de pessoal autorizado.
- Implementar medidas de vigilância, como alarmes em pontos críticos.

Redundância e Roteamento Alternativo:

- Planejar rotas alternativas para garantir a continuidade dos serviços em caso de falha ou danos em um trajeto específico.
- Utilizar sistemas redundantes para evitar interrupções.

Proteção Contra Interceptação:

- Criptografar os dados transmitidos pelos cabos para evitar interceptação, mesmo que fisicamente acessados.
- Realizar inspeções regulares para identificar sinais de manipulação ou acessos não autorizados.

Prevenção de Danos:

- Implementar sinalização adequada para evitar danos acidentais durante obras ou manutenção.
- Realizar mapeamento e documentação detalhada das rotas de cabos para prevenir perfurações acidentais.

11.1.10. Segurança de ativos fora das instalações da Unimed Ituiutaba:

11.1.10.1. Inventário e Classificação:

- Manter um inventário atualizado de todos os ativos externos, identificando sua localização, responsável e finalidade.
- Classificar os ativos de acordo com sua criticidade e sensibilidade para priorizar medidas de proteção.

11.1.10.2. Segurança Física:

- Armazenar os ativos em locais seguros, como armários trancados, cofres ou áreas monitoradas por câmeras e alarmes.
- Fornecer dispositivos de rastreamento para ativos de alto valor ou criticidade, como laptops e dispositivos móveis.

11.1.11. Controle de Acesso:

- Garantir que somente pessoal autorizado tenha acesso aos ativos externos.
- Usar autenticação multifator para dispositivos móveis, laptops ou sistemas remotos conectados à Unimed Ituiutaba

11.1.12. Proteção de Dados:

- Implementar criptografia em dispositivos e mídias que armazenem informações sensíveis.
- Garantir a utilização de VPNs seguras para conexões remotas à rede da Unimed Ituiutaba.

11.1.13. Segurança Contra Perda ou Roubo:

- Equipar dispositivos com soluções de rastreamento e capacidade de bloqueio ou limpeza remota em caso de perda ou roubo.
- Treinar os funcionários para seguirem práticas seguras de transporte e armazenamento de ativos.

11.1.14. Inspeções e Auditorias:

- Realizar inspeções periódicas para verificar as condições dos ativos externos e garantir sua proteção.
- Auditar regularmente o uso de dispositivos externos para identificar possíveis vulnerabilidades.

11.1.15. Contratos e Acordos com Terceiros:

- Estabelecer contratos claros com prestadores de serviços que utilizem ou tenham acesso aos ativos fora das instalações, incluindo cláusulas de segurança.
- Monitorar e avaliar continuamente os níveis de segurança implementados por terceiros.

11.1.16. Plano de Resposta a Incidentes:

- Definir procedimentos claros para responder a incidentes relacionados a ativos externos, como roubo, dano ou acessos não autorizados.
- Garantir que os responsáveis saibam como reportar e lidar com tais incidentes.

11.1.17. Proteção Contra Condições Ambientais:

- Fornecer embalagens e cases adequados para proteger dispositivos móveis e mídias de armazenamento contra impactos, umidade, poeira e temperaturas extremas.

11.2. Mídia de armazenamento:

11.2.1. Aquisição

- **Padronização:** Adquirir mídias de armazenamento somente de fornecedores confiáveis e previamente aprovados pela Unimed Ituiutaba.

- **Registro e Identificação**: Registrar todas as mídias adquiridas em um inventário detalhado, associando-as a um responsável e ao tipo de informação que será armazenada.
- **Classificação**: Definir o nível de classificação das informações que poderão ser armazenadas na mídia no momento da aquisição.

11.2.2. Uso

- **Autenticação e Controle de Acesso**: Configurar permissões de acesso baseadas na classificação da informação, utilizando autenticação segura (como senhas fortes ou criptografia).
- **Proteção Física e Lógica**: Proteger as mídias contra danos físicos, como impacto, umidade ou temperatura extrema, e contra acesso não autorizado, utilizando criptografia para dados sensíveis.

- **Rastreamento de Uso**: Registrar quem acessa e utiliza a mídia, mantendo logs auditáveis, especialmente para informações classificadas como confidenciais ou restritas.
- **Treinamento**: Garantir que os usuários sejam treinados no manuseio correto de mídias de armazenamento, especialmente aquelas contendo informações sensíveis.

11.2.3. Transporte

- **Proteção Contra Interceptação e Perda:**
  - Utilizar embalagens seguras e lacradas para transporte físico de mídias sensíveis.
  - Adotar meios seguros de transporte, como serviços de entrega confiáveis ou mensageiros treinados.
- **Criptografia Durante o Transporte**: Assegurar que os dados armazenados na mídia estejam criptografados para prevenir acessos não autorizados em caso de perda ou roubo.
- **Rastreamento**: Implementar mecanismos para rastrear mídias em trânsito, incluindo confirmações de entrega.

11.2.4. Descarte

- **Revisão e Aprovação**: Garantir que o descarte de mídias siga políticas internas e seja aprovado pelos responsáveis pela gestão de informações.
- **Destruição Física**: Realizar a destruição física de mídias classificadas como sensíveis ou confidenciais por meio de métodos certificados, como trituração ou desmagnetização.
- **Exclusão Segura de Dados**:

- Utilizar ferramentas de software para apagar permanentemente os dados de mídias reutilizáveis.
- Certificar que os dados não possam ser recuperados após o descarte.

Documentação: Registrar o descarte, incluindo o método utilizado, o responsável pelo procedimento e o tipo de mídia descartada.

11.2.5. Conformidade com o Esquema de Classificação e Requisitos

- **Adesão às Políticas de Classificação:**
  - Garantir que cada etapa do ciclo de vida da mídia esteja de acordo com o esquema de classificação da Unimed Ituiutaba, como restrito, confidencial ou público.
- **Requisitos de Manuseio**: Assegurar que o tratamento das mídias esteja alinhado aos requisitos de segurança definidos para cada nível de classificação, como períodos de retenção de dados e políticas de acesso.

11.3. Manutenção de equipamentos:

11.3.1. Planejamento e Registro da Manutenção

- **Cronograma de Manutenção:**
  - Estabelecer e seguir um cronograma de manutenção preventiva para todos os equipamentos.
  - Realizar inspeções regulares para identificar falhas potenciais antes que comprometam os serviços.
- **Registro de Atividades:**
  - Documentar todas as atividades de manutenção, incluindo data, responsável, equipamento, e ações realizadas.

- Manter histórico de manutenção para análise de desempenho e rastreabilidade.

11.3.2. Disponibilidade.

- **Redundância de Equipamentos:**
  - Implementar redundância para equipamentos críticos, como servidores, switches, e unidades de armazenamento.
  - Garantir que sistemas de backup estejam operacionais e testados periodicamente.
- **Monitoramento Contínuo**:
  - Utilizar ferramentas de monitoramento para identificar falhas e evitar interrupções no funcionamento dos equipamentos.
- **Reposição de Peças**:
  - Manter estoque adequado de peças de reposição para reparos rápidos em caso de falhas.

11.3.3. Integridade

- **Manutenção Física:**
  - Proteger os equipamentos contra danos físicos, como impacto, poeira, umidade e variações de temperatura, utilizando ambientes controlados.
- **Atualizações de Firmware e Software:**
  - Aplicar atualizações regularmente para corrigir falhas, otimizar o desempenho e proteger contra vulnerabilidades.

- Testar as atualizações antes de aplicá-las em ambientes de produção para evitar impactos negativos.

- **Inspeção de Componentes:**
  - Verificar regularmente o estado dos cabos, conectores, discos rígidos e demais componentes para garantir a integridade física dos equipamentos.

11.3.4. Confidencialidade

- **Acesso Restrito:**
  - Limitar o acesso físico aos equipamentos a pessoal autorizado, utilizando controles de acesso, como biometria ou cartões magnéticos.
- **Proteção de Dados:**
  - Garantir que todos os dados armazenados em equipamentos sejam criptografados, minimizando o risco de acessos não autorizados.
- **Manutenção Segura:**
  - Durante as atividades de manutenção, garantir que os dados confidenciais não sejam expostos. Sempre acompanhar técnicos terceirizados e aplicar políticas de segurança para terceiros.
- **Descarte Seguro:**
  - Antes de descartar ou substituir equipamentos, realizar a remoção segura de dados utilizando técnicas de sobrescrita ou destruição física.

11.3.5. Procedimentos de Recuperação

- **Planos de Contingência:**
  - Estabelecer planos de recuperação para rápida substituição ou reparo de equipamentos em caso de falhas inesperadas.
- **Testes Regulares:**
  - Realizar testes periódicos de recuperação para validar a eficácia dos procedimentos de contingência.

11.3.6. Conformidade com Políticas e Normas

- **Auditorias e Inspeções:**
  - Realizar auditorias regulares para garantir que as práticas de manutenção estejam alinhadas às políticas internas e a normas regulatórias.
- **Treinamento:**
  - Garantir que a equipe responsável pela manutenção esteja devidamente treinada e atualizada em práticas de segurança e manuseio de equipamentos.

11.4. Descarte seguro ou reutilização de equipamentos:

11.4.1. Identificação e Registro

- **Inventário dos Equipamentos:**
  - Manter um registro detalhado de todos os equipamentos que contenham mídia de armazenamento, identificando sua localização, responsável e classificação das informações armazenadas.

- **Avaliação Inicial:**
  - Determinar o tipo de dados armazenados (confidenciais, restritos ou públicos) e o software licenciado presente nos equipamentos.

11.4.2. Remoção Segura de Dados

- **Métodos de Exclusão:**
  - **Sobrescrita de Dados:** Utilizar ferramentas certificadas de sobrescrita para substituir os dados armazenados na mídia por padrões aleatórios, garantindo que não possam ser recuperados.
  - **Desmagnetização:** Aplicar processos de desmagnetização (degaussing) para inutilizar a mídia e apagar permanentemente os dados.
  - **Criptografia Prévia:** Para mídias previamente criptografadas, destruir as chaves de criptografia de maneira segura para tornar os dados irreversíveis.
  - **Verificação Pós-Exclusão:** Realizar testes para confirmar que os dados foram completamente removidos e não podem ser recuperados utilizando ferramentas de recuperação.

11.4.3. Desinstalação de Software Licenciado

- **Revogação de Licenças:**
  - Remover ou desativar licenças de software instaladas nos equipamentos, garantindo conformidade com contratos de licenciamento.
- **Registro de Desinstalação:**

- Documentar o processo de remoção de softwares para auditorias e conformidade legal.

11.4.4. Substituição ou Reutilização

- **Substituição Segura:**
  - Se a mídia será reutilizada internamente, sobrescrever os dados existentes com informações padrão ou sistemas operacionais aprovados.
  - Garantir que nenhum dado anterior esteja acessível antes da redistribuição.
- **Classificação Antes da Reutilização:**
  - Avaliar os requisitos de classificação e ajustar as permissões de acesso para uso futuro.

11.4.5. Descarte Seguro

- **Destruição Física:**
  - Para mídias que não serão reutilizadas, realizar a destruição física por meio de métodos certificados, como trituração ou pulverização.
- **Contratação de Empresas Especializadas:**
  - No caso de descarte terceirizado, contratar empresas certificadas que garantam a destruição segura de dados, com emissão de laudos ou certificados de descarte seguro.
- **Documentação do Descarte:**
  - Registrar o descarte de cada item, incluindo o método de destruição utilizado, o responsável pelo processo e a data.

11.4.6. Conformidade com Políticas e Normas

- **Alinhamento às Políticas da Unimed Ituiutaba:**
  - Garantir que todos os processos de remoção, substituição ou descarte estejam em conformidade com as políticas de segurança da informação da Unimed Ituiutaba.
- **Adesão a Normas e Regulamentações:**
  - Seguir normas e regulamentações aplicáveis, como a LGPD, ISO/IEC 27001 e outras específicas do setor.

11.4.7. Auditorias e Verificações

- **Inspeções Regulares:**
  - Realizar auditorias para garantir que as práticas de remoção e descarte sejam realizadas de forma consistente e eficaz.
- **Treinamento:**
  - Capacitar a equipe responsável para realizar os processos com precisão e de acordo com os padrões de segurança.

12.CONTROLES TECNOLÓGICOS

12.1. Configuração e Manuseio Seguros de Dispositivos Endpoint do Usuário:

Todos os ativos utilizados pela Unimed Ituiutaba, quando aplicáveis, possuem controles de endpoints. Os endpoints são controlados por meio de: firewall, antivírus, antimalware e vault.

12.2. Direitos de acessos privilegiados:

12.2.1. Princípio do Menor Privilégio

- **Atribuição Baseada na Necessidade:**
  - Garantir que os acessos privilegiados sejam concedidos somente a usuários cuja função requer explicitamente tais permissões.
- **Segmentação de Funções:**
  - Evitar que um único usuário tenha acesso a várias funções críticas que possam comprometer a segurança (ex.: separação de tarefas administrativas e financeiras).

12.2.2. Processo de Atribuição

- **Autorização Formal:**
  - Exigir uma solicitação formal e documentada para concessão de acessos privilegiados, aprovada por um gestor ou responsável autorizado.
- **Definição de Papéis e Perfis:**
  - Criar perfis de acesso com permissões específicas para cada função, reduzindo o risco de concessões excessivas.
- **Registro e Documentação:**
  - Registrar todas as concessões de acessos privilegiados, incluindo o responsável pela aprovação e o usuário beneficiado.

12.2.3. Gerenciamento Contínuo

- **Monitoramento de Acessos:**
  - Implementar ferramentas de monitoramento que registrem e analisem atividades realizadas com privilégios elevados.
  - Configurar alertas para acessos suspeitos ou não autorizados.

- **Revisão Periódica:**
  - Realizar revisões regulares das permissões concedidas, garantindo que acessos desnecessários sejam revogados imediatamente.
- **Limitação de Sessões Privilegiadas:**
  - Configurar políticas para restringir a duração das sessões com acesso privilegiado e forçar a desconexão após inatividade.

12.2.4. Controle de Senhas e Credenciais

- **Senhas Fortes:**
  - Exigir a utilização de senhas fortes e únicas para contas privilegiadas, com renovação periódica.
- **Gerenciadores de Senhas:**
  - Utilizar ferramentas seguras para armazenar e gerenciar credenciais de acessos privilegiados.
- **Autenticação Multifator (MFA):**
  - Implementar autenticação multifator para todas as contas privilegiadas, adicionando uma camada extra de segurança.

12.2.5. Restrição de Uso

- **Ambientes de Produção e Testes:**
  - Restringir o uso de acessos privilegiados em ambientes de produção e testes, permitindo apenas quando absolutamente necessário.
- **Acesso Temporário:**

- Conceder acessos privilegiados temporários para atividades específicas, com remoção automática após o término do prazo ou tarefa.

12.2.6. Registro e Auditoria

- **Logs Detalhados:**
  - Registrar todas as atividades realizadas com acessos privilegiados, incluindo alterações em sistemas, configurações e exclusão de dados.
- **Auditorias Regulares:**
  - Realizar auditorias periódicas para verificar o uso apropriado dos acessos privilegiados e identificar possíveis abusos ou violações.
- **Relatórios Gerenciais:**
  - Gerar relatórios detalhados para análise de conformidade e rastreamento de atividades suspeitas.

12.2.7. Treinamento e Conscientização

- **Capacitação dos Usuários:**
  - Oferecer treinamento contínuo para os usuários com acessos privilegiados, abordando as responsabilidades e boas práticas de segurança.
- **Conscientização de Riscos:**
  - Garantir que os usuários compreendam os riscos associados ao uso indevido de privilégios e as consequências de violações.

12.2.8. Gestão de Incidentes

- **Resposta a Incidentes:**

- Estabelecer um plano de resposta para casos de abuso de acessos privilegiados, com procedimentos claros de investigação e mitigação.

- **Revogação Imediata:**
  - Revogar imediatamente os acessos de usuários que deixam a Unimed Ituiutaba, mudam de função ou apresentem comportamento suspeito.

12.2.9. Conformidade com Normas e Políticas

- **Adesão às Políticas Internas:**
  - Alinhar a gestão de acessos privilegiados às políticas de segurança da informação da Unimed Ituiutaba.
- **Regulamentações e Normas:**
  - Seguir requisitos legais e normativos aplicáveis, como ISO/IEC 27001 e LGPD, para garantir a conformidade.

12.3. Restrição de acesso à informação:

O acesso às informações e a outros ativos associados deve ser restrito de acordo com as políticas específicas da Unimed Ituiutaba sobre controle de acesso, assegurando a confidencialidade, integridade e disponibilidade das informações. As diretrizes incluem:

- **Princípio do Menor Privilégio**: Os usuários devem ter acesso apenas às informações necessárias para desempenhar suas funções, com permissões configuradas com base em seus papéis e responsabilidades.
- **Controle Baseado em Funções (RBAC)**: Implementar controles de acesso baseados em funções, limitando permissões a grupos de usuários com necessidades específicas.
- **Autenticação e Autorizações**: Garantir que o acesso às informações seja autorizado e autenticado, utilizando tecnologias seguras, como autenticação multifator (MFA).

- **Revisões Periódicas**: Realizar revisões regulares das permissões de acesso, revogando acessos desnecessários ou desatualizados.
- **Monitoramento e Auditoria**: Monitorar e auditar continuamente o acesso às informações para identificar acessos não autorizados ou suspeitos.

12.4. Acesso ao código fonte:

O gerenciamento do acesso ao código-fonte, ferramentas de desenvolvimento e bibliotecas de software deve garantir a proteção contra alterações não autorizadas, vazamentos e mal uso. As práticas incluem:

- **Controle de Leitura e Escrita**:
  - Permitir acesso de leitura ao código-fonte apenas para desenvolvedores ou colaboradores autorizados.
  - Restringir acessos de escrita a membros específicos da equipe de desenvolvimento com autorização para modificar o código.
- **Ambientes Segregados**:
  - Garantir a segregação entre os ambientes de desenvolvimento, teste e produção para evitar impactos em sistemas críticos.
- **Ferramentas de Controle de Versão**:
  - Utilizar sistemas de controle de versão (como Git) para rastrear alterações no código e identificar autores de modificações.
- **Autenticação e Registro**:
  - Aplicar autenticação forte para acessar repositórios de código e manter registros detalhados de acessos e alterações realizadas.
- **Revisões de Código**:

- Estabelecer processos de revisão e aprovação de código antes da implementação em produção, garantindo qualidade e conformidade com os padrões organizacionais.

12.5. Autenticação segura:

As tecnologias e procedimentos de autenticação devem ser implementados com base nas políticas específicas de controle de acesso e restrição de informações. As medidas incluem:

- **Autenticação Multifator (MFA):**
  - Implementar MFA em todos os sistemas críticos, combinando algo que o usuário sabe (senha) com algo que o usuário possui (token, dispositivo móvel) ou algo que o usuário é (biometria).
- **Senhas Seguras:**
  - Exigir senhas fortes, com requisitos mínimos de comprimento e complexidade, e estabelecer políticas para renovação periódica.
- **Certificados Digitais:**
  - Utilizar certificados digitais para autenticar usuários e dispositivos, garantindo maior segurança nas conexões.
- **Sessões Seguras:**
  - Configurar limites para a duração das sessões e implementar bloqueio automático após períodos de inatividade.
- **Gerenciamento de Identidade e Acesso:**
  - Integrar tecnologias de gerenciamento de identidade para centralizar e simplificar a autenticação de usuários em diferentes sistemas.

12.6. Gestão de capacidade:

A gestão de capacidade dos recursos deve ser monitorada e ajustada de acordo com os requisitos atuais e esperados, para garantir o desempenho e a continuidade das operações. As práticas incluem:

- **Monitoramento Contínuo**:
  - Utilizar ferramentas de monitoramento em tempo real para acompanhar o uso de recursos, como CPU, memória, armazenamento e largura de banda.
- **Planejamento de Capacidade**:
  - Realizar análises periódicas para prever demandas futuras e ajustar a infraestrutura de TI de acordo com os requisitos esperados.
- **Escalabilidade**:
  - Adotar soluções escaláveis (verticais e horizontais) que permitam expandir ou reduzir recursos conforme necessário.
- **Relatórios e Alertas**:
  - Gerar relatórios regulares sobre o uso de capacidade e configurar alertas para antecipar problemas antes que impactem as operações.
- **Otimização de Recursos**:
  - Identificar e desativar sistemas subutilizados, redistribuindo recursos para maximizar a eficiência.

12.7. Proteção contra malware:

A proteção contra malware deve ser implementada de forma abrangente, acompanhada por iniciativas de conscientização do usuário para prevenir ataques e incidentes de segurança. As diretrizes incluem:

- **Soluções Antimalware:**

- Instalar e manter softwares antimalware atualizados em todos os dispositivos, servidores e endpoints conectados à rede.

- **Atualizações e Patches:**
  - Garantir que sistemas operacionais e aplicativos estejam atualizados com os patches mais recentes para corrigir vulnerabilidades.
- **Monitoramento de Ameaças:**
  - Implementar sistemas de detecção e resposta a ameaças (EDR) para monitorar e mitigar atividades suspeitas em tempo real.
- **Treinamento e Conscientização:**
  - Promover campanhas regulares de conscientização para os usuários, abordando boas práticas, como evitar clicar em links desconhecidos e baixar arquivos de fontes não confiáveis.
- **Isolamento de Incidentes:**
  - Estabelecer políticas para isolar dispositivos infectados e mitigar rapidamente a propagação de malware na rede.
- **Backups Seguros:**
  - Realizar backups regulares de dados críticos e armazená-los em locais seguros e desconectados da rede principal para recuperação em caso de ataque.

12.8. Segurança de Redes:

A rede da Unimed Ituiutaba é gerenciada e controlada para proteger as informações nos sistemas e aplicações. Os controles são implementados para garantir a segurança da informação nestas redes, e a proteção dos serviços a elas conectadas, de acesso não autorizado, considerados os seguintes pontos:

a) as responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede são apenas da equipe de Tecnologia da Unimed Ituiutaba ou terceiros autorizados;

b) são aplicados mecanismos apropriados de registro e monitoração para habilitar a gravação e detecção de ações que possam afetar, ou ser relevantes para a segurança da informação;

c) os sistemas sobre as redes são autenticados;

d) a conexão de sistemas à rede é restrita, em alguns casos controlados pelo Firewall.

12.9. Segurança dos serviços de rede:

Os serviços de rede devem ser protegidos por meio de mecanismos de segurança adequados, níveis de serviço bem definidos e monitoramento contínuo. As principais práticas incluem:

12.9.1. Identificação dos Requisitos de Segurança

- **Mapeamento de Serviços**: Identificar os serviços de rede necessários para suportar as operações da Unimed Ituiutaba, como DNS, e-mail, VPN e servidores web.
- **Classificação de Dados**: Determinar os requisitos de segurança com base na sensibilidade e criticidade das informações transmitidas e processadas pelos serviços de rede.
- **Avaliação de Riscos**: Realizar análises de risco para identificar possíveis vulnerabilidades, ameaças e impactos associados aos serviços de rede.

12.9.2. Implementação de Mecanismos de Segurança

- **Criptografia de Dados:**
  - Garantir o uso de criptografia em trânsito (TLS/SSL) para proteger os dados transmitidos pela rede.
  - Implementar VPNs seguras para conexões remotas.
- **Controles de Acesso:**

- Configurar firewalls, proxies e controles de acesso baseados em IP para restringir conexões não autorizadas.
- Adotar autenticação multifator (MFA) para acesso a serviços críticos.

- **Segurança de Infraestrutura:**
  - Proteger servidores e dispositivos de rede com atualizações regulares de firmware e sistemas operacionais.
  - Desativar serviços e portas desnecessários para reduzir a superfície de ataque.

12.9.3. Definição de Níveis de Serviço

- **Acordos de Nível de Serviço (SLAs):**
  - Estabelecer SLAs claros para garantir a disponibilidade, desempenho e tempo de resposta dos serviços de rede.
  - Incluir métricas específicas de segurança, como tempos de resposta para mitigar incidentes.

12.9.4. Monitoramento e Gestão Contínua

- **Soluções de Monitoramento:**
  - Implementar ferramentas de monitoramento de rede em tempo real para detectar e responder a anomalias, como tráfego incomum ou tentativas de invasão.
- **Auditorias e Testes de Segurança:**
  - Realizar auditorias periódicas e testes de intrusão para avaliar a eficácia das medidas de segurança implementadas.
- **Gerenciamento de Logs:**
  - Configurar sistemas para registrar atividades de rede e analisar logs regularmente, identificando possíveis incidentes de segurança.

12.10. Segregação de redes:

A segregação de redes deve ser aplicada para separar grupos de serviços de informação, usuários e sistemas, garantindo maior segurança, desempenho e controle. As diretrizes para implementar a segregação de redes incluem:

12.10.1. Planejamento e Estruturação

- **Segmentação por Função:**
  - Criar sub-redes (VLANs) específicas para diferentes departamentos, funções ou níveis de sensibilidade, como redes de usuários, servidores, sistemas financeiros e IoT.
- **Separação de Serviços:**
  - Garantir que serviços críticos (ex.: servidores de banco de dados) estejam isolados de redes de usuários ou redes externas.

12.10.2. Implementação de Controles

- **Firewalls Internos:**
  - Configurar firewalls entre segmentos de rede para controlar o tráfego interno e evitar acessos não autorizados.
- **Zonas de Segurança:**
  - Criar zonas de segurança, como DMZs (Demilitarized Zones), para hospedar serviços expostos à internet, mantendo-os separados da rede interna.
- **Políticas de Roteamento:**
  - Definir políticas de roteamento e filtragem para limitar o tráfego entre segmentos de rede com base na necessidade de comunicação.

12.10.3. Gestão de Acessos

- **Princípio do Menor Privilégio:**
  - Restringir o acesso entre segmentos de rede apenas ao necessário para as operações, bloqueando conexões não essenciais.

- **Autenticação em Segmentos Sensíveis:**
  - Exigir autenticação adicional para acessar redes que contenham sistemas críticos ou dados sensíveis.

12.10.4. Monitoramento e Auditoria

- **Monitoramento de Tráfego:**
  - Utilizar sistemas de detecção de intrusões (IDS) e prevenção de intrusões (IPS) para monitorar o tráfego entre segmentos de rede e identificar atividades suspeitas.
- **Auditorias Regulares:**
  - Revisar a configuração de segregação periodicamente para garantir sua eficácia e conformidade com as políticas de segurança.

12.10.5. Benefícios da Segregação

- **Redução de Impacto:**
  - Limitar o alcance de possíveis incidentes de segurança, como ataques ou vazamentos de dados, restringindo-os a um único segmento de rede.
- **Melhoria no Desempenho:**
  - Evitar congestionamentos ao isolar serviços de alta demanda em segmentos dedicados.
- **Conformidade:**
  - Atender a requisitos de normas regulatórias, como ISO 27001, que recomendam a segregação de redes para proteger informações sensíveis.

12.11. Backup:

As cópias de segurança das informações, softwares e das imagens do sistema, são efetuadas e testadas regularmente. As seguintes diretrizes são adotadas:

a) registros completos e exatos das cópias de segurança.

b) a abrangência e a frequência da geração das cópias de segurança refletem os requisitos de negócio da Unimed Ituiutaba, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da Unimed Ituiutaba.

c) os backups são regularmente testados para garantir que eles são confiáveis no caso do uso emergencial;

e) Em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de criptografia.

12.12. Criptografia e Gerenciamento de Chaves:

O uso de criptografia na Unimed Ituiutaba deve ser atrelado às seguintes diretrizes:

a) a abordagem do gerenciamento de chaves, incluindo métodos para lidar com a proteção das chaves criptográficas e a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas;

b) O impacto do uso de informações cifradas em controles que dependem da inspeção de conteúdos, antes de cifrar uma informação deve-se passar por um processo de detecção de códigos maliciosos.

Na Unimed Ituiutaba os controles criptográficos podem ser usados para alcançar diferentes objetivos de segurança, como por exemplo:

a) confidencialidade: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas;

b) integridade/autenticidade: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para verificar a autenticidade ou integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;

c) não-repúdio: usando técnicas de criptografia para obter evidência da ocorrência ou não ocorrência de um evento ou ação, implicando no uso de certificados digitais preferencialmente no padrão ICP/Brasil.

d) autenticação: usando técnicas criptográficas para autenticar usuários e outros sistemas que requeiram acesso para transações com usuários de sistemas, entidades e recursos.

12.13. Gestão de Vulnerabilidades Técnicas:

As informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, são obtidas em tempo hábil, com a exposição da Unimed Ituiutaba a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados por meio de varredura de vulnerabilidades automatizadas.

12.14. Gestão de configuração:

A gestão de configuração abrange o ciclo completo de vida das configurações de hardware, software, serviços e redes, incluindo aspectos de segurança. O processo deve garantir que todas as configurações sejam consistentes, seguras e alinhadas aos objetivos da Unimed Ituiutaba. As etapas principais incluem:

12.14.1. Estabelecimento de Configurações

- **Definição de Padrões:**
  - Criar padrões de configuração para hardware, software, serviços e redes, baseados em boas práticas do setor e nos requisitos específicos da Unimed Ituiutaba.
  - Garantir que as configurações de segurança, como controle de acesso, criptografia e restrições de rede, estejam integradas aos padrões.

- **Inventário de Ativos:**
  - Manter um inventário atualizado de todos os ativos de TI, incluindo suas configurações associadas.
- **Classificação e Priorização:**
  - Classificar os ativos e configurações com base em sua criticidade para as operações da Unimed Ituiutaba.

12.14.2. Documentação

- **Registro Detalhado:**
  - Documentar todas as configurações de hardware, software, serviços e redes, incluindo versões, parâmetros e alterações.
- **Controle de Versões:**
  - Utilizar sistemas de controle de versões para gerenciar alterações e garantir que versões anteriores possam ser restauradas, se necessário.
- **Políticas e Procedimentos:**
  - Definir políticas claras para a gestão de configuração, especificando como as alterações devem ser solicitadas, aprovadas e implementadas.

12.14.3. Implementação

- **Automação de Configuração:**
  - Utilizar ferramentas de automação (como Ansible, Puppet ou Chef) para aplicar configurações de forma consistente e reduzir erros manuais.
- **Testes e Validações:**

- Realizar testes em ambientes controlados antes de implementar configurações em produção, garantindo que atendam aos requisitos funcionais e de segurança.

- **Controle de Alterações:**
  - Implementar um processo formal de controle de mudanças, exigindo aprovação antes da aplicação de alterações em configurações críticas.

12.14.4. Monitoramento

- **Monitoramento Contínuo:**
  - Configurar ferramentas de monitoramento para verificar a conformidade das configurações em tempo real, identificando desvios ou alterações não autorizadas.
- **Alertas e Logs:**
  - Configurar alertas para alterações não autorizadas ou falhas em configurações críticas.
  - Registrar logs detalhados de todas as alterações realizadas, com informações sobre quem as realizou, quando e por quê.

12.14.5. Análise Crítica

- **Revisões Regulares:**
  - Realizar auditorias periódicas para analisar a adequação e a conformidade das configurações com as políticas de segurança e os requisitos organizacionais.
- **Análise de Impacto:**
  - Avaliar o impacto de alterações propostas nas configurações antes de implementá-las, garantindo que não comprometam a segurança ou a operação.

- **Melhoria Contínua:**
  - Identificar e corrigir configurações inadequadas ou desatualizadas como parte de um ciclo contínuo de melhorias.

12.14.6. Configurações de Segurança

- **Configurações Padrão Seguras:**
  - Remover ou desativar serviços e funcionalidades desnecessárias para reduzir a superfície de ataque.
  - Estabelecer configurações seguras para sistemas operacionais, bancos de dados e redes.
- **Gerenciamento de Vulnerabilidades:**
  - Realizar verificações regulares para identificar e corrigir vulnerabilidades nas configurações.
- **Segurança de Configuração:**
  - Proteger arquivos de configuração contra acessos não autorizados, utilizando criptografia e controles de acesso.

12.14.7. Benefícios da Gestão de Configuração

- **Consistência Operacional:**
  - Assegurar que todas as configurações estejam alinhadas com os padrões organizacionais, minimizando falhas e inconsistências.
- **Melhoria na Segurança:**
  - Reduzir riscos associados a configurações mal feitas ou desatualizadas, fortalecendo a proteção contra ataques e acessos não autorizados.
- **Conformidade Regulatória:**

- Garantir que as configurações atendam às normas e regulamentações aplicáveis, como ISO/IEC 27001, LGPD e outras.

12.15. Exclusão de informações:

As informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas de forma segura e permanente quando não forem mais necessárias, para garantir a proteção da confidencialidade, integridade e privacidade, bem como o cumprimento de regulamentos legais e políticas internas. A seguir estão as diretrizes para esse processo:

12.15.1. Identificação das Informações para Exclusão

- **Revisão de Necessidade:**
  - Identificar informações que não são mais necessárias para operações, conformidade legal ou requisitos de retenção.
- **Classificação:**
  - Classificar os dados a serem excluídos com base em sua sensibilidade (ex.: confidencial, restrito ou público) para determinar o método de exclusão adequado.
- **Aprovação Formal:**
  - Obter aprovação do responsável pela informação antes de iniciar o processo de exclusão.

12.15.2. Métodos de Exclusão

- **Exclusão Lógica (Dados Recuperáveis):**

- Para informações que não requerem remoção permanente, utilizar a exclusão lógica, como a exclusão de arquivos em sistemas operacionais ou bases de dados.

- **Sobrescrita de Dados (Dados Irrecuperáveis):**
  - Utilizar ferramentas de sobrescrita para substituir dados existentes com padrões aleatórios ou zeros, garantindo que não possam ser recuperados.
- **Desmagnetização (Degaussing):**
  - Aplicar desmagnetização para apagar de forma permanente dados em mídias magnéticas, como discos rígidos ou fitas.
- **Destruição Física:**
  - Para mídias que não serão reutilizadas, realizar a destruição física por meio de métodos como trituração, pulverização ou queima, garantindo que os dados sejam completamente irrecuperáveis.

12.15.3. Ferramentas e Tecnologias

- **Ferramentas Certificadas:**
  - Utilizar softwares e equipamentos certificados por padrões internacionais, como NIST 800-88 ou ISO/IEC 27040, para exclusão de dados.
- **Automação:**
  - Adotar ferramentas automatizadas para gerenciar a exclusão em larga escala e minimizar erros humanos.

12.15.4. Documentação e Registro

- **Registro do Processo:**
  - Documentar todas as exclusões realizadas, incluindo:

- Data e hora da exclusão.
- Método utilizado.
- Dispositivo ou mídia de armazenamento.
- Nome do responsável pela exclusão.
- Emitir certificados de destruição, quando necessário, especialmente para dispositivos sensíveis ou regulamentados.

- **Auditoria:**
  - Realizar auditorias periódicas para verificar a conformidade dos processos de exclusão com as políticas da Unimed Ituiutaba.

12.15.5. Conformidade e Políticas

- **Alinhamento às Políticas Internas:**
  - Assegurar que a exclusão de informações siga as políticas internas de segurança da informação e retenção de dados.
- **Cumprimento de Regulamentações:**
  - Garantir conformidade com regulamentações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD), GDPR ou normas setoriais específicas.
- **Retenção Legal:**
  - Antes de excluir informações, verificar se há exigências legais ou contratuais que demandem retenção adicional.

12.15.6. Sensibilização e Treinamento

- **Conscientização dos Funcionários:**
  - Capacitar os colaboradores sobre a importância da exclusão segura de informações e os métodos adequados para cada tipo de dado.

- **Responsabilidade Individual:**
  - Atribuir responsabilidades claras para o gerenciamento e exclusão de informações.

12.15.7. Processos de Exclusão em Diferentes Cenários

- **Dispositivos de Uso Interno:**
  - Aplicar métodos seguros, como sobrescrita ou desmagnetização, antes de reutilizar ou descartar dispositivos.
- **Mídias Externas ou Terceirizadas:**
  - Contratar empresas especializadas para a exclusão ou destruição de informações, exigindo certificados de conformidade.
- **Sistemas em Nuvem:**
  - Verificar que provedores de serviços em nuvem oferecem exclusão definitiva de informações, conforme contratos ou SLAs.
- **Informações Temporárias:**
  - Configurar sistemas para exclusão automática de informações temporárias ou desnecessárias, como arquivos em cache ou logs.

12.15.8. Benefícios da Exclusão Segura

- **Mitigação de Riscos:**
  - Reduzir o risco de vazamentos de dados e acessos não autorizados a informações sensíveis.
- **Eficiência Operacional:**
  - Liberar espaço de armazenamento e otimizar recursos tecnológicos.
- **Conformidade Legal:**

- Evitar penalidades relacionadas à retenção indevida ou ao vazamento de dados pessoais ou confidenciais.

12.16. Mascaramento de dados:

O mascaramento de dados é uma técnica essencial para proteger informações sensíveis, garantindo que elas sejam acessíveis apenas em um formato que não comprometa sua confidencialidade. O processo deve ser conduzido em conformidade com a política de controle de acesso da Unimed Ituiutaba, requisitos de negócios e legislação aplicável, como a LGPD (Lei Geral de Proteção de Dados) e GDPR (Regulamento Geral de Proteção de Dados). A seguir estão as diretrizes para o uso do mascaramento de dados:

12.16.1. Objetivos do Mascaramento de Dados

- **Proteção de Informações Sensíveis:**
  - Garantir a confidencialidade de dados pessoais, financeiros, médicos ou confidenciais.
- **Conformidade Legal:**
  - Atender aos requisitos regulatórios de proteção de dados.
- **Minimização de Riscos:**
  - Reduzir o impacto de vazamentos de dados ao impedir o acesso a informações reais por pessoas não autorizadas.

12.16.2. Aplicações do Mascaramento de Dados

- **Ambientes de Desenvolvimento e Teste:**
  - Utilizar dados mascarados em ambientes não produtivos para proteger informações reais, mantendo sua utilidade para testes.
- **Exposição a Terceiros:**

- Implementar o mascaramento ao compartilhar informações com fornecedores, parceiros ou auditores externos, garantindo que os dados sensíveis permaneçam inacessíveis.

- **Visualização Limitada:**
  - Aplicar mascaramento para limitar a visualização de informações sensíveis em sistemas acessados por colaboradores que não possuem autorização para visualizar os dados completos.

12.16.3. Métodos de Mascaramento

- **Substituição:**
  - Substituir valores reais por valores fictícios, como substituir nomes de clientes por "Cliente X".
- **Truncamento:**
  - Mostrar apenas uma parte do dado, como os últimos quatro dígitos de um CPF ou cartão de crédito.
- **Anonimização Parcial:**
  - Alterar dados para torná-los irreconhecíveis, mantendo o formato original para uso em análises.
- **Baralhamento de Dados:**
  - Misturar valores reais entre registros para preservar a estrutura, mas ocultar os dados originais.
- **Encriptação Temporária:**
  - Utilizar criptografia para mascarar dados, garantindo sua proteção em sistemas onde a descriptografia não é necessária.

12.16.4. Políticas de Uso

- **Controle de Acesso:**
  - Garantir que apenas usuários com permissões específicas possam acessar dados mascarados ou originais, conforme a política de controle de acesso da Unimed Ituiutaba.
- **Contextos de Aplicação:**
  - Definir cenários claros em que o mascaramento de dados deve ser aplicado, como geração de relatórios, exibição em interfaces de usuário ou compartilhamento externo.
- **Automatização do Mascaramento:**
  - Implementar soluções automatizadas para aplicar mascaramento em tempo real nos sistemas, garantindo consistência e minimizando erros humanos.

12.16.5. Requisitos de Negócios e Conformidade

- **Alinhamento com a Legislação Aplicável:**
  - Garantir que o mascaramento atenda às exigências legais de proteção de dados, como a anonimização para evitar a identificação de indivíduos (conforme artigos da LGPD e GDPR).
- **Requisitos Específicos do Negócio:**
  - Considerar os requisitos do setor para determinar quais dados devem ser mascarados e em quais contextos (ex.: setores de saúde, financeiro ou jurídico podem ter exigências adicionais).

12.16.6. Monitoramento e Auditoria

- **Auditoria de Aplicação:**

- Monitorar regularmente a aplicação do mascaramento para garantir que está sendo realizado conforme as políticas internas e requisitos legais.

- **Relatórios de Conformidade:**
  - Gerar relatórios periódicos sobre o uso do mascaramento e sobre a proteção de informações sensíveis para avaliação por equipes de governança.

12.16.7. Benefícios do Mascaramento

- **Segurança Aprimorada:**
  - Evita o acesso indevido a informações sensíveis, mesmo em caso de invasão ou vazamento.
- **Manutenção de Operações Seguras:**
  - Permite o uso de dados protegidos em ambientes de teste, desenvolvimento e análise, sem comprometer a segurança.
- **Atendimento a Normas e Regulamentos:**
  - Facilita a conformidade com legislações de proteção de dados e auditorias de segurança.

12.16.8. Conscientização e Treinamento

- **Capacitação de Usuários**:
  - Treinar colaboradores sobre a importância do mascaramento de dados e como utilizá-lo corretamente.
- **Sensibilização sobre Riscos**:
  - Garantir que os usuários entendam os riscos de acesso não autorizado e a necessidade de proteger dados sensíveis.

12.17. Prevenção de vazamento de dados:

As medidas de prevenção de vazamento de dados devem ser implementadas em sistemas, redes e dispositivos que tratam, armazenam ou transmitem informações sensíveis, com o objetivo de proteger a confidencialidade e integridade dessas informações, reduzir riscos de vazamentos acidentais ou maliciosos e garantir a conformidade com as legislações aplicáveis. As diretrizes incluem:

12.17.1. Identificação e Classificação de Dados

- **Mapeamento de Dados Sensíveis:**
  - Identificar e catalogar informações sensíveis (ex.: dados pessoais, financeiros, médicos ou confidenciais) em todos os sistemas e dispositivos.
- **Classificação de Informações:**
  - Aplicar políticas de classificação de dados, definindo níveis como "Confidencial", "Restrito" e "Público".
- **Etiquetagem de Dados:**
  - Etiquetar informações sensíveis para facilitar a aplicação de medidas de proteção.

12.17.2. Controles de Acesso

Princípio do Menor Privilégio:

Restringir o acesso às informações sensíveis apenas aos usuários que necessitam delas para suas funções.

Autenticação Segura:

Implementar autenticação multifator (MFA) para acesso a sistemas que contenham informações sensíveis.

Monitoramento de Sessões:

Configurar limites de tempo para sessões e bloquear acessos após períodos de inatividade.

12.17.3. Proteção em Trânsito e em Repouso

- **Criptografia de Dados:**
  - Utilizar criptografia para proteger informações sensíveis durante o armazenamento e transmissão.
  - Implementar protocolos seguros (ex.: TLS/SSL) para dados transmitidos por redes públicas ou internas.
- **Isolamento de Dados Críticos:**
  - Manter informações críticas em servidores ou bancos de dados isolados da rede principal.

12.17.4. Soluções de Prevenção de Vazamento de Dados (DLP)

- **Implementação de Sistemas DLP:**
  - Adotar ferramentas de DLP que monitoram e controlam o fluxo de dados em endpoints, redes e dispositivos de armazenamento.
- **Definição de Regras e Políticas:**
  - Configurar políticas no DLP para bloquear ou alertar sobre tentativas de envio de informações sensíveis para fora da Unimed Ituiutaba.
- **Monitoramento de Padrões:**
  - Detectar padrões específicos de dados sensíveis, como números de CPF, cartões de crédito ou registros médicos.

12.17.5. Proteção em Redes

- **Firewalls e IDS/IPS:**
  - Configurar firewalls e sistemas de detecção/prevenção de intrusões (IDS/IPS) para identificar e bloquear tráfego suspeito que possa indicar vazamento de dados.
- **Segmentação de Redes:**
  - Segmentar a rede para isolar sistemas críticos de redes acessadas por usuários e dispositivos menos confiáveis.
- **Filtragem de Conteúdo:**
  - Implementar filtros de conteúdo para impedir o envio de informações confidenciais por e-mail, uploads ou serviços de nuvem não autorizados.

12.17.6. Segurança de Dispositivos

- **Proteção de Endpoints:**
  - Instalar soluções de segurança em endpoints (como laptops e dispositivos móveis) para prevenir vazamentos acidentais ou maliciosos.
- **Bloqueio de Dispositivos de Armazenamento:**
  - Restringir o uso de dispositivos USB e mídias removíveis em sistemas que tratam dados sensíveis.
- **Rastreamento e Controle Remoto:**
  - Configurar dispositivos móveis com ferramentas de rastreamento e capacidade de exclusão remota de dados em caso de perda ou roubo.

12.17.7. Monitoramento e Auditoria

- **Logs de Atividades:**
  - Registrar todas as ações realizadas em sistemas que contenham informações sensíveis, incluindo acessos, modificações e transferências de dados.
- **Auditorias Regulares:**
  - Realizar auditorias periódicas para verificar a conformidade com políticas de segurança e identificar possíveis vulnerabilidades.
- **Alertas em Tempo Real:**
  - Configurar sistemas para emitir alertas em caso de atividades anômalas, como transferências de dados não autorizadas.

12.17.8. Conscientização e Treinamento

- **Treinamento de Funcionários:**
  - Capacitar os colaboradores sobre as políticas de prevenção de vazamento de dados, boas práticas de segurança e conscientização sobre phishing e engenharia social.
- **Cultura de Segurança:**
  - Promover uma cultura organizacional que valorize a proteção de informações sensíveis e incentive a denúncia de comportamentos suspeitos.

12.17.9. Resposta a Incidentes

- **Plano de Resposta a Incidentes:**
  - Estabelecer um plano claro para lidar com vazamentos de dados, com etapas para contenção, investigação, comunicação e mitigação.
- **Notificação de Vazamentos:**

- Garantir a conformidade com requisitos legais para notificação de vazamentos às autoridades competentes e aos titulares dos dados.

12.17.10. Conformidade Legal e Regulamentar

- **Legislação Aplicável:**
  - Assegurar que as medidas de prevenção de vazamento estejam alinhadas às legislações, como a LGPD e a GDPR, e às normas internas e setoriais.
- **Políticas Internas:**
  - Integrar as políticas de prevenção de vazamento de dados às políticas de segurança da informação e controle de acesso da Unimed Ituiutaba.

12.18. Redundância dos recursos de tratamento de informações:

A implementação de recursos redundantes para o tratamento de informações é essencial para garantir a **disponibilidade** dos sistemas e dados, mesmo em situações de falha ou interrupção. A seguir estão as diretrizes para o estabelecimento e manutenção de redundância suficiente para atender aos requisitos de disponibilidade:

12.18.1. Identificação dos Requisitos de Disponibilidade

- **Análise de Impacto no Negócio (BIA):**
  - Realizar uma análise de impacto para identificar os sistemas e serviços críticos que requerem alta disponibilidade.
- **Definição de Níveis de Serviço:**
  - Estabelecer requisitos de disponibilidade baseados nos Acordos de Nível de Serviço (SLAs) e nas necessidades do negócio.
- **Priorização de Recursos:**

- Priorizar a implementação de redundância para sistemas que suportam operações críticas e sensíveis.

12.18.2. Implementação de Redundância

- **Hardware**
  - **Servidores Redundantes:**
    - Implantar servidores redundantes em configuração de cluster para garantir continuidade em caso de falha de um servidor principal.
  - **Armazenamento Redundante:**
    - Utilizar sistemas de armazenamento redundante, como RAID (Redundant Array of Independent Disks), para proteger os dados contra falhas de disco.
  - **Componentes Duplicados:**
    - Configurar redundância de componentes internos, como fontes de alimentação, placas de rede e ventiladores.
- **Software**
  - **Balanceamento de Carga:**
    - Implementar balanceadores de carga para distribuir o tráfego entre servidores redundantes, evitando sobrecarga e garantindo a continuidade do serviço.
  - **Sistemas de Failover:**
    - Configurar failover automático para que, em caso de falha de um sistema, outro assuma imediatamente as operações sem interrupções perceptíveis.

- Redes
- Conexões de Rede Redundantes:
- Configurar múltiplos links de conexão à internet com provedores diferentes para garantir conectividade ininterrupta.
- Equipamentos de Rede Redundantes:
- Utilizar switches, roteadores e firewalls redundantes para minimizar o impacto de falhas em dispositivos de rede.
- Roteamento Dinâmico:
- Implementar protocolos de roteamento dinâmico, como BGP (Border Gateway Protocol), para redirecionar automaticamente o tráfego em caso de falha de uma rota.
- Locais
- Data Centers Redundantes:
- Implantar data centers secundários em locais geograficamente distintos, configurados como sites de recuperação (ativo-ativo, ativo-passivo ou cold site).
- Sistemas de Energia Redundantes:
- Garantir fontes de energia redundantes, como sistemas de energia ininterrupta (UPS) e geradores de backup, para suportar falhas no fornecimento elétrico.

12.18.3. Monitoramento e Gerenciamento

- **Soluções de Monitoramento Contínuo:**

Utilizar ferramentas de monitoramento para rastrear a integridade dos recursos redundantes e identificar falhas em tempo real.

- **Alertas Proativos:**

Configurar alertas automáticos para notificar equipes de suporte sobre falhas em sistemas redundantes.

- **Testes de Redundância:**

Realizar testes periódicos para validar a funcionalidade de sistemas redundantes, garantindo sua capacidade de operar em situações de falha.

12.18.4. Planos de Recuperação e Continuidade

- **Planejamento de Recuperação:**
  - Incorporar sistemas redundantes em um plano de recuperação de desastres (DRP) que assegure a continuidade das operações críticas.
- **Documentação de Configurações:**
  - Manter registros detalhados de todas as configurações de redundância para facilitar diagnósticos e recuperação em caso de falhas.

12.18.5. Benefícios da Redundância

- **Minimização de Interrupções:**
  - Reduzir o impacto de falhas de hardware, software ou rede nas operações diárias.
- **Garantia de Alta Disponibilidade:**
  - Manter os serviços disponíveis mesmo em situações de falha parcial de infraestrutura.
- **Escalabilidade:**
  - Permitir o crescimento contínuo das operações sem comprometer a confiabilidade dos sistemas.

12.18.6. Conformidade com Políticas e Normas

- **Adesão a Normas:**
  - Garantir que a configuração de redundância atenda a padrões reconhecidos, como ISO/IEC 27001, e regulamentos setoriais aplicáveis.
- **Políticas Internas:**
  - Alinhar as estratégias de redundância às políticas internas de segurança e continuidade do negócio.

12.18.7. Treinamento e Conscientização

- **Capacitação de Equipes:**
  - Treinar equipes de TI para gerenciar e manter sistemas redundantes, garantindo respostas rápidas e eficientes em casos de falha.
- **Simulações de Falhas:**
  - Realizar simulações regulares para treinar as equipes na recuperação de sistemas redundantes e validar sua eficácia.

12.19. LOG:

Os logs são registros críticos para o monitoramento, auditoria e identificação de eventos relevantes em sistemas, redes e dispositivos da Unimed Ituiutaba. Para garantir sua eficácia, o processo de **produção, armazenamento, proteção e análise de logs** deve ser realizado de maneira sistemática, atendendo às necessidades operacionais e requisitos legais. As diretrizes são descritas abaixo:

12.19.1. Produção de Logs

- **Identificação dos Eventos a Serem Registrados:**
  - Determinar quais atividades e eventos devem ser registrados, como:
  - Autenticação e acessos (sucessos e falhas).
  - Alterações em sistemas, configurações ou dados sensíveis.
  - Exceções, erros e falhas em aplicações ou dispositivos.
  - Acessos a informações confidenciais e dados sensíveis.
- **Granularidade e Detalhes:**
  - Garantir que os logs contenham informações essenciais, incluindo:
  - Data e hora do evento (com base em um servidor de tempo confiável).
  - Identidade do usuário ou sistema que gerou o evento.
  - Endereço IP ou dispositivo associado.
  - Descrição clara da atividade ou falha.
- **Padronização:**
  - Utilizar formatos padronizados (ex.: JSON, syslog) para facilitar a interpretação e análise dos registros.

12.19.2. Armazenamento de Logs

- **Centralização dos Logs:**
  - Implementar um sistema centralizado para coleta e armazenamento de logs, como SIEM (Security Information and Event Management), para facilitar a análise e correlação.
- **Capacidade e Retenção:**
  - Estabelecer políticas de retenção baseadas em requisitos legais e operacionais:

- Logs operacionais: reter por períodos mais curtos (ex.: 3 a 6 meses).
- Logs de segurança: reter por períodos mais longos (ex.: 1 a 5 anos), conforme regulamentações aplicáveis.

- **Segurança de Armazenamento:**
  - Proteger os logs contra alterações ou exclusões não autorizadas, utilizando:
  - Assinatura digital para garantir a integridade.
  - Controles de acesso restrito ao sistema de armazenamento de logs.
  - Backups regulares de registros importantes.

12.19.3. Proteção de Logs

- **Controle de Acesso:**
  - Restringir o acesso aos logs apenas a usuários autorizados, como administradores de sistemas ou analistas de segurança.
- **Criptografia:**
  - Utilizar criptografia para proteger logs armazenados e em trânsito, garantindo que informações sensíveis permaneçam confidenciais.
- **Prevenção de Perda:**
  - Implementar redundância no armazenamento para evitar perda de dados em caso de falhas.
- **Monitoramento de Integridade:**
  - Configurar ferramentas para detectar alterações não autorizadas nos registros de logs.

12.19.4. Análise de Logs

- **Monitoramento Contínuo:**
  - Utilizar ferramentas automatizadas para monitorar e analisar logs em tempo real, detectando atividades suspeitas, como:
    - Tentativas de acesso não autorizado.
    - Alterações inesperadas em sistemas ou dados.
    - Comportamentos fora do padrão.
- **Correlações e Alertas:**
  - Configurar sistemas de SIEM para correlacionar eventos entre diferentes logs, gerando alertas automáticos para incidentes críticos.
- **Relatórios Periódicos:**
  - Produzir relatórios regulares para equipes de TI e gestores, destacando eventos relevantes e tendências detectadas.
- **Auditorias Regulares:**
  - Realizar auditorias manuais ou automatizadas nos registros para validar conformidade com políticas internas e regulatórias.

12.19.5. Requisitos de Conformidade e Legislação

- **Alinhamento com Regulamentações:**
  - Garantir que a produção e armazenamento de logs atendam às legislações e normas aplicáveis, como:
    - LGPD (Lei Geral de Proteção de Dados): Manter logs relacionados ao tratamento de dados pessoais com segurança.
    - ISO/IEC 27001: Implementar controles de auditoria para registro e monitoramento de atividades.

- Requisitos setoriais específicos, como PCI-DSS (para transações financeiras).
- Políticas de Retenção e Exclusão:
- Seguir as políticas internas de retenção de logs, garantindo que registros antigos sejam excluídos de forma segura quando não forem mais necessários.

12.19.6. Benefícios dos Logs

- **Monitoramento de Segurança:**
  - Identificar e responder rapidamente a incidentes de segurança.
- **Auditoria e Conformidade:**
  - Fornecer evidências para auditorias internas ou externas.
- **Análise Forense:**
  - Facilitar investigações detalhadas em casos de falhas ou violações.
- **Otimização Operacional:**
  - Detectar gargalos e problemas em sistemas para otimizar desempenho.

12.19.7. Treinamento e Conscientização

- **Capacitação das Equipes:**
  - Treinar administradores e analistas para configurar, interpretar e gerenciar logs de maneira eficaz.
- **Conscientização sobre Importância dos Logs:**
  - Garantir que os colaboradores entendam o papel crítico dos logs na segurança e continuidade das operações.

12.20. Atividades de monitoramento:

Elaboração	Análise crítica	Classificação da Informação	Aprovação
Brunno Eduardo Vilela Batista	Murilo Morais De Oliveira	Pública	Dra. Rosane Abramo Dr. Raphael Gonçalves de Oliveira
Data: 12/01/2026	Data: 16/01/2026		

O monitoramento de redes, sistemas e aplicações é essencial para identificar comportamentos anômalos, avaliar possíveis incidentes de segurança e tomar ações apropriadas para proteger os ativos de informação da Unimed Ituiutaba. O processo deve ser contínuo, proativo e alinhado às políticas de segurança da informação. As diretrizes a seguir descrevem como essas atividades devem ser conduzidas:

12.20.1. Planejamento do Monitoramento

- **Identificação de Ativos Críticos:**
  - Mapear os ativos de informação, sistemas e aplicações que requerem monitoramento constante com base em sua criticidade e sensibilidade.
- **Definição de Escopo:**
  - Determinar o escopo do monitoramento, abrangendo redes, servidores, dispositivos de armazenamento, endpoints, aplicações e tráfego interno e externo.
- **Estabelecimento de Políticas:**
  - Criar políticas de monitoramento que definam responsabilidades, frequência, métodos e ações esperadas diante de comportamentos anômalos.

12.20.2. Ferramentas e Tecnologias

- **Soluções de Monitoramento:**
  - Implantar ferramentas especializadas, como:
  - SIEM (Security Information and Event Management): Para correlação e análise de eventos de segurança.
  - IDS/IPS (Sistemas de Detecção e Prevenção de Intrusões): Para monitorar tráfego de rede em tempo real e bloquear ataques.

- EDR (Endpoint Detection and Response): Para monitorar dispositivos finais contra ameaças e comportamentos suspeitos.

- **Monitoramento de Aplicações:**
  - Utilizar soluções de APM (Application Performance Monitoring) para detectar anomalias em aplicativos críticos.
- **Análise de Tráfego de Rede:**
  - Monitorar o tráfego de rede com ferramentas que detectem padrões anômalos, como picos de uso, acessos não autorizados ou transferências de dados incomuns.

12.20.3. Identificação de Comportamentos Anômalos

- **Parâmetros e Indicadores:**
  - Definir indicadores de comportamento normal (baseline) para redes, sistemas e aplicações, identificando:
  - Horários típicos de atividade.
  - Quantidade usual de tráfego ou transações.
  - Padrões de acesso de usuários.
  - Detecção de Ameaças:
- **Configurar as ferramentas para alertar sobre:**
  - Tentativas de acesso não autorizado.
  - Padrões de login incomuns (ex.: múltiplas falhas de login).
  - Transferências de dados em volume incomum.
  - Uso de contas privilegiadas fora do padrão.
  - Alterações não autorizadas em configurações ou aplicações.
- **Análise de Logs:**

- Examinar regularmente logs de sistemas, redes e aplicações para identificar eventos suspeitos.

12.20.4. Ações Apropriadas Diante de Incidentes

- **Respostas Automatizadas:**
  - Configurar ferramentas para realizar ações imediatas diante de certos eventos, como:
  - Bloquear IPs maliciosos detectados por IDS/IPS.
  - Isolar endpoints suspeitos com EDR.
  - Desativar contas comprometidas automaticamente após detecção de acessos não autorizados.
- **Escalonamento e Notificação:**
  - Estabelecer procedimentos para escalonar incidentes com base em sua gravidade.
  - Notificar as equipes responsáveis e gestores de segurança assim que um comportamento anômalo for identificado.
- **Investigação de Incidentes:**
  - Realizar análises forenses em logs e sistemas para determinar a origem e o impacto do comportamento anômalo.
  - Identificar vulnerabilidades exploradas e ações realizadas por possíveis invasores.
- **Documentação e Relatórios:**
  - Registrar todos os incidentes detectados, as ações tomadas e os resultados obtidos, para aprendizado e melhoria contínua.

12.20.5. Monitoramento Contínuo e Análises Periódicas

- **Revisão de Configurações:**
  - Verificar regularmente as configurações das ferramentas de monitoramento para garantir sua eficácia e alinhamento às ameaças mais recentes.
- **Auditorias:**
  - Realizar auditorias periódicas dos eventos monitorados para identificar padrões e melhorar os processos.
- **Análises Proativas:**
  - Conduzir análises de dados históricos para prever possíveis ameaças e ajustar estratégias de monitoramento.

12.20.6. Conscientização e Treinamento

- **Capacitação de Equipes:**
  - Treinar as equipes de TI e segurança para interpretar os resultados das ferramentas de monitoramento e agir de forma eficiente diante de alertas.
- **Sensibilização de Colaboradores:**
  - Conscientizar os usuários sobre a importância do monitoramento e sobre como reportar atividades suspeitas.

12.20.7. Conformidade com Normas e Regulamentações

- **Adequação às Políticas Internas:**
  - Garantir que as atividades de monitoramento estejam alinhadas às políticas de segurança da Unimed Ituiutaba.
- **Legislação e Regulamentações:**

- Assegurar que o monitoramento esteja em conformidade com leis e normas, como a LGPD, para respeitar a privacidade dos usuários.

12.20.8. Benefícios do Monitoramento

- **Identificação de Riscos em Tempo Real:**
  - Detectar rapidamente atividades anômalas e incidentes de segurança.
- **Prevenção de Incidentes:**
  - Mitigar ameaças antes que causem impacto significativo nas operações.
- **Melhoria Contínua:**
  - Coletar dados para aprimorar estratégias de segurança e fortalecer a resiliência da Unimed Ituiutaba.

12.21. Sincronização do relógio:

A sincronização precisa dos relógios dos sistemas de tratamento de informações é essencial para garantir a consistência nos registros de logs, a integridade dos dados e a conformidade com os padrões e regulamentações. A seguir estão as diretrizes para implementar a sincronização dos relógios com fontes de tempo aprovadas:

12.21.1. Fontes de Tempo Aprovadas

- **Servidores NTP (Network Time Protocol):**
  - Configurar todos os sistemas para sincronizar com servidores NTP confiáveis e seguros, preferencialmente:
  - Servidores internos da Unimed Ituiutaba configurados para sincronizar com fontes externas confiáveis.

- Fontes públicas aprovadas, como servidores do NIST (National Institute of Standards and Technology) ou pool.ntp.org.

- **Hierarquia de Sincronização:**
  - Designar servidores de tempo primários (servidores de nível superior) para sincronizar diretamente com as fontes externas e distribuir o tempo para os demais sistemas internos.

12.21.2. Configuração dos Sistemas

- **Padrões de Configuração:**
  - Configurar a sincronização de tempo em todos os sistemas, incluindo:
  - Servidores.
  - Estações de trabalho.
  - Dispositivos de rede (switches, roteadores e firewalls).
  - Aplicações críticas que dependam de marcações de tempo precisas.
- **Protocolo Seguro:**
  - Utilizar versões seguras do NTP (ex.: NTPv4) para evitar manipulação de tempo por ataques de spoofing.
- **Intervalos de Sincronização:**
  - Definir intervalos regulares para a sincronização automática (ex.: a cada 10 minutos ou conforme necessário para a precisão do sistema).

12.21.3. Monitoramento e Manutenção

- **Monitoramento Contínuo:**
  - Utilizar ferramentas para monitorar a sincronização de tempo em sistemas críticos e identificar possíveis desvios.

- **Alertas para Desvios:**
  - Configurar alertas automáticos para detectar e corrigir desvios significativos de tempo entre os sistemas.
- **Auditorias Periódicas:**
  - Realizar auditorias regulares para garantir que todos os sistemas estejam sincronizados com as fontes de tempo aprovadas.

12.21.4. Benefícios da Sincronização

- **Consistência em Registros de Logs:**
  - Garantir que todos os logs de eventos e atividades sejam registrados com marcações de tempo precisas, permitindo a análise e a correlação eficaz de incidentes.
- **Conformidade com Padrões:**
  - Atender aos requisitos de normas de segurança e auditoria, como ISO/IEC 27001 e LGPD.
- **Integridade Operacional:**
  - Evitar conflitos em aplicações ou sistemas que dependam de tempo sincronizado para execução correta, como sistemas financeiros ou transacionais.

12.21.5. Conformidade com Políticas e Regulamentações

- **Políticas Internas:**
  - Implementar diretrizes internas que obriguem todos os sistemas a estarem sincronizados com fontes de tempo aprovadas.
- **Requisitos Legais:**

- Garantir que a marcação de tempo em registros e documentos eletrônicos esteja em conformidade com requisitos legais e normativos.

12.21.6. Treinamento e Responsabilidades

- **Equipes de TI:**
  - Treinar equipes responsáveis para configurar, monitorar e manter os sistemas de sincronização de tempo.
- **Responsabilidade Centralizada:**
  - Designar responsáveis pelo gerenciamento dos servidores NTP internos e pela coordenação com fontes externas aprovadas.

12.21.7. Plano de Contingência

- **Servidores de Tempo Redundantes:**
  - Configurar servidores de tempo secundários para garantir continuidade em caso de falha do servidor primário.
- **Alternativas de Sincronização:**
  - Garantir que sistemas críticos tenham métodos alternativos para verificar a precisão do tempo em cenários de indisponibilidade das fontes primárias.

12.22. Uso de programas utilitários privilegiados:

O uso de programas utilitários privilegiados, que podem substituir controles de sistema e aplicações, deve ser rigorosamente restrito e controlado para minimizar os riscos associados ao acesso não autorizado ou uso indevido. A seguir estão as diretrizes para gerenciar e restringir esses programas de forma segura:

12.22.1. Identificação dos Programas Utilitários Privilegiados

- **Mapeamento de Utilitários:**
  - Identificar todos os programas utilitários com capacidades privilegiadas, como:
    - Ferramentas de gerenciamento de sistemas (ex.: ferramentas de administração de rede e servidores).
    - Softwares de configuração e manutenção.
    - Ferramentas para edição de registros, bancos de dados ou configurações críticas.
- **Classificação:**
  - Classificar esses utilitários com base em seu nível de impacto em caso de uso indevido ou comprometimento.

12.22.2. Restrições de Acesso

- **Princípio do Menor Privilégio:**
  - Garantir que apenas usuários com funções específicas tenham acesso a esses programas, limitado às suas responsabilidades.
- **Autenticação Forte:**
  - Exigir autenticação multifator (MFA) para todos os usuários que precisem utilizar utilitários privilegiados.
- **Controle Baseado em Funções (RBAC):**
  - Implementar controles baseados em funções, associando permissões específicas apenas a grupos de usuários autorizados.

12.22.3. Controle de Uso

- **Aprovação Prévia:**
  - Exigir aprovação formal antes da execução de programas utilitários privilegiados em ambientes críticos.
- **Sessões Limitadas:**
  - Restringir o tempo de uso de utilitários privilegiados, encerrando sessões automaticamente após períodos de inatividade.
- **Ambientes Isolados:**
  - Sempre que possível, utilizar programas utilitários em ambientes controlados ou isolados (ex.: máquinas virtuais ou sistemas de teste) para evitar impactos em produção.

12.22.4. Monitoramento e Registro

- **Registro de Atividades:**
  - Registrar todas as ações realizadas por programas utilitários privilegiados, incluindo:
    - Usuário que executou o utilitário.
    - Data, hora e duração do uso.
    - Comandos ou ações realizadas.
    - Garantir que esses registros sejam protegidos contra alterações não autorizadas.
- **Monitoramento Contínuo:**
  - Implementar ferramentas de monitoramento em tempo real para detectar o uso de utilitários privilegiados fora do padrão ou sem autorização.

- **Alertas Automáticos:**
  - Configurar alertas automáticos para notificações em caso de uso suspeito ou indevido desses programas.

12.22.5. Auditorias e Revisões

- **Auditorias Regulares:**
  - Realizar auditorias periódicas para revisar o uso de utilitários privilegiados, identificar padrões anômalos e verificar a conformidade com as políticas da Unimed Ituiutaba.
- **Revisão de Permissões:**
  - Revisar regularmente as permissões de acesso aos programas utilitários para garantir que estejam atualizadas e alinhadas às responsabilidades dos usuários.

12.22.6. Proteção contra Alterações e Uso Indevido

- **Restrição de Instalação:**
  - Impedir que usuários instalem ou executem programas utilitários privilegiados sem aprovação prévia.
- **Validação de Integridade:**
  - Utilizar assinaturas digitais ou verificações de hash para garantir que os programas utilitários não sejam alterados ou substituídos por versões maliciosas.

- **Desativação em Sistemas Não Críticos:**
  - Remover ou desativar programas utilitários em sistemas onde seu uso não seja necessário.

12.22.7. Treinamento e Conscientização

- **Capacitação de Usuários Autorizados:**
  - Treinar os usuários que utilizam programas utilitários privilegiados sobre seus riscos e responsabilidades.
- **Conscientização Geral:**
  - Sensibilizar todos os colaboradores sobre os riscos associados ao uso indevido de programas utilitários e como reportar atividades suspeitas.

12.22.8. Conformidade com Políticas e Regulamentações

- **Políticas Internas:**
  - Implementar e documentar políticas claras sobre o uso de programas utilitários privilegiados, definindo:
  - Quem pode acessá-los.
  - Em quais situações eles podem ser utilizados.
  - Procedimentos para solicitação e aprovação.
- **Atendimento às Normas:**
  - Garantir que os controles implementados estejam alinhados às regulamentações e normas de segurança, como ISO/IEC 27001 e requisitos de proteção de dados.

12.22.9. Resposta a Incidentes

- **Detecção e Contenção:**
  - Estabelecer processos claros para detectar e conter imediatamente qualquer uso indevido de programas utilitários privilegiados.
- **Investigação e Relatório:**
  - Investigar incidentes envolvendo esses programas, identificar falhas no processo e documentar lições aprendidas.
- **Correções e Melhorias:**
  - Atualizar políticas e controles após a análise de incidentes para mitigar riscos futuros.

12.23. Instalação de software em sistemas operacionais:

A instalação de software em sistemas operacionais deve ser gerenciada com procedimentos e medidas de segurança rigorosos para garantir a integridade do ambiente, evitar vulnerabilidades e manter a conformidade com as políticas da Unimed Ituiutaba. A seguir, são descritas as diretrizes para gerenciar com segurança esse processo:

12.23.1. Procedimentos para Instalação de Software

- **Autorização Prévia:**
  - Todo software a ser instalado deve passar por um processo de aprovação formal, com validação pela equipe de TI ou de segurança.
- **Softwares Permitidos:**
  - Manter uma lista de softwares aprovados e certificados pela Unimed Ituiutaba, limitando a instalação a esses programas.
  -

- **Política de Proibição:**
  - Proibir explicitamente a instalação de softwares não autorizados ou oriundos de fontes não confiáveis.

- **Registrar cada instalação, incluindo:**
  - Nome do software.
  - Versão.
  - Data de instalação.
  - Usuário responsável pela solicitação e pela execução.

12.23.2. Medidas de Segurança

- **Fontes Confiáveis:**
  - Garantir que os softwares sejam baixados apenas de repositórios oficiais ou de fornecedores confiáveis, verificando sua autenticidade.
- **Verificação de Integridade:**
  - Validar a integridade do software antes da instalação, utilizando assinaturas digitais, hashes ou verificações de checksum.
- **Aprovação e Teste Prévio:**
  - Testar softwares em ambientes controlados (sandbox ou laboratório) antes de instalá-los em sistemas de produção para avaliar riscos e compatibilidade.
- **Privilégios Mínimos:**
  - Restringir a capacidade de instalação de software apenas a usuários autorizados, como administradores de sistemas, utilizando o princípio do menor privilégio.

12.23.3. Automação e Controle

- **Gerenciamento Centralizado:**
  - Utilizar ferramentas de gerenciamento de software (ex.: SCCM, Intune ou Puppet) para controlar e monitorar a instalação de aplicativos em larga escala.
- **Catálogo de Software:**
  - Implementar um catálogo centralizado de aplicativos aprovados para facilitar o acesso dos usuários a softwares seguros e pré-aprovados.
- **Atualizações Automáticas:**
  - Configurar sistemas operacionais e softwares críticos para receber atualizações de segurança automaticamente, evitando versões desatualizadas ou vulneráveis.

12.23.4. Monitoramento e Auditoria

- **Registro de Atividades:**
  - Monitorar e registrar todas as atividades relacionadas à instalação, remoção e atualizações de software, gerando logs detalhados para auditorias futuras.
- **Verificação Contínua:**
  - Realizar auditorias periódicas para identificar e remover softwares não autorizados ou desnecessários.
- **Alertas de Alteração:**
  - Configurar sistemas para gerar alertas em caso de instalação ou execução de software não autorizado.

12.23.5. Proteção Contra Riscos

- **Prevenção de Malware:**
  - Realizar verificações com ferramentas antimalware antes e após a instalação de qualquer software.
- **Isolamento:**
  - Para softwares de risco ou desconhecidos, usar ambientes isolados (sandbox) para executar e avaliar seu comportamento.
- **Reversão de Alterações:**
  - Configurar sistemas de backup ou snapshots para reverter rapidamente alterações no caso de instalação inadequada ou impacto negativo.

12.23.6. Conformidade e Normas

- **Políticas Internas:**
  - Estabelecer políticas claras que definam:
  - Quem pode instalar software.
  - Quais softwares são permitidos.
  - Procedimentos de aprovação e validação.
- **Requisitos Regulatórios:**
  - Garantir conformidade com normas de segurança e regulamentações aplicáveis, como ISO/IEC 27001, LGPD ou outras específicas do setor.

12.23.7. Treinamento e Conscientização

- **Capacitação de Usuários:**

- Treinar usuários sobre as políticas de instalação de software e a importância de seguir os procedimentos estabelecidos.

- **Sensibilização sobre Riscos:**
  - Promover conscientização sobre os riscos de instalar softwares de fontes não confiáveis e os impactos de vulnerabilidades no ambiente.

12.23.8. Resposta a Incidentes

- **Detecção de Software Não Autorizado:**
  - Implementar mecanismos para identificar rapidamente instalações não permitidas e tomar ações corretivas.
- **Remoção Segura:**
  - Estabelecer procedimentos para remover softwares não autorizados ou que representem riscos ao ambiente.
- **Análise Pós-Incidente:**
  - Investigar incidentes relacionados à instalação de software, revisar os processos existentes e implementar melhorias.

12.23.9. Benefícios de Gerenciar a Instalação de Software com Segurança

- **Proteção do Ambiente:**
  - Reduzir riscos de malware, vulnerabilidades e impactos em sistemas operacionais.
- **Conformidade:**
  - Garantir alinhamento com políticas internas e regulamentações externas.
- **Otimização de Recursos:**

- Evitar softwares redundantes ou desnecessários, economizando recursos de TI e otimizando desempenho.

12.24. Filtragem da web:

O gerenciamento do acesso a sites externos é uma medida essencial para reduzir a exposição a conteúdos maliciosos, proteger os sistemas e dados da Unimed Ituiutaba e garantir a produtividade dos colaboradores. A seguir estão as diretrizes para a implementação de um sistema eficaz de filtragem da web:

12.24.1. Políticas de Acesso

- **Definição de Regras de Acesso:**
  - Criar políticas claras que definam:
    - Quais tipos de sites são permitidos (ex.: sites relacionados ao trabalho).
    - Quais tipos de sites são bloqueados (ex.: conteúdo adulto, jogos, redes sociais, e sites potencialmente maliciosos).
- **Classificação de Sites:**
  - Utilizar categorias predefinidas (ex.: financeiro, educacional, mídia social) para simplificar a aplicação de políticas de bloqueio ou permissão.
- **Acesso Restrito por Perfil:**
  - Configurar diferentes níveis de acesso com base nas funções e responsabilidades dos usuários, aplicando o princípio do menor privilégio.

12.24.2. Implementação de Soluções de Filtragem

- **Firewall com Filtragem de Conteúdo:**
  - Utilizar firewalls e proxies com capacidades de filtragem de URL para controlar o tráfego web e bloquear sites suspeitos.
- **Soluções de DNS Seguro:**
  - Configurar serviços de DNS seguro (ex.: OpenDNS, Cloudflare Gateway) para impedir conexões a sites maliciosos.
- **Filtragem Baseada em Nuvem:**
  - Adotar soluções de filtragem de web baseadas em nuvem, que oferecem atualizações em tempo real sobre ameaças e classificações de sites.
- **Lista de Bloqueio e Permissão:**
  - Manter listas dinâmicas de URLs bloqueados (blacklists) e URLs permitidos (whitelists), baseadas em categorias e necessidades da Unimed Ituiutaba.

12.24.3. Monitoramento e Análise

- **Monitoramento Contínuo:**
  - Implementar sistemas para monitorar o tráfego web e registrar acessos a sites bloqueados ou suspeitos.
- **Detecção de Comportamento Anômalo:**
  - Identificar padrões de navegação incomuns que possam indicar tentativas de acessar conteúdo malicioso ou violação de políticas.
- **Relatórios Regulares:**
  - Gerar relatórios detalhados sobre o uso da web, incluindo acessos bloqueados, categorias mais visitadas e incidentes detectados.

12.24.4. Proteção Contra Ameaças

- **Bloqueio de Sites Maliciosos:**
  - Bloquear automaticamente o acesso a sites conhecidos por distribuírem malware, phishing ou outras ameaças cibernéticas.
- **Prevenção de Downloads Não Autorizados:**
  - Configurar políticas para impedir o download de arquivos potencialmente perigosos (ex.: executáveis, scripts) de sites externos.
- **Inspeção de Tráfego Criptografado:**
  - Implementar inspeção SSL/TLS para analisar o conteúdo de tráfego criptografado e identificar ameaças ocultas.

12.24.5. Gestão de Exceções

- **Processo de Solicitação:**
  - Estabelecer um processo formal para que usuários solicitem acesso a sites bloqueados, sujeito à aprovação da equipe de TI ou de segurança.
- **Validação de Exceções:**
  - Revisar regularmente as exceções concedidas para garantir sua relevância e conformidade com as políticas.

12.24.6. Treinamento e Conscientização

- **Educação dos Usuários:**
  - Promover treinamentos regulares para conscientizar os colaboradores sobre os riscos associados ao acesso a sites maliciosos e como evitá-los.
- **Boas Práticas de Navegação:**

- Orientar os usuários sobre como identificar sites suspeitos e práticas seguras de navegação na web.

12.24.7. Resposta a Incidentes

- **Isolamento de Dispositivos Comprometidos:**
  - Implementar políticas para isolar rapidamente dispositivos que tentarem acessar sites maliciosos ou que apresentem sinais de comprometimento.
- **Análise Pós-Incidente:**
  - Investigar tentativas de acesso a sites bloqueados ou maliciosos para identificar vulnerabilidades ou falhas nas políticas de filtragem.
- **Aprimoramento Contínuo:**
  - Ajustar as políticas de filtragem com base nas lições aprendidas durante os incidentes.

12.24.8. Benefícios da Filtragem da Web

- **Redução de Riscos:**
  - Minimizar a exposição a conteúdos maliciosos, como malware e phishing.
- **Aumento da Produtividade:**
  - Reduzir o uso indevido da internet no ambiente de trabalho.
- **Conformidade:**
  - Garantir alinhamento com regulamentações e políticas internas de segurança.

12.24.9. Conformidade com Regulamentações

- **Privacidade e LGPD:**

- Assegurar que o monitoramento e a filtragem respeitem as leis de proteção de dados pessoais, como a LGPD, limitando a coleta e análise de dados ao necessário.

- **Documentação:**
  - Manter documentação das políticas de filtragem e do uso de soluções tecnológicas para fins de auditoria e conformidade.

12.25. Desenvolvimento Seguro:

O Ciclo de vida de desenvolvimento seguro:

- Regras para o desenvolvimento seguro de software e sistemas devem ser estabelecidas e aplicadas.
- O Desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um software e um sistema seguro.
- As regras para o desenvolvimento de sistemas e software são estabelecidas e aplicadas aos desenvolvimentos realizados dentro da Unimed Ituiutaba, e registradas através de documentações, abordando os aspectos considerados:

a) segurança do ambiente de desenvolvimento;

b) orientações sobre a segurança no ciclo de vida do desenvolvimento do software:

- Segurança na metodologia de desenvolvimento do software;
- Diretrizes de codificação segura para cada linguagem de programação usada.

c) requisitos de segurança na fase do projeto;

d) pontos de verificação de segurança no cronograma do projeto;

e) repositórios seguros;

f) segurança no controle de versões;

g) conhecimentos de segurança de aplicações;

h) capacidade dos desenvolvedores de evitar, encontrar e corrigir vulnerabilidades;

i) separação dos ambientes de desenvolvimento, teste e produção;

j) testes de segurança em desenvolvimento, aceitação e informações de teste.

12.26. Informações de teste:

As informações utilizadas em ambientes de teste devem ser selecionadas, protegidas e gerenciadas de forma rigorosa para garantir a segurança, a integridade e a conformidade com as políticas organizacionais e a legislação aplicável. As diretrizes abaixo descrevem como isso deve ser implementado:

12.26.1. Seleção de Informações de Teste

- **Dados Sintéticos Preferenciais:**
  - Sempre que possível, utilizar dados fictícios ou sintetizados para testes, evitando o uso de informações reais e sensíveis.
- **Dados Reais (Com Exceções):**
  - Quando o uso de informações reais for imprescindível, garantir que apenas o mínimo necessário seja utilizado e que os dados sejam despersonalizados ou mascarados.
- **Adequação aos Requisitos:**

- Selecionar informações de teste que sejam relevantes e suficientes para atender aos objetivos do teste, garantindo a representatividade do ambiente produtivo.

- **Classificação de Dados:**
  - Identificar e classificar as informações de teste de acordo com o nível de sensibilidade e os requisitos de segurança associados.

12.26.2. Proteção das Informações de Teste

- **Mascaramento e Anonimização:**
  - Implementar técnicas de mascaramento ou anonimização para dados reais, removendo informações que possam identificar indivíduos ou comprometer a privacidade.
- **Controle de Acesso:**
  - Restringir o acesso às informações de teste apenas a equipes autorizadas, aplicando o princípio do menor privilégio.
- **Ambientes Seguros:**
  - Garantir que os testes sejam realizados em ambientes isolados e seguros, sem conexão direta com sistemas produtivos.
- **Criptografia:**
  - Utilizar criptografia para proteger informações de teste em trânsito e em repouso, evitando acessos não autorizados.

12.26.3. Gerenciamento de Informações de Teste

- **Planejamento e Documentação:**

- Documentar o processo de seleção, uso e descarte das informações de teste, incluindo justificativas para o uso de dados reais, se aplicável.

- **Retenção e Exclusão:**
  - Estabelecer prazos claros para a retenção das informações de teste, garantindo sua exclusão segura ao término do ciclo de testes.
- **Monitoramento e Auditoria:**
  - Monitorar o uso das informações de teste e realizar auditorias periódicas para garantir conformidade com as políticas de segurança e proteção de dados.
- **Backup:**
  - Criar backups das informações de teste críticas para evitar perda de dados, armazenando-os de forma segura e com acesso restrito.

12.26.4. Conformidade com Regulamentações

- **Legislação Aplicável:**
  - Garantir que o uso de informações de teste esteja em conformidade com a LGPD (Lei Geral de Proteção de Dados), GDPR (Regulamento Geral de Proteção de Dados) ou outras regulamentações aplicáveis.
- **Consentimento e Notificação:**
  - Caso dados reais sejam utilizados e envolvam informações pessoais, assegurar que o consentimento adequado tenha sido obtido e que as partes envolvidas sejam notificadas, conforme necessário.
- **Relatórios de Conformidade:**
  - Manter registros detalhados das práticas de proteção de dados de teste para fins de auditoria e conformidade legal.

12.26.5. Benefícios da Proteção Adequada de Informações de Teste

- **Redução de Riscos:**
  - Mitigar riscos de vazamento de dados ou exposição indevida em ambientes de teste.
- **Integridade Operacional:**
  - Garantir que os dados de teste sejam consistentes e representativos, permitindo uma validação eficaz de sistemas e processos.
- **Conformidade e Confiança:**
  - Demonstrar responsabilidade e conformidade com regulamentações, fortalecendo a confiança de clientes e partes interessadas.

12.26.6. Treinamento e Conscientização

- **Capacitação das Equipes:**
  - Treinar as equipes responsáveis pelos testes em boas práticas de seleção, proteção e gerenciamento de informações de teste.
- **Conscientização Sobre Riscos:**
  - Promover a conscientização sobre os riscos associados ao uso inadequado de informações de teste e as consequências de violações de dados.

12.27. Proteção de sistemas de informação durante os testes de auditoria:

Os testes de auditoria e outras atividades de garantia que envolvem a avaliação de sistemas operacionais devem ser cuidadosamente planejados, executados e monitorados para garantir a proteção dos sistemas de informação e a integridade dos dados. A seguir estão as diretrizes para conduzir esses testes de forma segura e controlada:

12.27.1. Planejamento dos Testes de Auditoria

- **Definição de Objetivos:**
  - Identificar claramente os objetivos da auditoria, incluindo os sistemas, processos e controles que serão avaliados.
- **Escopo do Teste:**
  - Estabelecer o escopo detalhado dos testes, especificando quais sistemas, aplicações, dados e redes serão incluídos ou excluídos.
- **Planejamento Formal:**
  - Criar um plano de auditoria detalhado que inclua:
  - Objetivos e escopo.
  - Métodos e ferramentas utilizadas.
  - Cronograma das atividades.
  - Equipes e responsáveis.

12.27.2. Acordo com a Gestão Apropriada

- **Aprovação Prévia:**
  - Submeter o plano de auditoria à aprovação da alta gestão e das equipes responsáveis pelos sistemas que serão auditados.
- **Definição de Responsabilidades:**
  - Acordar papéis e responsabilidades entre o testador (auditores internos ou externos) e a gestão, garantindo supervisão adequada.
- **Políticas e Normas Internas:**
  - Garantir que os testes estejam alinhados às políticas internas de segurança e às regulamentações aplicáveis.

12.27.3. Proteção Durante os Testes

- **Ambientes Isolados:**
  - Sempre que possível, realizar testes em ambientes isolados ou de simulação (ex.: sandbox) para evitar impactos nos sistemas de produção.
- **Mínima Interferência:**
  - Garantir que os testes sejam projetados para minimizar a interrupção das operações e o impacto nos usuários finais.
- **Acesso Controlado:**
  - Restringir o acesso dos auditores a apenas informações, sistemas e áreas diretamente relacionadas ao escopo aprovado.
- **Backup Antes dos Testes:**
  - Realizar backups completos dos sistemas e dados críticos antes do início da auditoria para possibilitar a restauração em caso de falhas ou alterações acidentais.
- **Monitoramento Durante os Testes:**
  - Monitorar em tempo real as atividades dos auditores para identificar e responder rapidamente a quaisquer ações que possam comprometer a integridade dos sistemas.

12.27.4. Registro e Documentação

- **Registro de Atividades:**
  - Documentar todas as atividades realizadas durante os testes, incluindo:
  - Ferramentas utilizadas.
  - Dados acessados.
  - Alterações realizadas, se aplicável.

- **Logs de Auditoria:**
  - Manter logs detalhados de acesso e atividades realizadas nos sistemas para análise pós-teste e conformidade.

12.27.5. Revisão Pós-Teste

- **Análise de Resultados:**
  - Compartilhar os resultados da auditoria com as equipes envolvidas, destacando achados relevantes e recomendações.
- **Correção de Vulnerabilidades:**
  - Desenvolver um plano de ação para corrigir vulnerabilidades ou problemas identificados durante os testes.
- **Lições Aprendidas:**
  - Revisar o processo de auditoria para identificar oportunidades de melhoria nas futuras avaliações.

12.27.6. Garantia de Conformidade

- **Regulamentações Aplicáveis:**
  - Garantir que os testes estejam em conformidade com normas regulatórias e padrões de segurança, como ISO/IEC 27001, LGPD e outras aplicáveis.
- **Políticas Internas:**
  - Aderir às políticas internas de auditoria e segurança da informação, alinhando os testes com os requisitos organizacionais.

12.27.7. Ferramentas e Técnicas de Teste

- **Ferramentas Seguras:**
  - Utilizar ferramentas de auditoria confiáveis e certificadas, que sejam compatíveis com os sistemas avaliados.
- **Testes Não Intrusivos:**
  - Sempre que possível, priorizar testes não intrusivos que não modifiquem os sistemas ou dados avaliados.
- **Simulação de Ataques (Opcional):**
  - Caso aprovado, realizar testes de penetração (pentests) simulando ataques controlados para avaliar a segurança do sistema.

12.27.8. Treinamento e Conscientização

- **Capacitação de Auditores:**
  - Garantir que os auditores possuam o treinamento adequado para conduzir testes de forma segura e eficiente.
- **Engajamento das Equipes:**
  - Conscientizar as equipes internas sobre o propósito da auditoria e sua importância para a segurança e a melhoria contínua dos processos.

12.27.9. Benefícios de Proteção Durante os Testes de Auditoria

- **Garantia de Integridade:**
  - Proteger a integridade dos sistemas e dados durante a auditoria, evitando impactos indesejados.
- **Confiabilidade dos Resultados:**

- Assegurar que os resultados dos testes sejam precisos e representem o estado real dos sistemas.

- **Redução de Riscos:**
  - Minimizar riscos operacionais e de segurança associados às atividades de auditoria.

12.28. Princípios de arquitetura e engenharia de sistemas seguros:

Os princípios de arquitetura e engenharia de sistemas seguros são fundamentais para garantir que os sistemas desenvolvidos sejam resilientes, protegidos contra ameaças e alinhados às políticas de segurança da Unimed Ituiutaba. Abaixo, são descritas as diretrizes para estabelecer, documentar, manter e aplicar esses princípios em qualquer atividade de desenvolvimento de sistemas.

12.28.1. Estabelecimento dos Princípios de Sistemas Seguros

- **Definição de Padrões:**
  - Estabelecer um conjunto de princípios baseados em padrões reconhecidos, como ISO/IEC 27001, OWASP (para aplicações web) e NIST Cybersecurity Framework.
  - Incorporar requisitos específicos da Unimed Ituiutaba, considerando riscos, regulamentações aplicáveis e necessidades de negócios.

- **Princípios Fundamentais:**
  - Confidencialidade: Garantir que informações sensíveis sejam acessadas apenas por pessoas autorizadas.
  - Integridade: Proteger os dados e sistemas contra modificações não autorizadas.
  - Disponibilidade: Assegurar que os sistemas estejam operacionais e acessíveis conforme necessário.

- Autenticidade e Não-Repúdio: Validar identidades e garantir que ações realizadas sejam verificáveis.

12.28.2. Documentação dos Princípios

- **Manuais de Segurança:**
  - Criar documentação que descreva os princípios de segurança aplicáveis à arquitetura e engenharia de sistemas.
  - Incluir padrões, frameworks e melhores práticas recomendados para cada etapa do ciclo de vida do sistema.
- **Diretrizes por Fase do Ciclo de Vida:**
  - Documentar princípios específicos para as fases de concepção, design, desenvolvimento, testes, implementação, operação e manutenção.
- **Requisitos de Conformidade:**
  - Incorporar exigências de conformidade regulatória, como LGPD, GDPR e outros requisitos setoriais.

12.28.3. Aplicação dos Princípios no Desenvolvimento

Planejamento e Concepção

- **Análise de Riscos:**
  - Identificar ameaças e vulnerabilidades potenciais logo no início do projeto, utilizando metodologias como STRIDE ou MITRE ATT&CK.
- **Segurança por Design:**
  - Garantir que os requisitos de segurança sejam incorporados desde o planejamento, evitando a necessidade de ajustes tardios.

- Design

- **Princípio do Menor Privilégio:**
  - Projetar sistemas para que usuários e processos tenham apenas as permissões necessárias.
- **Defesa em Camadas:**
  - Implementar múltiplos níveis de proteção, como autenticação, firewalls e criptografia, para dificultar ataques.
- **Separação de Ambientes:**
  - Garantir a separação clara entre ambientes de desenvolvimento, teste e produção.
- **Redundância e Tolerância a Falhas:**
  - Incorporar mecanismos redundantes e tolerantes a falhas para garantir a disponibilidade do sistema.
  - Desenvolvimento
- **Codificação Segura:**
  - Adotar práticas de codificação segura, como evitar vulnerabilidades comuns (ex.: injeção de SQL, cross-site scripting), utilizando as diretrizes do OWASP Top 10.
- **Revisão de Código:**
  - Implementar revisões regulares de código por pares para identificar e corrigir possíveis vulnerabilidades.
  - Testes
- **Testes de Segurança:**
  - Realizar testes de vulnerabilidades e penetração em cada fase do desenvolvimento para identificar possíveis fraquezas.

- **Ferramentas Automatizadas:**
  - Utilizar ferramentas de análise estática e dinâmica para identificar falhas no código e na arquitetura.
  - Implantação
- **Validação Final:**
  - Garantir que os sistemas sejam validados por equipes de segurança antes da implantação.
- **Configuração Segura:**
  - Implementar controles, como criptografia de dados em repouso e em trânsito, autenticação multifator e proteção contra ataques conhecidos.

12.28.4. Manutenção e Atualizações

- **Gerenciamento Contínuo de Riscos:**
  - Monitorar continuamente os sistemas para identificar novas ameaças e corrigir vulnerabilidades.
- **Atualizações e Patches:**
  - Manter o sistema atualizado com patches de segurança e versões mais recentes de bibliotecas e frameworks utilizados.
- **Revisões Periódicas:**
  - Realizar revisões regulares da arquitetura e dos controles de segurança para garantir alinhamento com novas ameaças e requisitos.

12.28.5. Treinamento e Conscientização

- **Capacitação de Equipes:**

- Treinar desenvolvedores, arquitetos e equipes de TI em princípios de segurança e boas práticas de engenharia de sistemas.

- **Cultura de Segurança:**
  - Promover uma cultura organizacional que valorize e priorize a segurança em todas as etapas do desenvolvimento.

12.28.6. Benefícios de Sistemas Seguros

- **Mitigação de Riscos:**
  - Reduzir vulnerabilidades e a exposição a ataques, como vazamentos de dados e interrupções de serviço.
- **Conformidade e Confiança:**
  - Atender a requisitos regulatórios e aumentar a confiança de clientes e parceiros nos sistemas da Unimed Ituiutaba.
- **Eficiência Operacional:**
  - Evitar retrabalho e custos associados à correção de problemas de segurança identificados tardiamente.

12.28.7. Conformidade e Normas

- **Aderência a Normas e Regulamentações:**
  - Garantir que os princípios de segurança estejam alinhados com normas como ISO/IEC 27001, NIST SP 800-53 e PCI DSS.
- **Auditorias e Certificações:**
  - Submeter os sistemas a auditorias regulares para validar a aplicação dos princípios e garantir conformidade.

12.28.8. Monitoramento e Melhoria Contínua

- **Feedback do Ciclo de Vida:**
  - Incorporar feedback de eventos de segurança, auditorias e análises de desempenho para melhorar continuamente os princípios de segurança.
- **Ferramentas de Monitoramento:**
  - Implementar soluções de monitoramento para identificar violações de segurança e responder a incidentes em tempo hábil.

12.29. Desenvolvimento terceirizado:

A terceirização do desenvolvimento de sistemas deve ser gerenciada de forma rigorosa para garantir que as atividades realizadas por fornecedores externos estejam alinhadas aos padrões de segurança, qualidade e objetivos da Unimed Ituiutaba. A seguir, são descritas as diretrizes para dirigir, monitorar e analisar criticamente essas atividades.

12.29.1. Direção e Gestão do Desenvolvimento Terceirizado

12.29.1.1. Seleção de Fornecedores

- **Avaliação de Credibilidade:**
  - Escolher fornecedores com histórico comprovado de entregas bem-sucedidas e expertise no desenvolvimento de sistemas.
- **Critérios de Seleção:**
  - Avaliar fornecedores com base em critérios como:
  - Conformidade com regulamentações aplicáveis (ex.: LGPD, GDPR).
  - Capacidade técnica e de segurança.

- Certificações, como ISO/IEC 27001.
- Due Diligence:
- Realizar análises de due diligence para avaliar riscos financeiros, jurídicos e técnicos associados ao fornecedor.

12.29.2. Contratos e Acordos

- **Cláusulas Contratuais:**
  - Incluir cláusulas específicas para garantir:
  - Confidencialidade das informações compartilhadas.
  - Proteção de propriedade intelectual.
  - Cumprimento de prazos e SLAs (Acordos de Nível de Serviço).
  - Padrões de segurança no desenvolvimento.
  - Direitos de Auditoria:
  - Garantir o direito de auditar o fornecedor para avaliar conformidade com requisitos de segurança e qualidade.
- **Responsabilidades Definidas:**
  - Estabelecer claramente as responsabilidades do fornecedor e da Unimed Ituiutaba durante o projeto.

12.29.3. Monitoramento das Atividades de Desenvolvimento

12.29.3.1. Acompanhamento do Processo

- **Plano de Projeto:**
  - Solicitar um plano detalhado do projeto, incluindo cronograma, entregáveis e marcos de progresso.
- **Relatórios Regulares:**

- Exigir relatórios de progresso periódicos que detalhem o status das atividades, eventuais desvios e ações corretivas.

- **Pontos de Controle (Milestones):**
  - Definir checkpoints em fases críticas do projeto para revisar entregas e alinhar expectativas.

12.29.4. Garantia de Qualidade

- **Revisão de Código:**
  - Solicitar revisões de código, realizadas internamente ou pelo fornecedor, para garantir aderência às boas práticas e padrões de segurança.
- **Testes de Segurança:**
  - Exigir que o fornecedor realize testes de segurança, como análises estáticas e dinâmicas, além de testes de penetração, antes de entregar o sistema.
- **Conformidade com Padrões:**
  - Verificar se o fornecedor segue padrões reconhecidos, como OWASP (para aplicações web) e NIST.

12.29.5. Controle de Acesso

- **Compartilhamento de Informações:**
  - Limitar o acesso do fornecedor apenas às informações e sistemas estritamente necessários para o desenvolvimento.
- **Monitoramento de Acessos:**
  - Registrar e monitorar todos os acessos realizados pelo fornecedor nos sistemas da Unimed Ituiutaba.

12.29.6. Análise Crítica das Atividades Terceirizadas

12.29.6.1. Avaliação de Entregáveis

- **Validação de Requisitos:**
  - Verificar se os sistemas entregues atendem aos requisitos técnicos, funcionais e de segurança previamente estabelecidos.
- **Teste de Conformidade:**
  - Realizar testes internos para validar que os sistemas estão em conformidade com as políticas de segurança e regulamentações aplicáveis.
- **Feedback e Ajustes:**
- Fornecer feedback claro ao fornecedor para correções e melhorias necessárias antes da aceitação final.

12.29.7. Revisão Periódica

- **Avaliação de Desempenho:**
  - Avaliar regularmente o desempenho do fornecedor com base em métricas, como qualidade do código, cumprimento de prazos e aderência aos requisitos de segurança.
- **Auditorias e Relatórios:**
  - Conduzir auditorias periódicas nas atividades terceirizadas e revisar relatórios de auditoria fornecidos pelo fornecedor.
- **Lições Aprendidas:**
  - Documentar lições aprendidas durante o projeto para melhorar futuras iniciativas de terceirização.

12.29.8. Mitigação de Riscos

- **Planos de Contingência:**
  - Desenvolver planos de contingência para mitigar riscos associados ao fornecedor, como interrupção de serviços ou falhas de entrega.
- **Backup e Redundância:**
  - Garantir que os dados e sistemas críticos sejam protegidos, realizando backups regulares e mantendo redundância adequada.
- **Plano de Resposta a Incidentes:**
  - Estabelecer procedimentos claros para lidar com incidentes de segurança que envolvam o fornecedor, como vazamento de dados ou violações contratuais.

12.29.9. Treinamento e Conscientização

- **Capacitação Interna:**
  - Treinar equipes internas para gerenciar fornecedores e monitorar projetos terceirizados com eficácia.
- **Integração com o Fornecedor:**
  - Conscientizar o fornecedor sobre as políticas de segurança e requisitos específicos da Unimed Ituiutaba.

12.29.10. Conformidade com Regulamentações

- LGPD e GDPR:
- Garantir que o fornecedor implemente controles para proteger dados pessoais em conformidade com leis de proteção de dados.
- Normas de Segurança:

- Exigir que o fornecedor atenda a normas aplicáveis, como ISO/IEC 27001, PCI-DSS (para dados financeiros) ou outras regulamentações setoriais.
- Contratos de Confidencialidade (NDAs):
- Firmar NDAs (Acordos de Não Divulgação) com o fornecedor para proteger informações sensíveis.

12.29.11. Benefícios de uma Gestão Eficiente do Desenvolvimento Terceirizado

- **Qualidade e Segurança:**
  - Garantir entregas de alta qualidade e sistemas seguros, alinhados aos objetivos da Unimed Ituiutaba.
- **Mitigação de Riscos:**
  - Reduzir riscos associados a falhas de segurança, atrasos ou violações contratuais.
- **Eficiência Operacional:**
  - Otimizar recursos internos e garantir que os projetos sejam concluídos dentro dos prazos e do orçamento.

12.30. Gestão de mudanças:

A gestão de mudanças é essencial para garantir que quaisquer alterações nos recursos de tratamento de informações e sistemas de informação sejam implementadas de forma controlada, minimizando riscos à segurança, integridade e disponibilidade. Abaixo estão as diretrizes para os procedimentos de gestão de mudanças.

12.30.1. Planejamento de Mudanças

12.30.1.1. 1Identificação e Classificação

- **Solicitação de Mudança (RFC - Request for Change):**
  - Todas as mudanças devem ser formalmente solicitadas por meio de uma RFC, que deve incluir:
  - Descrição detalhada da mudança.
  - Justificativa e objetivos.
  - Sistemas ou recursos impactados.
  - Nível de criticidade.
- **Classificação de Mudanças:**
  - Categorizar as mudanças com base no impacto e urgência:
  - Mudanças Normais: Alterações planejadas, com avaliação completa de riscos.
  - Mudanças de Emergência: Alterações críticas que exigem implementação imediata.
  - Mudanças Padrão: Alterações recorrentes e de baixo risco.

12.30.1.2. Planejamento Detalhado

- **Avaliação de Impacto:**
  - Avaliar os impactos da mudança nos sistemas, processos e usuários.
  - Identificar riscos potenciais e desenvolver planos de mitigação.
- **Plano de Implementação:**
  - Criar um plano detalhado para a execução da mudança, incluindo cronograma, recursos necessários e responsáveis.

- **Plano de Reversão (Rollback):**
  - Definir um plano de contingência para reverter a mudança em caso de falhas.

12.30.2. Aprovação de Mudanças

- **Revisão por Comitê de Mudanças (CAB - Change Advisory Board):**
  - Submeter todas as mudanças classificadas como "normais" ou de alto impacto ao CAB para aprovação.
- **Critérios de Aprovação:**
  - Assegurar que as mudanças atendam aos seguintes critérios antes da aprovação:
  - Impacto mínimo na operação.
  - Plano de mitigação de riscos documentado.
  - Conformidade com as políticas de segurança e regulamentações.

12.30.3. Implementação de Mudanças

12.30.3.1. Execução Controlada

- **Responsáveis pela Execução:**

  Garantir que somente pessoal autorizado e qualificado execute as mudanças.
- **Isolamento de Ambientes:**

  Sempre que possível, implementar mudanças inicialmente em ambientes de teste antes de aplicar em produção.
- **Janela de Implementação:**

  Agendar mudanças em horários que minimizem o impacto operacional (ex.: fora do horário comercial).

12.30.4. Monitoramento Durante a Implementação

- **Monitoramento em Tempo Real:**
  - Acompanhar o progresso da mudança para identificar problemas imediatamente.
- **Comunicação:**
  - Manter as partes interessadas informadas sobre o status da implementação.

12.30.5. Pós-Implementação

12.30.5.1. Validação

- **Testes Pós-Mudança:**
  - Realizar testes para confirmar que a mudança foi implementada conforme o planejado e que os sistemas continuam operacionais.
- **Confirmação de Sucesso:**
  - Obter a aprovação dos responsáveis pelo sistema para validar a efetividade da mudança.

12.30.5.2. Monitoramento e Ajustes

- **Monitoramento Contínuo:**
  - Monitorar o desempenho do sistema após a mudança para identificar impactos inesperados.
- **Correção de Problemas:**
  - Corrigir problemas identificados com base no plano de reversão ou ajustes necessários.

12.30.6. Documentação

- **Registro de Mudanças:**
  - Documentar todas as etapas da mudança, incluindo:
  - RFC original.
  - Planos de implementação e reversão.
  - Resultados de testes e validações.
  - Problemas enfrentados e ações tomadas.
- **Histórico de Mudanças:**
  - Manter um histórico centralizado de todas as mudanças realizadas para fins de auditoria e aprendizado.

12.30.7. Comunicação

- **Notificação de Stakeholders:**
  - Informar stakeholders relevantes antes, durante e após a implementação das mudanças.
- **Manual de Usuário Atualizado:**
  - Atualizar documentações, manuais e treinamentos para refletir as mudanças realizadas.

12.30.8. Auditoria e Revisão

- **Revisão Pós-Mudança:**
  - Realizar uma revisão formal para avaliar o sucesso da mudança e identificar melhorias para o processo de gestão de mudanças.
- **Auditorias Periódicas:**

- Revisar o histórico de mudanças para garantir conformidade com as políticas e identificar tendências.

12.30.9. Conformidade com Regulamentações

- **Atendimento a Normas e Leis:**
  - Garantir que todas as mudanças sigam as regulamentações aplicáveis, como LGPD, ISO/IEC 27001, e outras normas específicas do setor.
- **Aprovação e Evidências:**
  - Manter evidências documentadas de conformidade e aprovação para auditorias externas ou internas.

12.30.10. Benefícios da Gestão de Mudanças

- **Redução de Riscos:**
  - Minimizar impactos operacionais e de segurança associados a alterações nos sistemas.
- **Maior Controle:**
  - Garantir que as mudanças sejam implementadas de forma planejada e organizada.
- **Melhoria Contínua:**
  - Aprender com mudanças anteriores para otimizar processos futuros.

13.CONSCIENTIZAÇÃO

O Gestor responsável de SI, junto ao Comitê Gestor de Privacidade e de Segurança da Informação da Unimed Ituiutaba, dentro de suas responsabilidades, deverá promover a todos os

colaboradores e vinculados à Unimed Ituiutaba que utilizam ativos de informação, a conscientização a respeito dos procedimentos de segurança da informação de forma periódica, por meio de eventos, treinamentos, palestras, campanhas, workshops e demais medidas educativas.

14.PLANO DE CONTINUIDADE DE NEGÓCIOS

A gestão da continuidade do negócio deve estar incorporada aos processos e a estrutura organizacional da Unimed Ituiutaba junto com o Responsável de TI, a elaboração, aprovação e implementação dos planos que garantam o fluxo de informações necessárias à continuidade das atividades críticas e o retorno à situação de normalidade.

15.MESA LIMPA E TELA LIMPA

A política de mesa limpa e tela limpa se refere a práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

Visando a redução dos riscos de acesso não autorizado a informações, perda ou danos a informações, devem ser adotadas pelos Colaboradores da Unimed, a política que visa a inexistência de papéis e outras mídias sobre as mesas e a inexistência de informações disponíveis por muito tempo em telas de computador, durante e após o horário normal de trabalho. Desta forma, em conformidade com a ISO 27002:

- papéis e mídias utilizadas por computadores sejam armazenados em dispositivos adequadamente protegidos contra acesso, tais como armários, gavetas, cofres e outros;
- computadores portáteis, estações e terminais sejam bloqueados ou protegidos por senhas quando estiverem inativos ou estiverem desacompanhados de seus responsáveis;
- adoção de uma cultura e conscientização sem papel e descarte apropriado de informações.

16.RESPONSABILIDADES

Em regra, cabe a todos os Diretores, Colaboradores, Usuários, Clientes, Parceiros, Fornecedores, e demais partes interessadas da Unimed Ituiutaba:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Unimed Ituiutaba;
- Realizar os treinamentos obrigatórios disponibilizados pela Unimed Ituiutaba;
- Proteger as informações contra acessos, modificações, destruição ou divulgação não autorizada pela Unimed Ituiutaba;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Unimed Ituiutaba;
- Comunicar imediatamente à área de Segurança da Informação sobre qualquer descumprimento ou violação desta Política e/ou Normas ou Procedimentos, pelo e-mail: ti@unimedituiutaba.coop.br respectivamente, bem como reportar àqueles quaisquer incidentes de Segurança da Informação.

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

Diretoria

- Aprovar esta Política de Segurança da Informação.

Área de Tecnologia da Informação

- Monitorar os recursos e os ambientes sob a sua responsabilidade, com o objetivo de garantir a proteção contra as possíveis ameaças e o uso inadequado, assim como mantê-los em dia com as suas atualizações e com as mudanças na legislação e/ou nos requisitos do negócio.

Área de Segurança da Informação

- Elaboração e revisão de Políticas, Procedimentos Operacionais (POPs) e manuais;
- Gerenciar os controles e as ferramentas de Segurança da Informação, assim como tratar os incidentes, problemas, mudanças e quaisquer requisições e/ou reportes relacionados à Segurança da Informação;
- Promover junto ao Comitê Gestor de Privacidade de Dados e Segurança da Informação a conscientização e cultura em Segurança da Informação.

Comitê Gestor de Privacidade de Dados e Segurança da Informação

- Assessorar na implementação das ações de segurança da informação e comunicações na Unimed Ituiutaba;
- Constituir grupos de trabalho para tratar temas e propor soluções específicas sobre segurança da informação e comunicações;
- Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a PSI e regulamentos existentes sobre o tema.
- O Comitê Gestor de Privacidade de Dados e Segurança da Informação (CGPSI) é constituído por meio de um representante de cada área existente da Unimed Ituiutaba.

Gestores

- Disseminar a cultura em Segurança da Informação por meio do exemplo, verificando o cumprimento dos controles, bem como orientando os colaboradores e estagiários sob sua gestão;
- Definir os privilégios de acesso dos colaboradores e estagiários sob sua gestão de acordo com as atividades que desempenham.

Terceiros e fornecedores

- Tomar conhecimento e cumprir as diretrizes desta PSI.

17.SANÇÕES

Nos casos em que houver o descumprimento ou violação de um ou mais itens da PSI ou de suas Normas, procedimentos ou atividades pertinentes à Segurança da Informação os infratores estarão sujeitos a sindicâncias e processos administrativos, bem como as penalidades previstas na legislação e regulamentos internos aplicáveis.

18.AUDITORIA

Deve ser realizada, com periodicidade mínima anual, a verificação da conformidade das práticas de SI da Unimed Ituiutaba desta PSI e procedimentos complementares, bem como com a legislação específica de SIC.

A área de Tecnologia da Informação deve identificar a necessidade de geração de logs e seu nível de detalhamento nos sistemas e ambientes sob sua responsabilidade, bem como a periodicidade de realização de auditoria dos logs gerados.

A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo Comitê Gestor de Privacidade de Dados e Segurança da Informação (CGPSI).

Os resultados de cada ação verificada nos ambientes da Unimed Ituiutaba serão documentados em relatório de avaliação de conformidade, o qual será encaminhado aos Gestores das áreas, para ciência e tomada das ações cabíveis.

19.DISPOSIÇÕES GERAIS

Os integrantes do CGPSI (Comitê Gestor de Privacidade de Dados e Segurança da Informação) são responsáveis por conhecer e entender toda a documentação orientadora aplicável a eles. Da mesma forma, os Diretores e Gestores de cada área da Unimed Ituiutaba são responsáveis por garantir que todos os seus colaboradores entendam e sigam as documentações orientadoras aplicáveis da Unimed Ituiutaba.

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

A Política de Segurança da Informação, Normas, Procedimentos e Termos complementares enunciados no item 9 fazem parte do presente documento, com o intuito de mantê-lo operacional, aplicável e auditável, tendo em vista a característica dinâmica da Segurança da Informação.

Os colaboradores que apresentem dúvidas ou preocupações com relação a esta Política, os termos ou as obrigações deste documento, devem entrar em contato com a área de Segurança da Informação ou Comitê Gestor de Privacidade de Dados e Segurança da Informação.

20.ATUALIZAÇÃO

A PSI e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 01 (hum) ano.

21.DIVULGAÇÃO

A PSI e suas atualizações, bem como as normas complementares, devem ser divulgadas a todos os colaboradores que habitualmente trabalham na Unimed Ituiutaba.

22.VIGÊNCIA

Esta política de Segurança da Informação entra em vigor na data da aprovação e assinatura.

Integrante(s) envolvido(s):

Diretores, Comitê Gestor de Privacidade de Dados e Segurança da Informação da Unimed Ituiutaba.

Elaboração	Análise crítica	Classificação da Informação	Aprovação
Brunno Eduardo Vilela Batista	Murilo Morais De Oliveira	Pública	Dra. Rosane Abramo Dr. Raphael Gonçalves de Oliveira
Data: 12/01/2026	Data: 16/01/2026		

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

23.HISTÓRICO DE ALTERAÇÕES

EMISSÃO	REVISÃO	DESCRIÇÃO DA ALTERAÇÃO	ELABORADO POR	APROVADO POR

24.REFERÊNCIAS

- NBR/ISO/IEC 27000:2018 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27001:2022 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27701:2019 Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes;
- Lei nº 9.983, de 14 de julho de 2000, que altera o Código Penal Brasileiro;
- Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI);
- Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet (MCI);

Processo:	Gerir e estabelecer os conceitos e diretrizes de segurança da informação.
Atividade:	proteger as informações e todos os ativos de informação, em meio físico e digital, da Unimed Ituiutaba.
Título:	Política De Segurança Da Informação.

Aprovação:

rosane.abramo@unimedituiutaba.coop.br
Assinado
Rosane Abramo
D4Sign

Rosane Abramo

Diretora Presidente

raphael.oliveira@unimedituiutaba.coop.br
Assinado
Raphael
D4Sign

Raphael Gonçalves de Oliveira

Diretor Administrativo/Financeiro

Elaboração	Análise crítica	Classificação da Informação	Aprovação
Brunno Eduardo Vilela Batista	Murilo Morais De Oliveira	Pública	Dra. Rosane Abramo Dr. Raphael Gonçalves de Oliveira
Data: 12/01/2026	Data: 16/01/2026		

144 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 19 de January de 2026, 14:53:30

POL ITU 05 - Política De Segurança Da Informação pdf

Código do documento 5b486709-7d67-419c-ab11-e10243ab4e3f

Assinaturas

Rosane Abramo
rosane.abramo@unimedituiutaba.coop.br
Assinou

Raphael Gonçalves de Oliveira
raphael.oliveira@unimedituiutaba.coop.br
Assinou

Eventos do documento

16 Jan 2026, 10:26:57
Documento 5b486709-7d67-419c-ab11-e10243ab4e3f **criado** por BRUNNO EDUARDO VILELA BATISTA (e774cb56-8571-4664-8d9b-5c2646f5d040). Email:ti@unimedituiutaba.coop.br. - DATE_ATOM: 2026-01-16T10:26:57-03:00

16 Jan 2026, 10:33:27
Assinaturas **iniciadas** por BRUNNO EDUARDO VILELA BATISTA (e774cb56-8571-4664-8d9b-5c2646f5d040). Email: ti@unimedituiutaba.coop.br. - DATE_ATOM: 2026-01-16T10:33:27-03:00

16 Jan 2026, 13:17:45
RAPHAEL GONÇALVES DE OLIVEIRA **Assinou** (da0f1a67-939a-4af1-88f3-2240d4fde565) - Email: raphael.oliveira@unimedituiutaba.coop.br - IP: 177.191.62.179 (177-191-062-179.xd-dynamic.algarnetsuper.com.br porta: 48694) - Geolocalização: -18.9982717 -49.4482778 - Documento de identificação informado: 025.426.081-05 - DATE_ATOM: 2026-01-16T13:17:45-03:00

16 Jan 2026, 19:01:31
ROSANE ABRAMO **Assinou** (81fde611-50a9-42ef-94f4-d200387673f7) - Email: rosane.abramo@unimedituiutaba.coop.br - IP: 104.28.63.117 (104.28.63.117 porta: 1148) - Geolocalização: -18.88868190838905 -48.23037860958977 - DATE_ATOM: 2026-01-16T12:01:31-10:00

Hash do documento original
(SHA256):447d80d6d878a1b1727eb337fbdee5a2c6eff324e24fe32539c21350214a28ba
(SHA512):63206d9cfbb4dbba016b6bfae77bd539b8bf1b6d3aa0a72968920d09f87790bc6c0f3721eabedfc3e71973733cf8e86308cab622b24af1644b574431525a8d3e

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

144 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 19 de January de 2026, 14:53:30

Esse documento está assinado e certificado pela D4Sign
Integridade certificada no padrão ICP-BRASIL
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.