Etapas	Responsáveis	Função
Elaboração	André Ciriaco	Coordenador de TI
Verificação	Thais Xavier	Consultoria DUO
	Gabriella Soares Teixeira	Analista da Qualidade
	Maria de Fátima Fiorino Biancardi	Diretora Administrativa
Validação	Kelin C. Bock Hummes	Gerente de Qualidade

1 OBJETIVO

Orientar e estabelecer as diretrizes corporativas da Fundação Beneficente Rio Doce para proteção dos ativos de informação, além da prevenção de responsabilidade legal para todos os usuários. Desta forma, deve ser aplicada e cumprida em todas as áreas da empresa. A gestão da segurança da informação é baseada nas premissas da confidencialidade, integridade, disponibilidade e autenticidade, conforme definido na norma ISO/IEC 17799:2005. Toma como base a LGPD – Lei Geral de Proteção de Dados - Lei nº 13.709, de 14 de agosto de 2018.

2 APLICAÇÃO

As diretrizes estabelecidas deverão ser seguidas por todos os colaboradores independente a posição dentro da instituição (estratégico, tático ou operacional), bem como prestadores de serviço.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, equipamentos (computadores, impressoras, tabletes, celulares, notebooks) e redes da empresa poderão ser monitorados e gravados.

É também obrigação de cada colaborador se manter atualizado em relação a este documento e aos procedimentos e normas relacionadas, buscando orientação do Departamento da Tecnologia da Informação sempre que não estiver absolutamente seguro quanto ao uso de recurso, equipamentos e de informações.

3 DEFINIÇÕES

NA

4 DOCUMENTOS RELACIONADOS

FORM.RH.036: Termo de Compromisso Sigilo e Confidencialidade
FORM.TI.004: Termo de Responsabilidade para Uso de VPN
FORM.TI.001: Termo de Compromisso para Uso de Equipamentos
POP.TI.008: Orientações aos Usuários
RI.DIR.001: Regulamento Interno dos Colaboradores do Hospital Rio Doce

5 DESCRIÇÃO

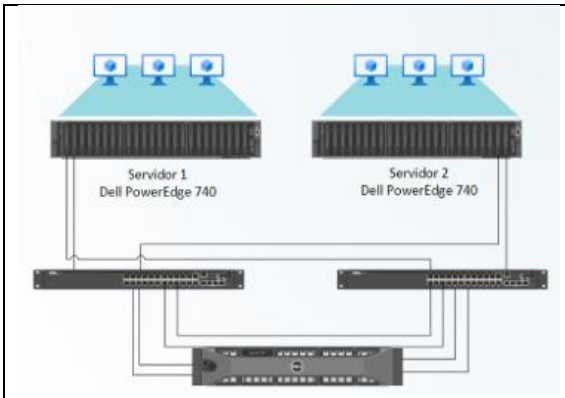
5.1 Responsabilidades

Setor	Responsabilidade
Diretoria	○ Determinar o nível de acesso de cada setor e seu coordenador; ○ Intervir na utilização indesejada de dados pessoais a qualquer momento; ○ Definir o DPO (*Data Protection Officer*), que será responsável pelos dados da empresa, e alterá-lo caso necessário;
Setor de Tecnologia da Informação	○ Garantir (Confidencialidade, Integridade e Disponibilidade); ○ Gerir e realizar manutenção dos equipamentos, rede e sistemas locais e na nuvem; ○ Garantir a segurança dos dados contra vazamentos e acessos indesejados; ○ Garantir o acesso e atualização dos dados armazenado nos sistemas; ○ Gerenciar as autorizações de cada colaborador ao sistema da empresa.
Setor de Departamento Pessoal	○ Manter os dados pessoais de cada funcionário sempre atualizados e resguardados; ○ Averiguar constantemente a necessidade e finalidade de cada informação; ○ Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política Interna da Tecnologia da Informação e o consentimento da cessão de dados pessoais, aplicando o termo de sigilo e confidencialidade; ○ Estabelecer junto ao Setor de tecnologia os requisitos mínimos de conhecimento em informática para contratação. ○ Solicitar o cancelamento imediato de funcionários desligados.
Colaboradores de Todos Departamentos	○ Seguir as diretrizes e normas estabelecidas pela política de segurança; ○ Aplicar os princípios da confidencialidade, disponibilidade e integridade dentro da Instituição, não importando o cargo ou setor que esteja atuando; ○ ***Aos Gestores de forma geral cabe ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;***

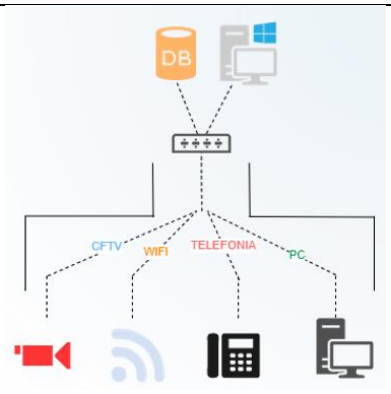
5.2 Estratégias de Segurança

5.2.1 Política de Infraestrutura de Servidores

- ✓ A rede tem o backbone todo de fibra óptica monomodo, saindo do datacenter de um switch core camada 3 (todo de fibra óptica) localizado no DataCenter, fazendo conexão com 6 concentradores de 44U e 17 racks de 14U. Todos os Switchs de borda são gerenciais camada 2;
- ✓ Existem 3 unidades fora do Hospital que são interconectadas com fibra apagada (fibras próprias, que só passam dados do hospital), essa metodologia se aplica garantindo maior segurança para os dados que trafegam;
- ✓ Os servidores são de grande porte, mantendo uma estrutura virtualizada;



Estrutura de Servidores e Switchs.



Estrutura de Trafego de Dados

5.2.2 Política de Acesso Físico ao Departamento de Tecnologia

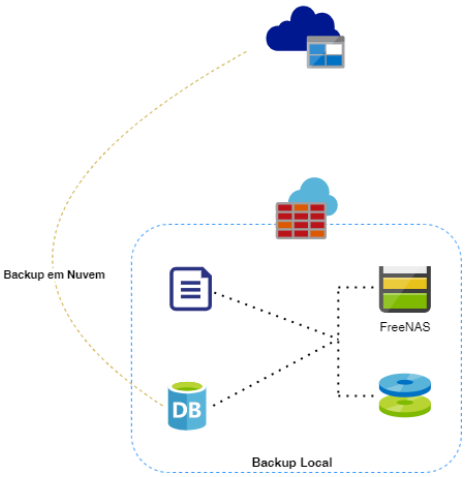
- O departamento de tecnologia da informação é um setor estratégico dentro da Fundação Beneficente Rio Doce;
- Como forma de bloqueio e acesso ao departamento existe uma porta com dupla proteção: **chave física e biométrica digital;**
- Só tem acesso ao departamento mediante posse da chave da porta e também com a liberação por biometria digital;

5.2.3 Política de Segurança contra falha Elétrica: Nobreak e Gerador

- A Fundação Beneficente Rio Doce possui 2 geradores elétricos que são acionados automaticamente mediante a falha de recebimento de energia da Distribuidora EDP;
- Em todos os armários e concentradores que alojam os switchs da rede existem Nobreak para resguardo da falha elétrica enquanto o Gerador assume a operação no caso da falta de energia;
- Dentro do Departamento de Tecnologia todos os servidores e switch core estão conectados num conjunto de nobreak (capacidade 1.4 VA). Estes nobreaks estão interligados a um banco de baterias (12v 60A), dando autonomia de 1h caso exista falha elétrica na rede e no gerador;

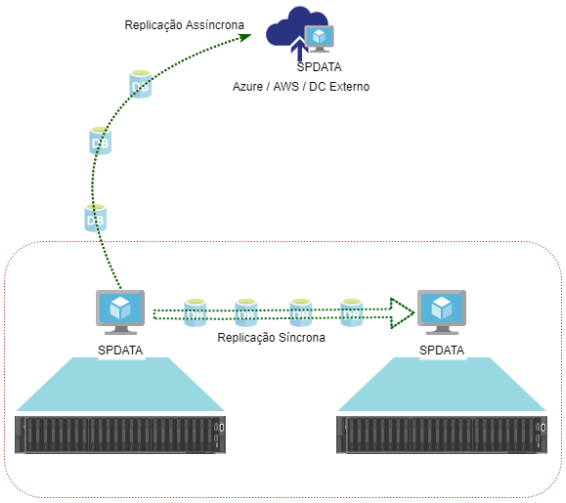
5.2.4 Política de Backup

- A estrutura de backup atual possui cópia local de arquivos e base de dados, além de uma cópia fora da estrutura (backup em nuvem);
- Sistemas hospedados na nuvem (Tasy e Effetivo) o backup é de responsabilidade dos prestadores contratados (Redix e Effetivo);
- Todas as cópias locais são enviadas para um disco externo (HD) e um Storage local (FreeNAS);
- Os envios feitos para a storage são criptografados com chave 256bits, garantindo integridade e Segurança em caso de vazamento das cópias;
- No servidor de arquivos é aplicada o recurso de shadow copy (cópia sombra realizada todos os dias às 12h), facilitando quando existe a necessidade de restaurar qualquer arquivo;



Estrutura de cópias de segurança

- Para segurança do banco de dados do Sistema (spdata), é utilizada de uma ferramenta para replicação síncrona (HQBird);
- O sistema faz a réplica do banco de dados, backups incrementais, backups diferenciais e restore de validação do backup;
- Existem 2 servidores, 1 de produção e outro de replicação;



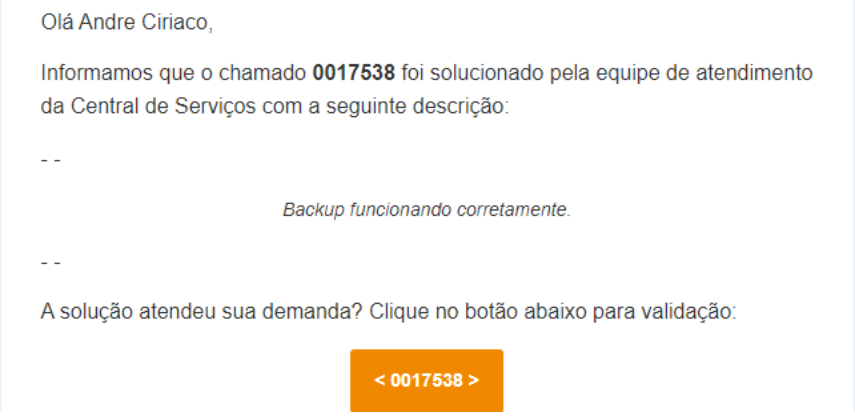
Estrutura de backup (spdata)

Rotina de Backup Nuvem

TAREFA	TIPO	HORÁRIO	RETENÇÃO
System State	Incremental	00:00	Limite de 30GB
System State (Azure)	Incremental	02:00	3 dias
Aplicações PULMAO03 (Azure - 12h30)	Incremental	12:30	3 dias
Dados (Local - BARRIGA04)	Incremental	19:00	30 dias
Athenas (Azure)	Incremental	19:40	3 dias
Athenas (Local)	Incremental	19:45	30 dias
Aplicações PULMAO03 (Local)	Incremental	19:30	30 dias

Aplicações PULMAO03 (Azure - 19h50)	Incremental	19:50	3 dias
TacticalRMM	Full	20:00	3 dias
TacticalRMM (Azure)	Incremental	21:00	3 dias

- Os backups de arquivos feitos pela empresa Linetwork e armazenados na Nuvem são validados todos os meses;
- Após a validação do restore do backup é enviado uma notificação por e-mail:


Olá Andre Ciriaco,

Informamos que o chamado **0017538** foi solucionado pela equipe de atendimento da Central de Serviços com a seguinte descrição:

- -

Backup funcionando corretamente.

- -

A solução atendeu sua demanda? Clique no botão abaixo para validação:

< 0017538 >

- O atual ERP Tasy fica hospedado na OCI da Oracle Cloud, seguindo todos protocolos Internacionais vigentes em relação a Data Center´s;
- Toda rotina de backup e validações é de responsabilidade da empresa Redix (*empresa homologada pela Philips para gestão do banco de dados na Oracle*)
- A rotina de backup é:

RMAN_CLOUD_ARCH	Backup dos logs (archive logs) do banco. É o backup das últimas alterações que ocorreram. (Todo dia cada 30 minutos)
RMAN_CLOUD_FULL_INC	Backup incremental completo. É o backup completo de todo o banco de dados. (Sábado as 01:00)
RMAN_CLOUD_FULL_INC_C	Backup incremental cumulativo. É o backup das modificações que contém tudo o que foi alterado desde o último backup completo. (Quarta as 01:00)
RAMN_CLOUD_FULL_INC_D	Backup incremental diferencial. É o backup que contém todas as modificações desde o último backup incremental. (Dom, Seg, Ter, Qui, Sex as 01:00)

5.2.5 Política de Aplicação do Termo De Sigilo e Confidencialidade

- A Fundação Beneficente Rio Doce possui seu termo de sigilo e confidencialidade alinhado com a política de segurança da informação e estratégica do negócio;
- O termo de sigilo e confidencialidade é identificado pelo formulário FORM.RH.036, com sua aplicação feita pelo departamento de Recursos Humanos no ato da formalização contratual do funcionário;
- O termo de sigilo e confidencialidade fica armazenado na pasta do funcionário no departamento de Recursos Humanos;
- Como premissa da Segurança da Informação todo funcionário ao ser aprovado no processo de recrutamento e seleção passa por uma orientação do coordenador de tecnologia da informação, conforme POP.TI.008;

- O novo colaborador tem como pré-requisito a liberação de acesso aos sistemas um treinamento introdutório à Lei Geral de Proteção de Dados na plataforma online PROTEGON;

5.2.6 Gestão de Acesso (Inclusão, Alterações e Cancelamento de Usuários)

- A gestão de acesso é essencial para garantir a segurança e integridade dos sistemas de uma organização, controlando quem tem acesso a quais recursos. Essa prática abrange desde a inclusão inicial de usuários até a manutenção de seus acessos ao longo do tempo e, eventualmente, o cancelamento quando necessário;
- Inclusão de Usuários: Ao integrar novos membros à organização, é crucial coletar informações básicas para identificação, atribuir cargos e departamentos;
- Autenticação e Autorização: Estabelecer políticas robustas de senha e definir permissões específicas garantindo que tenham acesso aos recursos, fortalecendo a segurança do sistema;
- Alterações de Acesso: Manter as informações dos usuários atualizadas para garantir que os dados de contato e as atribuições de cargo estejam sempre precisos, facilitando a comunicação e a gestão interna;
- Avaliação de Necessidades de Acesso: Reavaliar regularmente as necessidades de acesso dos usuários para garantir as permissões apropriadas para desempenhar suas funções, evitando excessos ou deficiências de acesso.
- Cancelamento de Acesso: Cancelamento dos funcionários desligados. Agir rapidamente para desativar contas ao detectar desligamentos ou situações de risco minimiza a exposição a possíveis vulnerabilidades para manter a segurança do sistema e dados.
- Auditoria Pós-Cancelamento: Realizar auditorias após o cancelamento para assegurar que todas as permissões foram revogadas corretamente. Auxiliar na identificação de possíveis atividades suspeitas após o desligamento do usuário.

5.2.7 Política de Senhas

- A senha é a segurança eletrônica do usuário. Desta forma, ela nunca deverá ser revelada a ninguém, nem mesmo a equipe de TI;
- A senha é secreta, tudo que for executado será de inteira responsabilidade do usuário, por isso, deve ser tomada todas as precauções possíveis;
- A periodicidade máxima para troca das senhas é 180 dias, não podendo ser repetida as 5 últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 180 dias. Os sistemas irão forçar a troca das senhas dentro desse prazo máximo;
- Na desconfiança de algum procedimento, ou acreditar que não esteja mais seguro, o usuário deve modificar sua senha imediatamente.

5.2.8 Política de Uso de E-MAIL

- Não utilizar o e-mail da empresa para assuntos pessoais;
- Utilizar linguagem culta, polida e formal nas mensagens, sendo vedado o uso de gírias e palavreado inapropriado;
- Identificar-se devidamente em todos os e-mails que enviar. Utilizar sempre a assinatura, no modelo corporativo, para troca de e-mails;
- Nunca baixar arquivos e nem executar anexos que tenha recebido de endereços suspeitos ou que não tenha certeza do que se trata;
- Sempre que receber e-mail com material indevido ou impróprio ao ambiente de trabalho, comunicar imediatamente à gerência de TI;

- Desconfiar de e-mails com remetentes, assuntos suspeitos e/ou domínio do endereço, realizando o bloqueio. Nunca será solicitado que realize pagamentos ou forneça dados pessoais, não repassar informações duvidosas.

5.2.9 Política de Uso de INTERNET

- É estritamente proibido o uso da internet para realização de atividades que não sejam destinadas a função que esteja exercendo e/ou pessoais;
- Visitar sites da Internet que contenham material obsceno e/ou pornográfico;
- Usar a Internet para criar e/ou enviar material ofensivo, calunioso difamatório e/ou de assédio para outros usuários;
- Baixar (download) software comercial ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licença;
- Baixar ou acessar qualquer programa ou plataforma de comunicação, bate-papo online ou rede social, para fins pessoais, exemplos: Facebook, Instagram, Gmail;
- Invadir áreas em qualquer âmbito da internet, assim como efetuar buscas por documentações que não sejam de sua competência;
- Introduzir, de qualquer forma, vírus eletrônico de computador dentro da rede corporativa.

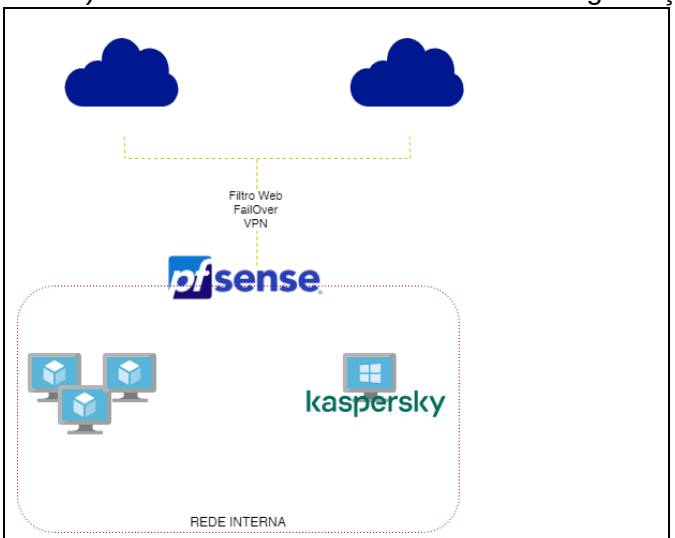
5.2.10 Política de Uso de Equipamentos

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido;
- Não é permitido que se faça nenhum tipo de compartilhamento em estações de trabalho: Impressoras, pastas ou quaisquer outros recursos da estação;
- Todos os dados gerados nos equipamentos devem ser gravados (armazenados) no servidor. Todo e qualquer arquivos salvo no computador não fará parte do backup de segurança;
- Notebook´s e celulares para uso em Home Office, atividades de Coordenação, Supervisão e Direção é aplicado o formulário FORM.TI.001. O documento é arquivado na pasta do funcionário no departamento de Recursos Humanos;
- Na devolução de Notebook´s e celulares por não mais necessidade de uso, encerramento de contrato, mudança de atribuição do cargo é aplicado o formulário FORM.TI.001. O documento é arquivado na pasta do funcionário no departamento de Recursos Humanos;

5.2.11 Política de Uso de FIREWALL

- Ambiente conta com um appliance de borda com Sistema PfSense embarcado;
- A técnica aplicada para segurança é bloquear todos os acessos e liberar o que é solicitado, sendo a liberação feita por grupos;
- As premissas de acessos são baseadas na integração do Sistema PfSence com o Active Diretory, onde todos os usuários possuem GRUPOS, USUÁRIOS E SENHAS;
- O Firewall de borda faz o balanceamento de 3 links de internet de operadoras distintas, dessa forma caso exista falha em 1 os demais já assumem a operação;
- A liberações e parametrizações são realizados somente pelos analistas internos da equipe de tecnologia da informação (Nível 2), mas caso existam falhas e desafios maiores existe uma empresa prestadora de serviço (Nível 3);

– A empresa prestadora (Nível 3) faz o monitoramento constante de segurança no firewall de borda;



Estrutura de segurança: Firewall e Antivirus

5.2.12 Política de Uso de ANTIVIRUS

– Todas estações de trabalho (computadores \ notebooks) pertencente a Fundação Beneficente Rio Doce é monitorada por um Sistema de Antivírus (kaspersky);
– As atualizações do Sistema Antivírus são automáticas, não sendo necessária a intervenção do usuário;
– O Sistema Antivírus possuir bloqueios de: PenDrive, CD, Vírus de todas as classificações, certificados web indevidos, baixar arquivos, sites indevidos);
– Caso seja detectado algum vírus ou malware pelo sistema, deverá entrar em contato com o suporte no mesmo instante para evitar possíveis danos.

5.2.13 Política de Uso de VPN

– O objetivo geral e os propósitos do uso da VPN na organização é garantir acesso remoto seguro aos recursos da empresa, proteger a privacidade dos dados;
– A política é aplicada aos funcionários em tempo integral, contratados, terceiros ou parceiros;
– A VPN só deve ser usada em dispositivos corporativos seguros;
– Para uso de VPN em equipamentos que não sejam do Hospital Rio Doce é necessário:
– Liberação formal da Direção;
– Validação técnica do Departamento de Tecnologia do Hospital no que diz respeito a configurações mínimas, existência de antivírus;
– Assinatura do formulário FORM.TI.007_TERMO DE RESPONSABILIDADE PARA USO DE VPN;
– Proíba o uso da VPN em locais públicos não seguros;
– É proibido compartilhar credenciais da VPN, é OBRIGATÓRIO uso de autenticação de dois fatores USUÁRIO E SENHA;
– As senhas devem ser complexas que incluam letras maiúsculas, minúsculas, números e caracteres especiais, com comprimento mínimo de 8 dígitos;

5.2.14 Política de Uso e Acesso ao Sistema ERP Tasy

a) Responsabilidade do Coordenador do Setor:

O coordenador do setor é responsável por garantir a correta implementação e aderência à política de segurança da informação no acesso ao Sistema ERP Tasy. Isso inclui a supervisão da distribuição

de responsabilidades, treinamento contínuo da equipe e a manutenção de práticas que assegurem a segurança da informação.

b) Integração de Serviços:

A integração de serviços deve ser realizada com o máximo de segurança, garantindo a confidencialidade, integridade e autenticidade das informações. As interfaces de integração devem ser protegidas e o acesso a esses serviços deve ser estritamente controlado e monitorado.

c) Contingência:

Procedimentos de contingência devem ser estabelecidos para garantir a disponibilidade contínua do Sistema ERP Tasy. Isso inclui a implementação de backups regulares, a definição de planos de recuperação de desastres e a realização de testes periódicos para validar a eficácia desses planos. Os coordenadores dos setores devem junto com a tecnologia da informação elaborar a rotina de contingência bem como os formulários usados nesses momentos.

d) Usuário e Senha:

A autenticação no Sistema ERP Tasy será realizada por meio de usuário e senha. Os usuários são responsáveis por manter suas credenciais de forma confidencial, sendo proibido o compartilhamento de senhas. A política de senhas deve seguir padrões indicados no item 5.6 deste manual.

e) Perfis:

Os perfis de acesso serão definidos com base nas funções e responsabilidades de cada usuário. O acesso será concedido de acordo com a necessidade da função, seguindo o princípio do menor privilégio para mitigar riscos de acesso não autorizado. Cabe o coordenador do setor junto com a tecnologia montar os perfis dos colaboradores.

f) Mudança de Acesso:

Toda solicitação de mudança de acesso deve ser submetida a um processo formal de aprovação. A alteração nos privilégios de acesso será realizada somente após confirmação da necessidade e validação pela equipe de tecnologia da informação. Registros dessas mudanças serão mantidos para fins de auditoria.

g) Encerramento de Acesso:

O acesso de um usuário ao Sistema ERP Tasy deve ser imediatamente revogado ao término de sua relação com a organização ou se sua função não requer mais o acesso ao sistema. Procedimentos específicos serão seguidos para garantir a completa remoção de direitos de acesso, minimizando possíveis riscos de segurança.

h) LGPD (Lei Geral de Proteção de Dados):

Todas as práticas relacionadas ao acesso e uso do Sistema ERP Tasy devem estar em conformidade com a LGPD. Isso inclui a proteção adequada de dados pessoais, a obtenção de consentimento quando necessário, a notificação de incidentes de segurança e o estabelecimento de medidas de segurança para garantir a privacidade dos dados.

Essa política visa garantir que o acesso ao Sistema ERP Tasy seja realizado de maneira segura e em conformidade com os princípios de segurança da informação, promovendo a confidencialidade, integridade, disponibilidade e autenticidade dos dados. A atualização constante e a revisão periódica desta política são essenciais para adaptar-se a novos desafios e garantir a eficácia contínua das medidas de segurança.

5.3 Medidas para Garantir a Segurança Cibernética Relacionada aos Equipamentos Médicos

A Fundação Beneficente Rio Doce reconhece a importância da segurança cibernética em relação aos equipamentos médicos para garantir a integridade, confidencialidade e disponibilidade das informações críticas de saúde. As medidas adotadas visam proteger contra ameaças cibernéticas e assegurar o funcionamento seguro dos dispositivos médicos.

5.3.1 Isolamento de Rede

a) Separação das redes de equipamentos médicos das redes corporativas para mitigar o risco de propagação de ameaças cibernéticas.
b) Utilização de firewalls, antivírus e políticas de segmentação para restringir o tráfego entre as redes, garantindo a proteção dos dados sensíveis.
c) Não é permitido médicos e demais profissionais não funcionários conectar seus equipamentos na rede do hospital.

5.4 Recuperação de Desastres (Disaster Recovery)

5.4.1 Backup e teste de recuperação

a) O banco de dados do Sistema Tasy fica alocado na OCI (Data Center da Oracle). Existem dois ambientes distintos PRODUÇÃO e HOMOLOGAÇÃO. O ambiente de HOMOLOGAÇÃO é utilizado para validação de rotinas, atualizações e validação da restauração da base de dados;
b) Manutenção de cópias de backup redundantes, tanto localmente quanto em nuvem, para garantir a recuperação eficiente de dados em caso de perda ou corrupção;

6 REFERÊNCIAS

NA

7 FLUXOGRAMA

NA

8 ANEXOS

NA

9 HISTÓRIO DE ALTERAÇÕES

Controle Histórico			
Nº da Versão	**Itens alterados**	**Data da Versão Atual**	**Data da Próxima Versão**
000	• NA	24/12/2023	24/12/2025
001	•		
002	•		