1. OBJETIVO

A Política de Segurança da Informação tem por objetivo prover as diretrizes no âmbito do Hospital de Urgências de Goiás, dos ativos formados por dados, informações e materiais sigilosos, bem como dos sistemas computacionais e das áreas e instalações onde são produzidos, armazenados ou trafegam, além da preservação da inviolabilidade e da intimidade da vida privada, da honra e imagem das pessoas e da instituição.

As ações de segurança da informação e das comunicações a serem elaboradas no âmbito institucional do Hospital de Urgências de Goiás - HUGO, deverão observar sempre a garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, lembrando sempre que as informações classificadas em qualquer grau de sigilo devem estar disponíveis estritamente a quem estiver autorizado.

2. DEFINIÇÕES

As definições constantes deste item se aplicam de forma a auxiliar a interpretação da Política de Segurança da Informação e das Comunicações no âmbito institucional e também no estabelecimento de futuras normas complementares.

3.SIGLAS

HUGO: Hospital de Urgências de Goiás;

4.PÚBLICO – ALVO

5.APLICAÇÃO

Unidades Setoriais e Departamento de Tecnologia da Informação

6.DESCRIÇÃO DO PROTOCOLO

O setor de tecnologia da Informação é responsável pelo Gerenciamento da rede de dados da unidade, Gerenciamento das Políticas de acesso as informações, Gerenciamento do Sistema Hospitalar, Manutenção das estações de trabalho (computadores), assim como seus servidores, Manutenção dos Arquivos produzidos pela unidade, Manutenção da rede de dados Física (exceto a de terceiros), Distribuição, Instalação e Remanejo dos computadores da Unidade e Suporte ao Usuário.

6.1 Descrição

- A segurança é direcionada contra ameaças – naturais, acidentais ou intencionais - de destruição, modificação ou divulgação indevida das informações e para o impedimento de fraudes;
- A informação deve ser tratada como um patrimônio a ser protegida no acesso, tráfego, uso e armazenamento, de acordo com sua classificação em graus de sigilo e criticidade;
- A política de segurança deve ser conhecida e seguida por todos os usuários da instituição;
- O Departamento de Tecnologia da Informação é responsável pela gestão da segurança de toda informação produzida e deve promover e disseminar a importância da segurança da informação, por meio de programas de sensibilização e conscientização dos seus usuários;
- Registros e informações sigilosas devem ser protegidos contra perda, destruição e falsificação, sendo mantidos de forma segura para atender requisitos legais e regulamentares;
- Os sistemas e equipamentos de informação estão sujeitos a monitoramento remoto e eventual inspeção local, a fim de prestar suporte e coibir a utilização indevida dos mesmos e danos resultantes desta utilização;
- O resultado de qualquer monitoramento é considerado sigiloso e deverá tramitar como tal dentro da instituição;
- Devem ser mantidos planos de contingência e recuperação de desastres, formais e periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade, de acordo com os critérios definidos pelo Departamento de Tecnologia da Informação;
- O usuário deve ter acesso autorizado apenas às informações, instalações e recursos necessários e indispensáveis ao seu trabalho, de acordo com perfis do setor e departamentos definidos formalmente e:

a. Com o objetivo de resguardar a rede (internet/Intranet) serão bloqueados o uso de jogos, redes sociais, receitas, site de vídeos e músicas ou qualquer outro site que não seja compatível com as atribuições do setor;

b. É obrigatório o uso de conta e-mail funcional para o exercício das atividades; e

c. A autorização de acesso dos itens "a" deverá ser justificada e encaminha ao Departamento de Tecnologia previamente assinados por Gestor da área solicitante ou Coordenador da Unidade através do e-mail Institucional ou Memorando interno.

- O acesso a informações e sistemas de que trata o item 6.11 será concedido, ao usuário que tenha a necessidade de conhecer, mediante identificador pessoal (**login**) e senha, pessoal e intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento;
- O usuário que tem acesso a informações confidenciais ou reservadas somente poderá fazer uso destas para os fins aprovados pelo respectivo gestor das informações, respeitando as regras de proteção estabelecidas;
- Os usuários devem estar cientes das normas de segurança das informações vigentes, bem como, dos procedimentos de segurança vigentes.
- Deve ser disciplinado o uso correto da informação e de recursos computacionais de forma a minimizar possíveis riscos à segurança;
- O acesso às informações que não sejam classificadas como públicas, dependerá da autorização do gestor da informação e deverá respeitar o grau de sigilo necessário, utilizando-a no estrito interesse da Administração em razão das suas atividades funcionais;
- Quando do afastamento ou desligamento do usuário das suas atribuições faz-se necessário o cancelamento imediato dos direitos de acesso e uso da informação, além do preenchimento de termo de desligamento;
- Os incidentes de segurança, tais como: indícios de fraude, sabotagem ou falha na segurança em processos, sistemas, instalações ou equipamentos devem ser prontamente notificados à chefia imediata e ao responsável pela gestão de segurança da informação;
- As condições e termos de licenciamento de software e os direitos de propriedade intelectual devem ser respeitados, estando vedada a instalação de programas de computador não homologados e licenciados.
- Os recursos do parque tecnológico e suas vinculações não podem ser utilizados para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, nem veicular opiniões político-partidárias;
- A entrada ou saída de equipamento computacional (patrimônio) das instalações da instituição deve ser informada pelo detentor do equipamento (responsável pelo bem patrimonial), sendo o trânsito permitido mediante a autorização da unidade competente;

6.2 Organização e composição do setor de tecnologia da informação

O setor de tecnologia da informação do hospital de urgências de Goiás e composto por um coordenador e uma equipe de 09 (Nove) pessoas dividias nas áreas de Administração, Desenvolvimento, Redes, Suporte e Manutenção, com seu funcionamento de 24 horas por sete dias na semana.

6.3 Softwares e Hardwares

O setor de Tecnologia da Informação – HUGO Trabalha com a política de Respeitar os direitos de propriedade intelectual, de acordo com a regulamentação pertinente, em particular a lei de direitos autorais de software, com os softwares licenciados que esta empresa possui, o setor de TI homologa a instalação dos seguintes softwares:

- Libreoffice, OpenOffice, Mozila ThunderBird, SOUL MV, BMA SISTEMAS, SIPEF Navegadores de Internet (Chrome, Mozila e Internet Explorer), sistemas desenvolvidos pela TI e ou contratados pela gestão do Hospital.
- Havendo necessidade de instalação de um determinado software que não esteja na lista de softwares permitidos e que o mesmo seja explicitamente para fins de trabalho, deverá ser encaminhado um memorando para a TI solicitando autorização para a instalação do devido software e seu licenciamento.
- Não é permitido sincronizar, plugar ou carregar a bateria de qualquer tipo de equipamento não autorizado pela TI nos equipamentos de informática (CPU, Monitor, Estabilizador, Régua, Switch e etc.), e em suas respectivas portas USB.
- O uso de Pendrive, Hds Externos e Cartões Sds estão bloqueados para o uso para fins de segurança contra possíveis Vírus que possam ser propagados por tais.

6.4 Servidores de Arquivos

Possuímos um servidor exclusivo para o arquivamento de documentos dos setores, cada qual com o nome do setor e com as permissões de acesso para apenas para os funcionários lotados nos mesmos ou autorizados pela chefia do setor, onde o gerenciamento é de respondibilidade do setor (Inserção e retira de arquivos) onde nenhum arquivo é apagado pelo setor de T.I que é diferente da pasta de transferência em que todos os colaboradores têm acesso independente do seu setor, temos uma rotina diária de backup dos arquivos, sendo possível a recuperação de arquivos apagados ou alterados acidentalmente. Salientamos que as pastas de rede compartilhadas no HUGO têm o

objetivo de servir o compartilhamento de arquivos relacionados aos trabalhos desenvolvidos pelos departamentos e não possuem cunho particular. A boa prática de utilização dessas pastas não contempla transferência de arquivos particulares, tais como músicas, fotos, vídeos, pois ocupam muito espaço nos servidores de dados, concorrendo com o espaço dedicado aos arquivos de trabalho. Além disso, há possibilidade de contaminação por vírus, pois esses arquivos particulares geralmente são transferidos de computadores pessoais desprotegidos.

6.5 Backups de Arquivos

Os backup's realizados na unidade são gerenciados pelo setor de TI HUGO, onde são alocados em diversos servidores. No servidor 'Hydmedia/Torax/Timo/Externo' Hydmedia ficam os backup das pastas compartilhadas dos setores e backup do sistema de Prestação de contas (SIPEF/BMA).Torax, ficam os Bacukps do ano anteiror e uma cópia do Bacukp do Hydmedia do ano Atual Os backups são feitos através da aplicação Cobian, onde são cadastradas as pastas para serem realizados os backups. No servidor 'Timo' também e feito um backup do sistema BMA. No servidor Radio fica uma Cópia da pasta de Transferência, também temos Bacukp do servidor de Arquivos em HD externo, e em serviço externo.

Os backups são realizados uma vez ao dia, os horários de realização dos backups acontecem em horários alternados. Os backups feitos no servidor tórax, pastas compartilhadas são realizadas a partir das 14 horas. Os backups feitos no servidor timo a partir das 02 horas. Os backups feitos no servidor crânio são realizados as 23 horas.

6.6 Cadastro de usuário no Active Directory (AD)/SOULMV

O cadastro de usuários para acesso à rede de dados (computadores/SOULMV) é feito através da solicitação da chefia do setor, onde encaminha um pedido via memorando ou e-mail, para o setor de TI – HUGO, onde é solicitado o login para o colaborador e suas permissões de acesso (internet, pastas compartilhas e impressoras). O login é criado no servidor "Metacarpo" na aplicação Active Directory, onde as permissões de acesso são atribuídas para cada usuário de forma individual ou por grupos de acesso. O Login para o sistema hospitalar SOULMV após a verificação das informações do colaborador e encaminhado para SES-GO, que confecciona o login de acordo com o perfil do prestador.

6.7 Monitoramento

O Hospital de Urgência de Goiás reafirma que o uso da tecnologia e da Internet é uma ferramenta valiosa para o desempenho das atividades. Dessa forma, o mau uso desses recursos pode ter impacto negativo sobre a produtividade dos colaboradores e os resultados. Portanto, a empresa pode aplicar restrições de navegação e monitorar o uso da internet na rede corporativa, de forma individual, aplicado a cada equipamento e colaborador. Através do serviço de Firewall e Proxy, são aplicadas regras de navegação definidas de acordo com a política de uso da internet do Hospital, com o objetivo de garantir maior foco e produtividade dos colaboradores. Da mesma forma é registrado todo e qualquer tipo de acesso à internet realizada por equipamento conectado à rede vinculado ao usuário (Login e Senha).

6.8 Significado

Ativo: Todo recurso utilizado para produção, tratamento, tráfego e armazenamento de dados;

Confidencial: Informações que devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos.

Confidencialidade: Garantia de acesso à informação somente por pessoas autorizadas;

Incidente: Ato ocorrido identificado com grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

Informação: Resultante do processamento, manipulação e organização de dados.

Integridade: Exatidão da informação e dos métodos de processamento;

Login: Identificador de usuário em um programa ou rede de computadores;

Malware: Código / software malicioso para causar danos ou apropriar de informações indevidas;

Públicas: Todas as informações que não possuem grau de sigilo atribuído.

Reservado: Aqueles cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos

Segurança: Percepção de se estar protegido de riscos, perigos ou perdas.

Spam: qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.

Usuário: Pessoa física autorizada a acessar o ambiente e as informações e de suas estações;

URL: endereço utilizado para trafegar dados, seja a internet, intranet ou rede privada de computadores.

7. AÇÕES CORRETIVAS

Não se aplica

8. REFERÊNCIA BIBLIOGRÁFICA

Não se aplica

9. ANEXOS

Não se aplica

10. CONTROLE DO DOCUMENTO

Elaboração:	Julia Barros Neves **Supervisora de Tecnologia da Informação**	31/08/2022	Julia Barros Neves Supervisora de TI Hospital de Urgência de Goiás HUGO
Revisão	Ana Paula Costa Viana Montalvão **Enfermeira NQSP**	29/11/2022	Ana Paula Costa V. Montalvão COREN-GO 690.257 Enfermeira do Núcleo da Qualidade e Segurança do Paciente
	Murilo Alves Luiz Pereira **Coordenador de Tecnologia da Informação**	29/11/2022	Murilo Alves Luiz Pereira Coordenador de TI Hospital de Urgências de Goiás-HUGO
Validação:	Tamilles da Silva Borges **Supervisora NQSP**	29/11/2022	Tamilles da Silva Borges Supervisora do Núcleo da Qualidade e Segurança do Paciente COREN-GO 496.302
Aprovação:	Jonatha Junio da Rocha **Gerente de Tecnologia da Informação**	29/11/2022	