RESUMO DAS REVISÕES		
Edição	**Data**	**Alteração**
01	01/02/2023	Emissão inicial

1. OBJETIVO

Esta política fornece diretrizes para práticas de gestão de segurança da informação, incluindo a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

2. APLICAÇÃO

Toda Unimed de Tupã, suas unidades e partes interessadas.

3. DEFINIÇÕES

DPONET- Suporte técnico sobre proteção e privacidade de dados, na forma de orientações objetivas ao CLIENTE sobre práticas a serem tomadas em relação à proteção de dados pessoais;

BACKUP- cópia de segurança ou salvaguarda é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

TI- Tecnologia da Informação

4. RESPONSABILIDADES

4.1 Responsabilidades e papéis da segurança da informação

Alta Direção: Demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização;

b) garantindo a integração dos requisitos do sistema de gestão da segurança da informação dentro dos processos da organização;

c) assegurando que os recursos necessários para o sistema de gestão da segurança da informação estejam disponíveis;

d) comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;

e) assegurando que o sistema de gestão da segurança da informação alcança seus resultados pretendidos;

f) orientando e apoiando pessoas que contribuam para eficácia do sistema de gestão da segurança da informação;

g) promovendo a melhoria contínua; e

h) apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade.

Gestor do SGSI: responsável por coordenar a implementação e manutenção do Sistema de Gestão da Segurança da Informação, bem como assegurar que o sistema de gestão da segurança da informação está em conformidade com os requisitos da Norma ISO 27001 (Anexo A) e relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção.

Gestor da Tecnologia da Informação: responsável pela gestão dos recursos da tecnologia da informação pelos seguintes meios:

Manutenção dos recursos.

Identificar e avaliar riscos.

Garantir que os recursos atendam as recomendações de seus fabricantes e desenvolvedores.

Inventariar os recursos.

Preservar controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações.

Manter mecanismos adequados para garantir a rápida recuperação em situações de contingência.

Gestor de Recursos Humanos: responsável pela gestão da capacitação dos colaboradores, incluindo a documentação definida em 5.1.1, realização de campanhas de conscientização e atuar nos

processos disciplinares.

Jurídico: responsável pela validação da informação documentada e práticas pertinentes ao sistema de gestão da segurança da informação.

Colaboradores: responsável pela proteção de seus ativos e cumprimento do conjunto de políticas definidas em 5.1.1.

4.1.1 Segregação de funções

Para reduzir o risco de mau uso, acidental ou deliberado, dos ativos da organização, o processo de tecnologia da informação restringe os meios aos quais uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção por meio do Active Directory e segmentação de rede.

4.1.2 Contato com autoridades

As autoridades a serem contatadas em casos de incidentes de segurança de informação são definidas por meio do FOR-01.

4.1.3 Contato com grupos especiais

A organização, por meio do processo de Tecnologia da Informação mantém contato com fóruns de segurança da informação para ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação e receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades.

4.1.4 Segurança da informação no gerenciamento de projetos

A organização incorpora a segurança da informação no gerenciamento de projetos conforme formulário de planejamento de mudanças [FOR-03-Planejamento de Mudanças.xlsx].

Os controles de projeto incluem que:

a) os objetivos de segurança da informação sejam contemplados nos objetivos do projeto;

b) uma avaliação dos riscos de segurança da informação é conduzida em estágios iniciais do projeto para identificar os controles que são necessários;

c) a segurança da informação é parte integrante de todas as fases da metodologia do projeto.

As questões de segurança da informação são consideradas e analisadas criticamente a intervalos planejados, em todos os projetos e as responsabilidades pela segurança da informação são definidas e alocadas para papéis específicos.

4.2 Dispositivos móveis e trabalho remoto

4.2.1 Política para uso de dispositivos móvel

Na utilização de dispositivos móveis os seguintes cuidados especiais devem ser tomados para assegurar que as informações do negócio não sejam comprometidas.

a) registros dos dispositivos móveis: Ferramenta OCS.

b) restrições quanto à instalação de *software, somente com a autorização da T.I.*

c) técnicas criptográfica: Nativa do Android.

d) Proteção contra códigos maliciosos: através do antivírus **Eset EndPoint Secutiry.**

e) desativação, bloqueio e exclusão de forma remota: **Através de configuração de conta do Google.**

f) *backups*: **É feito através da conta do Google.**

Em caso de roubo de dispositivos móveis, entrar em contato com as autoridades pertinentes previstas no [FOR-01-Contato com Autoridades.xlsx].

4.2.1.a. Uso de dispositivos pessoais.

A separação do uso do dispositivo para negócio e para fins pessoais é realizada por meio de:

Conscientização.

Os colaboradores que fazem uso de dispositivos pessoais tem conhecimento das suas responsabilidades quanto aos cuidados especiais previstos em 6.2.1, renunciando direitos autorais dos dados do negócio, que permita a exclusão remota dos dados pela organização no caso de furto, roubo ou perda do dispositivo móvel ou ainda, quando não mais houver autorização para o uso dos serviços.

4.2.2 Trabalho remoto

Trabalho remoto é realizado pelo escritório de contabilidade, e as configurações de acesso

são formalizados por meio de [Unimed - Acesso TS contabilidade.DOCX]

5. DESCRIÇÃO

5.1 REQUISITOS DE SEGURANÇA DE INFORMAÇÃO

Existem três fontes principais de requisitos de segurança da informação.

a) Uma fonte é obtida a partir da avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos, e as vulnerabilidades destes e realizada uma estimativa da probabilidade de ocorrência das ameaças e da consequência potencial ao negócio.

b) Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

c) A terceira fonte são os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

5.1.1 POLÍTICAS DE SEGURANÇA DE INFORMAÇÃO

5.1 1 a Políticas para segurança da informação

A organização definiu um conjunto de políticas estruturado nos seguintes documentos:

SGSI-01 – Política de segurança de informação.

(O SGSI-01 contempla informações a nível de controles).

SGSI-02 – Norma de segurança da informação.

(O SGSI-02 contempla informações a nível operacional).

5.1.1 b Análise crítica das políticas para segurança da informação

As políticas e normas do SGSI devem ser analisadas criticamente e revisadas no mínimo semestralmente, ou quando mudanças significativas ocorrerem.

5.2 GESTÃO DE ATIVOS

5.2 .1 Responsabilidade pelos ativos

5.3 a Inventário dos ativos

Os ativos associados com informação e com os recursos de processamento da informação são identificados por meio da Ferramenta OCS e um inventário destes ativos é mantido por meio da própria ferramenta.

Ativos é qualquer elemento que tenha valor para a organização e que precise de proteção:

• Hardware (Computadores, servidores, impressoras, celulares, cartões de memória).
• Software (Independente da licença).
• Informação (mídias eletrônicas como banco de dados, arquivos em PDF, Word, Excel, e outros formatos, além de papéis e outras formas): DPOnet.
• Senhas (Sites).

A organização identifica os ativos relevantes no ciclo de vida da informação e documenta o ciclo de vida da informação por meio do **DPO Net** incluindo: a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição.

5.3.1 Proprietário dos ativos

Os proprietários dos ativos são identificados por meio da ferramenta OCS.

5.3.2 Uso aceitável dos ativos

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

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

5.3.3 Devolução dos ativos

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

Caso o funcionário use o seu próprio equipamento pessoal, os procedimentos adotados para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura, são realizados conforme requisito 11.2.7.

5.4 Classificação da informação

A informação deve receber um nível adequado de proteção, de acordo com a sua importância para a organização. (A responsabilidade de classificação é do proprietário do ativo).

Os níveis de classificação são:

1. **Público**: quando sua divulgação não causa nenhum dano;
2. **Uso Interno**: quando a divulgação causa constrangimento menor ou inconveniência operacional menor;
3. **Restrito**: quando a divulgação tem um pequeno impacto significativo nas operações ou objetivos táticos;

4. **Confidencial**: quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

A classificação do ativo é registrada pelos seguintes meios:

- Hardware: OCS.
- Software: OCS.
- Informação: DPOnet.
- Infraestrutura: OCS.
- Serviços de terceiros: OCS.
- Senhas: Formulário.

5.4.1 Rótulos e tratamento da informação

A rotulação reflete o esquema de classificação estabelecido em 8.2.1.

Não é necessário rotular informação com classificação: Público.

Os rótulos devem ser reconhecidos pelos seguintes meios:

- Hardware: Placa.
- Software: Não necessita rótulo, sendo identificado nesta política.
- Informação: Na própria informação.
- Infraestrutura: Placa.
- Serviços de terceiros: Não necessita rótulo, sendo identificado nesta política.
- Senhas: Formulário.

5.4.2 Tratamento de ativos:

a. Restrições de acesso para apoiar os requisitos de proteção para cada nível de classificação por meio do Active Directory.

b. Armazenamento dos ativos de TI de acordo com as especificações dos fabricantes.

5.5 Tratamento de mídias

5.5.1 Gerenciamento de mídias removíveis

O gerenciamento de mídias removíveis segue as seguintes diretrizes:

a. quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável é destruído, caso venha a ser retirado da organização;

b. quando houver necessidade de remoção de qualquer mídia da organização é mantido o registro dessa remoção por meio de [FOR-08-Controle de remoção de ativos.xlsx].

c. toda mídia é guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;

d. Para mitigar o risco de degradar a mídia enquanto os dados armazenados ainda são necessários, convém que os dados sejam transferidos para uma mídia nova antes de se tornar ilegíveis;
e. As mídias removíveis são registradas no **OCS** para limitar a oportunidade de perda de dados;

5.6 Descarte de mídias

As mídias não mais necessárias para uso, são descartadas por meio de Destruição interna com foto e o registro do descarte é realizado por meio de [FOR22-Controle de descarte de mídia.xlsx].
As mídias acumuladas para descarte devem ser armazenadas na sala de T.I.

5.6.1 Transferência física de mídias

Para proteger as mídias que contém informações, quando transportadas, recomenda-se:
a) Que o meio de transporte ou o serviço de mensageiros sejam confiáveis e autorizados em concordância com o gestor.
b) A embalagem deve ser suficiente para proteger o conteúdo contra qualquer dano físico.

5.7 CONTROLE DE ACESSO

5.7.1 Requisitos do negócio para controle de acesso

Objetivo: Limitar o acesso à informação e aos recursos de processamento da informação.

5.7.1 a Política de controle de acesso

Os requisitos a serem atendidos pelo controle de acesso são:
requisitos de segurança de aplicações por meio do A.D.
a) Obrigação contratual relativa à proteção de acesso para dados ou serviços.
b) gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis por meio do firewall e A.D.
c) segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso por meio do A.D.
d) requisitos para análise crítica periódica de direitos de acesso semestralmente.
e) remoção de direitos de acesso por meio de A.D.
f) arquivo dos registros de todos os eventos significativos, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta por meio do Graylog.

5.7.1 b Acesso às redes e aos serviços de rede

Os usuários somente recebem acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar por meio do A.D.

5.8 Gerenciamento de acesso do usuário

Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

5.8.1 Registro e cancelamento de usuário

Um processo formal de registro e cancelamento de usuários é implementado para permitir a atribuição de direitos de acesso por meio do A.D.

O processo para gerenciar o identificador de usuário (ID de usuário) inclui:

a) o uso de um ID de usuário único;

b) a imediata remoção ou desabilitação do ID de usuário que tenha deixado a organização;

c) a remoção e identificação, de forma periódica, ou a desabilitação de usuários redundantes com ID;

d) a garantia de que o ID de usuário redundante não é emitido para outros usuários;

5.8.2 Provisionamento para acesso de usuário

Um processo formal de provisionamento de acesso do usuário é implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços por meio do A.D.

5.8.3 Gerenciamento de direitos de acesso privilegiados

O direito de acesso privilegiado é restrito ao coordenador de T.I. com usuário específico.

5.8.4 Gerenciamento da informação de autenticação secreta de usuários

A concessão de informação de autenticação secreta inclua os seguintes requisitos:

a) O usuário declara por meio desta política a manter a confidencialidade da informação de autenticação secreta e manter as senhas de grupos de trabalho, exclusivamente com os membros do grupo.

b) garantir, onde os usuários necessitam manter suas próprias informações de autenticação secreta, que lhes sejam fornecidas uma informação de autenticação secreta temporária, as quais o usuário é obrigado a alterá-la no primeiro uso;

c) fornecer informação de autenticação secreta temporárias aos usuários de maneira segura;

d) Informação de autenticação secreta temporária seja única para uma pessoa e que não seja fácil de ser adivinhada;

5.8.5 Análise crítica dos direitos de acesso de usuário

Os proprietários de ativos analisem criticamente os direitos de acesso dos usuários semestralmente.

5.8.6 Retirada ou ajuste de direitos de acesso

Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação devem ser retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.

5.9 Responsabilidades dos usuários

Objetivo: Tornar os usuários responsáveis pela proteção das suas informações de autenticação

5.9.1 Uso da informação de autenticação secreta

Os usuários são orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta:

a) manter a confidencialidade da informação de autenticação secreta, garantindo que ela não é divulgada para quaisquer outras partes, incluindo autoridades e lideranças;

b) evitar manter anotadas a informação de autenticação secreta (por exemplo, papel, arquivos ou dispositivos móveis).

c) alterar a informação de autenticação secreta, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

d) Quando as senhas são usadas como informação de autenticação secreta, selecione senhas de qualidade com um tamanho mínimo que sejam:

1) fáceis de lembrar;

2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;

3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras incluídas no dicionário);

4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;

5) Conter no mínimo 08 caracteres, incluindo letras maiúsculas e minúsculas, assim como números e caracteres especiais.

e) não compartilhar a informação de autenticação secreta de usuários individuais;

f) não utilizar a mesma informação de autenticação secreta para uso com finalidades profissionais e pessoais.

5.10 Controle de acesso ao sistema e à aplicação

Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.

5.10.1Restrição de acesso à informação

O acesso à informação e às funções dos sistemas de aplicações é restrito, de acordo com a política de controle de acesso.

As restrições para o acesso são baseadas nos requisitos das aplicações individuais do negócio e de acordo com a política de controle de acesso definida.

Os seguintes controles são considerados de forma a apoiar os requisitos de restrição de acesso:

a) fornecer *menus* para controlar o acesso às funções dos sistemas de aplicação;

b) controlar quais dados podem ser acessados por um usuário em particular;

c) controlar os direitos de acesso dos usuários, por exemplo, ler, escrever, excluir e executar;

5.10.2 Procedimentos seguros de entrada no sistema (log-on)

Técnicas de autenticação adequada são escolhidas para validar a identificação alegada de um usuário.

O procedimento para entrada no sistema operacional é configurado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada (*log-on*) revele o mínimo de informações sobre o sistema ou aplicação, de forma a evitar o fornecimento de informações desnecessárias a um usuário não autorizado.

Convém que a entrada no sistema (*log-on*):

a) mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados;

b) não forneça mensagens de ajuda durante o procedimento de entrada (*log-on*) que poderiam auxiliar um usuário não autorizado;

c) proteja contra tentativas forçadas de entrada no sistema (*log-on*);

d) registre tentativas de acesso ao sistema, sem sucesso e bem sucedida por meio do graylog;

e) mostre as seguintes informações quando o procedimento de entrada no sistema (*log-on*) finalizar com sucesso:

1) data e hora da última entrada no sistema (*log-on*) com sucesso;

2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (*log-on*) desde o último acesso com sucesso;

f) não mostre a senha que está sendo informada;

5.10.3 Sistema de gerenciamento de senha

O sistema de gerenciamento de senha:

a) obrigue o uso individual de ID de usuário e senha para manter responsabilidades;

b) permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

c) obrigue a escolha de senhas de qualidade (Conter no mínimo 08 caracteres, incluindo letras maiúsculas e minúsculas, assim como números e caracteres especiais);

d) obrigue os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema;

e) force as mudanças de senha a intervalos regulares (trimestral).

f) mantenha um registro das senhas anteriores utilizadas e bloquei a reutilização;

g) não mostre as senhas na tela quando forem digitadas;

h) armazene os arquivos de senha separadamente dos dados do sistema da aplicação;

i) armazene e transmita as senhas de forma protegida.

5.10.4 Uso de programas utilitários privilegiados

O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações é uso restrito do coordenador de T.I.

5.10.5 Controle de acesso ao código-fonte de programas

O acesso ao código-fonte do programa Autorizador on-line é restrito ao coordenador de T.I.

É conveniente que as seguintes orientações sejam consideradas para o controle de acesso às bibliotecas de programa-fonte, com a finalidade de reduzir o risco de corrupção de programas de computador:

a) convém que o pessoal de suporte não tenha acesso irrestrito às bibliotecas de programa-fonte;

b) convém que a atualização das bibliotecas de programa-fonte e itens associados, e a entrega de fontes de programas a programadores seja apenas efetuada após o recebimento da autorização pertinente;

c) convém que a manutenção e a cópia das bibliotecas de programa-fonte estejam sujeitas a procedimentos estritos de controles de mudanças.

5.11 CRIPTOGRAFIA

5.11.1Controles criptográficos

Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

5.11.1a Política para uso de controles criptográficos

Controles criptográficos são utilizados em:

Aplicações Web, armazenamento do banco de dados.

5.11.1b Gerenciamento de chaves

Aplicações Web: Certificado SSL com ciclo de vida anual e renovação automática.

Banco de dados: Aplicação do banco.

5.12 SEGURANÇA FÍSICA E DO AMBIENTE

5.12.1 Áreas seguras

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

5.12.1Perímetro de segurança física

As seguintes diretrizes são consideradas e implementadas, onde apropriado, para os perímetros de segurança física:

a) o perímetro de segurança se dá pela entrada lateral chaveada e monitorada por câmera;

b) após acesso à entrada lateral, o acesso às dependências da Unimed se dá por outra porta chaveada;

c) o acesso físico às dependências da Unimed é controlado por meio de visualização da câmera, liberação e recepção da pessoa por parte de um colaborador Unimed;

d) os sistemas de detecção de intrusos são monitorados por meio de câmera de acordo com normas regionais e a organização possui sistema de alarme;

5.12.1. Controle de entrada física

As seguintes diretrizes são implementadas:

a) A data e hora da entrada e saída de visitantes são registradas na planilha [controle de visitantes.xlsx], e todos os visitantes são supervisionados durante a permanência na Unimed;

b) Uma trilha de auditoria eletrônica de todos os acessos é mantida e monitorada de forma segura;

c) é exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, se identifiquem por meio de crachá;

5.12.1 Segurança em escritórios, salas e instalações

As seguintes diretrizes são implementadas para proteger escritórios, salas e instalações:

a) o acesso público não controlado se dá somente pela recepção;

b) o controle de acesso às instalações da Unimed é realizado por portão e porta lateral;

5.12.1 Proteção contra ameaças externas e do meio-ambiente

A organização possui proteções contra ameaças externas e do meio-ambiente conforme previsto no AVCB.

11.1.1) **Trabalhando em áreas seguras**

A sala de reunião da diretoria é considerada uma sala segura:

a) Não é permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

11.1.2) **Áreas de entrega e de carregamento**

São consideração as seguintes diretrizes:

a) o acesso a área de entrega e carregamento a partir do exterior do prédio é restrito ao pessoal identificado e autorizado;

b) as áreas de entrega e carregamento é projetada de tal maneira que é possível carregar e descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício;

c) as portas externas da área de entrega e carregamento são trancadas enquanto não estiverem sendo realizado entrega e carregamento;

5.13 Equipamentos

Objetivo: Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.

5.13.1Escolha do local e proteção do equipamento

Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.

As seguintes considerações devem ser seguidas para proteger os equipamentos:

a) convém que os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;

b) convém que as instalações de processamento da informação que manuseiam dados sensíveis sejam posicionadas cuidadosamente para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização;

c) convém que as instalações de armazenagem sejam protegidas de forma segura para evitar acesso não autorizado;

d) convém que os itens que exigem proteção especial sejam protegidos para reduzir o nível geral de proteção necessário;

e) convém que sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

f) convém que alimentos e bebidas sejam consumidos na cozinha da organização.

g) convém que as condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação;

h) convém que todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

5.13.2 Utilidades

Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades por meio de nobreaks nos equipamentos essenciais.

5.13.3 Segurança do cabeamento

O cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações é protegido contra interceptação, interferência ou danos.

5.13.4 Manutenção dos equipamentos

Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.

Convém que sejam levadas em consideração as seguintes diretrizes para a manutenção dos equipamentos:

a) convém que a manutenção dos equipamentos seja realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

b) convém que a manutenção e os consertos dos equipamentos só sejam realizados por pessoal de manutenção autorizado;

c) convém que sejam mantidos registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas por meio do formulário [FOR-21 Registro de operações];

d) antes de colocar o equipamento em operação, após a sua manutenção, convém que ele seja inspecionado para garantir que o equipamento não foi alterado indevidamente e que não está em mau funcionamento.

5.13.5 Remoção de ativos

Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

A remoção de ativos deve ser registrada por meio de planilha FOR-08-Controle de remoção de ativos.

5.13.6 Segurança de equipamentos e ativos fora das dependências da organização

Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

Convém que o uso de qualquer equipamento de processamento e armazenamento de informações fora das dependências da organização seja autorizado pela gerência. Isto se aplica aos próprios equipamentos da organização e aos equipamentos pessoais, usados em nome da organização.

5.13.7 Reutilização e alienação segura de equipamentos

Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre-gravados com segurança, antes do descarte ou do seu uso.

5.13.8 Equipamento de usuário sem monitoração

Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

Convém que todos os usuários estejam cientes dos requisitos de segurança da informação e procedimentos para proteger equipamentos desacompanhados, assim como suas responsabilidades por implementar estas proteções.

Convém que os usuários sejam informados para:

a) encerrar as sessões ativas, a menos que elas possam ser protegidas por meio de um mecanismo de bloqueio, por exemplo tela de proteção com senha;

b) proteger os computadores ou dispositivos móveis contra uso não autorizado através de tecla de bloqueio ou outro controle equivalente, por exemplo, senha de acesso, quando não estiver em uso.

5.13.9 Política de mesa limpa e tela limpa

É adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

5.14 SEGURANÇA NAS OPERAÇÕES

5.14.1 Responsabilidade e procedimentos operacionais

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

5.14.2 Documentação dos procedimentos de operação

Os procedimentos de operação são documentados e disponibilizados a todos os usuários que necessitem deles.

5.14.3 Gestão de mudanças

As mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, são controladas por meio do FORM 089 Solicitação de Mudanças.

5.14.4 Gestão de capacidade

A utilização dos recursos é monitorada e ajustada e as projeções são feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema por meio de Reunião de Análise Crítica.

5.14.5 Separação dos ambientes de desenvolvimento, teste e de produção

Os ambientes de desenvolvimento, teste e produção são separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

5.15 Proteção contra códigos maliciosos

Objetivo: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos.

12.2.1) **Controles contra códigos maliciosos**

É implementado controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário por meio de Antivirus Node 32 e Firewall Linux.

5.16 Cópias de segurança

Objetivo: Proteger contra a perda de dados.

5.16.1Cópias de segurança das informações

As cópias de segurança das informações, softwares e das imagens do sistema, são efetuadas e testadas regularmente conforme: a política de geração de cópias de segurança definida.

5.17 Registro e monitoramento

Objetivo: Registrar eventos e gerar evidências.

5.17.1Registro de eventos

Os registros *(log*) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da

informação são produzidos, mantidos e analisados criticamente, a intervalos regulares por meio do Graylog.

5.17.2Proteção das informações dos registros de eventos (logs)

As informações dos registros de eventos (log) e seus recursos são protegidas contra acesso não autorizado e adulteração por meio de senha de usuários.

5.17.3Registros de eventos (log) de administrador e operador

As atividades dos administradores e operadores do sistema são registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares por meio do Graylog.

5.17.4Sincronização dos relógios

Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, são sincronizados com uma única fonte de tempo precisa GMT-3 por meio de fonte pública a.ntp.br

5.18 Controle de software operacional

Objetivo: Assegurar a integridade dos sistemas operacionais.

5.18.1Instalação de software nos sistemas operacionais

A instalação de software em sistemas operacionais é controlado por meio de acesso administrador somente ao processo de T.I.

5.19 Gestão de vulnerabilidades técnicas

Objetivo: Prevenir a exploração de vulnerabilidades técnicas.

5.19.1Gestão de vulnerabilidades técnicas

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

5.19.2Restrições quanto à instalação de software

A restrição quanto à instalação de software segue a seguinte sistemática:

A. software não legalizado (pirata)

B. camada de Interação com comunicadores

C. softwares para uso particulares

5.20 Considerações quanto à auditoria de sistemas de informação

Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

5.20.1 Controle de auditoria de sistemas de informação

Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais são cuidadosamente planejados e acordados para minimizar a interrupção dos processos do negócio por meio do active directory, ocs, graylog, openvas, planilha de gestão de capacidade, análise crítica e auditoria interna.

5.21 SEGURANÇA NAS COMUNICAÇÕES

5.21.1 Gerenciamento da segurança em redes

Objetivo: Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

5.21.2 Controles de redes

As redes são gerenciadas e controladas para proteger as informações nos sistemas e aplicações por meio do AD e segregação de grupos de redes.

5.21.3 Segurança dos serviços de rede

Os mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, são identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados por meio do firewall.

5.21.4 Segregação de redes

Os grupos de serviços de informação, usuários e sistemas de informação são segregados em redes por meio do firewall e grupos do active directory.

5.22 Transferência de informação

Objetivo: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

5.22.1 Políticas e procedimentos para transferência de informação

Políticas, procedimentos e controles de transferências formais, são estabelecidos para proteger a transferência de informações, por meio de:

• comunicação interna ou externa obrigatoriamente por email ou teams (não permissível por outros aplicativos de mensagens instantâneas);

• as mensagens de email, incluindo seus anexos, são protegidas contra códigos maliciosos por meio de antivírus;
• não utilização do email corporativo para uso pessoal;
• documentação física é protegida por meio de envelope;
• a utilização do pendrive é proibido se não for autorizado pelo T.I;

5.22.2 Acordos para transferência de informações

As transferências de informações são restritas a informações do negócio entre a organização e também partes externas. Não é permitida a transmissão de informações pessoais e sensíveis não destinadas ao negócio.

5.22.3 Mensagens eletrônicas

As informações que trafegam em mensagens eletrônicas são adequadamente protegidas por meio de E-mail, WhatsApp e Skype.

5.22.4 Acordos de confidencialidade e não divulgação

Controle

Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.

Diretrizes para implementação

Convém que os acordos de confidencialidade e de não divulgação considerem os requisitos para proteger as informações confidenciais, usando termos que são obrigados do ponto de vista legal. Acordos de confidencialidade ou não divulgação são aplicáveis as partes externas ou aos funcionários da organização.

Convém que os elementos sejam selecionados ou acrescentados considerando-se o tipo do acesso permitido para a outra parte, ou para o tratamento da informação confidencial. Para identificar os requisitos para os acordos de confidencialidade ou de não divulgação, convém que os seguintes elementos sejam considerados:

a) uma definição da informação a ser protegida (por exemplo, informação confidencial);
b) o tempo de duração esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;
c) ações requeridas quando um acordo está encerrado;
d) responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação;

e) o proprietário da informação, segredos comerciais e de propriedade intelectual, e como isto se relaciona com a proteção da informação confidencial;

f) o uso permitido da informação confidencial, e os direitos do signatário para usar a informação;

g) o direito de auditar e monitorar as atividades que envolvem as informações confidenciais;

h) o processo para notificação e relato de divulgação não autorizada ou vazamento das informações confidenciais;

i) termos para a informação ser retornada ou destruída quando do término do acordo;

j) ações esperadas a serem tomadas no caso de uma violação deste acordo.

Baseado nos requisitos de segurança da informação da organização, outros elementos podem ser necessários em um acordo de confidencialidade ou de não divulgação.

Convém que os acordos de confidencialidade e de não divulgação estejam em conformidade com todas as leis e regulamentações aplicáveis na jurisdição para a qual eles se aplicam (ver 18.1).

Convém que os requisitos para os acordos de confidencialidade e de não divulgação, sejam analisados criticamente de forma periódica e quando mudanças ocorrerem que influenciem estes requisitos.

Informações adicionais

Acordos de confidencialidade e de não divulgação protegem as informações da organização e informam aos signatários das suas responsabilidades, para proteger, usar e divulgar a informação de maneira responsável e autorizada.

Pode haver uma necessidade de uma organização usar diferentes formas de acordos de confidencialidade ou de não divulgação, em diferentes circunstâncias.

5.23 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Requisitos de segurança de sistemas de informação

Objetivo: Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

5.23.1 Análise e especificação dos requisitos de segurança da informação

Os requisitos relacionados com segurança da informação são incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes por meio do planejamento de mudanças.

5.23.2 Serviços de aplicação seguros em redes públicas

As informações envolvidas nos serviços de aplicação que transitam sobre redes públicas são protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não

autorizadas por meio de certificado de segurança SSL, e também usuário e senha forte para acesso.

5.23.3 Protegendo as transações nos aplicativos de serviços

As informações envolvidas em transações nos aplicativos de serviços são protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada, quando aplicável, por meio de:

a) o uso de assinaturas eletrônicas para cada uma das partes envolvidas na transação;

b) todos os aspectos da transação, ou seja, garantindo que:

1) informação de autenticação secreta de usuário são válidas e verificadas para todas as partes;
2) a transação permaneça confidencial;
3) a privacidade de todas as partes envolvidas seja mantida;

c) o caminho de comunicação entre todas as partes envolvidas é criptografado;

d) protocolos usados para comunicações entre todas as partes envolvidas é seguro;

5.24 Segurança em processos de desenvolvimento e de suporte

Objetivo: Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação.

5.24.1 Política de desenvolvimento seguro

Políticas seguras de desenvolvimento de sistemas e *software* são estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização por meio de:

a) segurança do ambiente de desenvolvimento por meio de segregação de pasta e código; teste de intrusão nas aplicações desenvolvidas.

5.24.2 Procedimento para controle de mudanças de sistemas

As mudanças em sistemas no ciclo de vida de desenvolvimento são controladas utilizando registro de controle de versão.

5.24.3 Análise crítica técnica das aplicações após mudanças nas plataformas operacionais

Quando plataformas operacionais forem modificadas, as aplicações críticas de negócio são analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.

5.24.4 Restrições sobre mudanças em pacotes de Software

As modificações em pacotes de *software* são desencorajadas e são limitadas às mudanças necessárias, e todas as mudanças são estritamente controladas.

5.24.5 Princípios para projetar sistemas seguros

Princípios para projetar sistemas seguros são estabelecidos, documentados, mantidos e aplicados por meios de ferramentas de segurança e validados por teste de intrusão.

5.24.6 Ambiente seguro para desenvolvimento

A organização estabelece e protege adequadamente ambientes de desenvolvimento por meio de acesso ao Coordenador de T.I.

5.24.7 Desenvolvimento terceirizado

Não há desenvolvimento terceirizado.

5.24.8 Teste de segurança do sistema

Testes de segurança do sistema são realizados por meio de testes de intrusão.

5.24.9 Teste de aceitação de sistema

Programas de testes de aceitação e critérios relacionados são estabelecidos para novos sistemas de informação, atualizações e novas versões nas plataformas operacionais.

5.25 Dados para teste

Objetivo: Assegurar a proteção dos dados usados para teste.

5.25.1 Proteção dos dados para teste

Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados por meio de criptografia.

5.26 RELACIONAMENTO NA CADEIA DE SUPRIMENTO

5.26.1Segurança da informação na cadeia de suprimento

Objetivo: Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.

5.26.2 Política de segurança da informação no relacionamento com os fornecedores

Os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização são acordados com o fornecedor e documentados por meio

de contratos ou aditivos.

5.26.3 Identificando segurança da informação nos acordos com fornecedores

Todos os requisitos de segurança da informação relevantes são estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização por meio de contratos ou aditivos.

5.26.4 Cadeia de suprimento na tecnologia da comunicação e informação

Acordos com fornecedores incluem requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação por meio de contrato ou aditivos.

5.27 Gerenciamento da entrega do serviço do fornecedor

Objetivo: Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

5.27.1 Monitoramento e análise crítica de serviços com fornecedores

A organização monitora, analisar criticamente e audita, a intervalos regulares, a entrega dos serviços executados pelos fornecedores por meio de planilha [FOR-23-IQF.xlsx].

5.27.2 Gerenciamento de mudanças para serviços com fornecedores

As mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, são gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação de riscos por meio de informação documentada.

5.28 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.28.1 Gestão de incidente de segurança da e melhorias

Objetivo: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

5.28.2 Responsabilidades e procedimentos

As responsabilidades e procedimentos de gestão são estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidente de segurança da informação. O detalhamento dos processos estão descritos nos requisitos 16.1.2 a 16.1.7.

5.28.3 Notificação de eventos de segurança da segurança

Os eventos de segurança da informação são relatados através dos canais apropriados da direção, o mais rapidamente possível por meio do formulário Comunicação Anônima.

Situações a serem consideradas para notificar um evento de segurança da informação incluem:

a) controle de segurança ineficaz;

b) violação da disponibilidade, confidencialidade e integridade da informação;

c) erros humanos;

d) não-conformidade com políticas ou diretrizes;

e) violações de procedimentos de segurança física;

f) mudanças descontroladas de sistemas;

g) mau funcionamento de *software* ou *hardware*;

h) violação de acesso.

5.28.4 Notificando fragilidades de segurança da informação

Os funcionários que usam os sistemas e serviços de informação da organização, são instruídos a registrar e notificar quaisquer fragilidades de segurança da informação suspeita ou observada, nos sistemas ou serviços por meio do formulário Comunicação Anônima.

5.28.5 Avaliação e decisão dos eventos de segurança da informação

Os eventos de segurança da informação são avaliados e é decidido se eles são classificados como incidentes de segurança da informação por meio do PMC.

5.28.6 Resposta aos incidentes de segurança da informação

Os incidentes de segurança da informação são reportados para as partes envolvidas e partes legais.

5.28.7 Aprendendo com os incidentes de segurança da informação

Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação são usados para reduzir a probabilidade ou o impacto de incidentes futuros observando a extensão dos processos por meio do PMC.

5.28.8 Coleta de evidências

A organização identifica coleta, adquire e preserva as informações, as quais podem servir como evidências.

Os procedimentos para evidência fornecem processos de identificação, coleta, aquisição e preservação de evidências, de acordo com diferentes tipos de mídia, dispositivos e situação dos dispositivos, por exemplo, se estão ligados ou desligados. Convém que os procedimentos levem em

conta:

a) a cadeia de custódia;

b) a segurança da evidência;

c) a segurança das pessoas;

d) papéis e responsabilidades das pessoas envolvidas;

e) competência do pessoal;

f) documentação;

g) resumo do incidente.

5.30 ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

5.30.1Continuidade da segurança da informação

Objetivo: É recomendado que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização.

5.30.2 Planejando a continuidade da segurança da informação

A organização determina seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, durante uma crise ou desastre por meio de um plano de continuidade dos negócios.

5.30.3 Implementando a continuidade da segurança da informação

A organização estabelece, documenta, implementa e mantém processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa por meio do PMC conforme estabelecido no plano de continuidade de negócios.

5.30.4 Verificação, análise crítica e avaliação da continuidade da segurança da informação.

A organização verifica os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalo semestral, para garantir que eles são válidos e eficazes em situações adversas por meio do plano de continuidade de negócios.

5.31 Redundância

Objetivo: Assegurar a disponibilidade dos recursos de processamento da informação.

5.31.1Disponibilidade dos recursos de processamento da informação

Os recursos de processamento da informação são implementados com redundância suficiente para atender aos requisitos de disponibilidade.

5.32 CONFORMIDADE

5.32.1 Conformidade com requisitos legais e contratuais

Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

5.32.2 Identificação da legislação aplicável e de requisitos contratuais

Todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, são explicitamente identificados, documentados e mantidos atualizados por meio do processo legal, administrativo, tecnologia e recursos humanos

5.32.3 Direitos de propriedade intelectual

A organização segue a legislação de propriedade intelectual sobre o uso de produtos de *software* proprietários.

5.32.4 Proteção de registros

Os registros são protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

5.32.5 Proteção e privacidade de informação de identificação pessoal

A privacidade e a proteção das informações de identificação pessoal são asseguradas conforme requerido por legislação.

5.32.6Regulamentação de controles de criptografia

Controles de criptografia são usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

5.33 Análise crítica de segurança da informação

Objetivo: Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.

18.2.1) Análise crítica independente da segurança da informação

O sistema de gestão da segurança da informação é analisado criticamente, de forma independente, anualmente, ou quando ocorrerem mudanças significativas.

18.2.2) Conformidade com as políticas e procedimentos de segurança da informação

Os gestores analisam criticamente, semestralmente, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

18.2.3) Análise crítica da conformidade técnica

Os sistemas de informação são analisados criticamente, anualmente, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

6. MONITORAMENTO

Notificações no Quallix qualquer situações de riscos a segurança da informação.

7. DISTRIBUIÇÃO DE CÓPIAS

Não aplicável.

8. REGISTROS

ISO 9001.

ISO 27001.

ISO 27002.

LEI 13.709/2018.

Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

9. ANEXOS

Não aplicável.

10. REFERÊNCIAS

BRASIL. Programa de integridade. Diretrizes para empresas privadas. Controladoria Geral da União (CGU), Brasília, DF. Disponível em < http://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa- deintegridade-diretrizes-para-empresas-privadas.pdf >.

Políticas Corporativas Unimed Belo Horizonte. Disponível em: https://portal.unimedbh.com.br/wps/portal/inicio/home/conheca_a_unimed/governanca/politicascorporativas . Acessado em 15/10/2018

Unimed Tupã	**POLÍTICA**	Código: POL_TI_018
		Data de Emissão: 01/02/2023
	SEGURANÇA DA INFORMAÇÃO	Data da Revisão: 01/02/2024
		Revisão Nº:

André Gustavo Bisi Gerente de TI	**Roberta S. Boaventura** Analista da Qualidade	**Ana Paula A. A. Pereira** Gerente