Tipo do Documento	NORMA OPERACIONAL	NO.SETISD.001 - Página 1/8	
Título do Documento	**RESPONSABILIDADE DOS AGENTES PÚBLICOS NO USO DE CONTAS DE ACESSO E RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**	Emissão: 16/8/2022 Versão: 3	Próxima revisão: 16/8/2024

1. OBJETIVO

Esta Norma Operacional (NO) dispõe sobre as responsabilidades dos agentes públicos quanto ao uso de contas de acesso e recursos de Tecnologia da Informação e Comunicação (TIC) do Hospital de Clínicas da Universidade Federal do Triângulo Mineiro (HC-UFTM).

2. PÚBLICO-ALVO

Agentes Públicos do HC-UFTM.

3. DEFINIÇÕES E TERMINOLOGIAS

- Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal.
- Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, entidade ou órgão não autorizado e credenciado.
- Conta de acesso: conjunto do “nome de usuário” (conhecido também por *login*) e “senha”, utilizado para acesso aos sistemas informatizados e recursos de TIC.
- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
- Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
- Recursos de TIC: recursos que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, *notebooks*, *tablets*, telefones, *smartphones*, servidores de rede, equipamentos de conectividade e infraestrutura.
- Servidor de Arquivos: servidor de rede disponibilizado especificamente para o armazenamento de arquivos dos setores e agentes públicos.

4. DISPOSIÇÕES GERAIS

- Todo agente público deve conhecer e cumprir a Política de Segurança da Informação e Comunicações (POSIC), legislações em vigor referenciadas e quaisquer outros atos normativos complementares a fim de que não comprometa a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações no HC-UFTM.
- O HC-UFTM deve estabelecer um processo de divulgação permanente da sua POSIC para a conscientização de todos os agentes públicos.

5. REGRAS

5.1 Concessão e uso da conta de acesso

- O agente público somente terá acesso às informações e aos recursos de TIC após a conclusão do processo de credenciamento/concessão de acesso, que se dará através do preenchimento de formulário específico de criação de conta de acesso *on-line* disponível no Portal de Serviços do HC-UFTM.
- A cada agente público deve ser disponibilizada uma conta de acesso aos recursos de TIC, somente após a entrega ao Setor de Tecnologia da Informação e Saúde Digital (SETISD) do Termo de Responsabilidade de Uso de Recursos de TIC e Confidencialidade (Anexo A) devidamente assinado. Independentemente do sistema a ser acessado ou rede, essa identificação deve ser única, pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese.
- As permissões e perfis de acesso seguem as definições solicitadas pela chefia imediata do agente público em concordância com os padrões estabelecidos pelo SETISD.
- A conta de acesso aos recursos de TIC qualifica o agente público como único e total responsável por seu uso e suas consequências.
- A senha deverá obrigatoriamente conter no mínimo 8 (oito) caracteres.
- Recomenda-se que o agente público troque sua senha de acesso aos recursos de TIC a cada 90 (noventa) dias, no máximo, por questões de segurança.
- O agente público que não utilizar a sua conta por mais de 60 (sessenta) dias terá a mesma desativada.
- Cabe à Divisão de Gestão de Pessoas comunicar ao SETISD imediatamente quaisquer alterações de situações funcionais de agentes públicos (admissão, alteração de cargo e/ou função, alteração de lotação, desligamento) para que a devida manutenção de conta de acesso aos recursos de TIC seja efetuada.

5.2 Uso de recursos de TIC

- Os agentes públicos devem proteger os recursos de TIC do HC-UFTM contra acesso, modificação, destruição ou divulgação de dados e informações não autorizadas.
- Os agentes públicos devem utilizar os recursos de TIC colocados à sua disposição somente para os fins institucionais aos quais se destinam.
- É de responsabilidade do agente público zelar pela integridade dos equipamentos, sistemas e redes.
- É expressamente proibida a abertura do gabinete das estações de trabalho ou computador portátil, bem como modificar qualquer configuração, seja de *hardware* ou *software*. Essas configurações são padronizadas, conforme definições do SETISD:
  - ✓ Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada ao SETISD para análise.
- É expressamente proibida a instalação ou execução de *software* próprio ou de terceiros sem prévia homologação e autorização do SETISD.
- É responsabilidade do agente público desligar a estação de trabalho ou computador portátil corretamente e diariamente ao final do expediente, seguindo os procedimentos do sistema

operacional.

- A estação de trabalho será bloqueada caso o sistema fique ocioso por 5 (cinco) minutos.
- Não será permitido armazenar arquivos pessoais, tais como fotos, músicas, vídeos ou documentos não inerentes à instituição nas estações de trabalho bem como nas pastas compartilhadas.
- As cópias de segurança (*backups*) dos arquivos armazenados nas estações de trabalho, nas pastas compartilhadas, ou de qualquer programa ou sistema de terceiros que não tenha sido homologado pelo SETISD, e que são inerentes à instituição, são de responsabilidade do agente público:
  - ✓ Caso o mesmo não detenha conhecimento técnico necessário, ele pode solicitar ao SETISD capacitação para execução de tal tarefa.
- Não é permitido que seja conectado/ligado às redes ou computadores do HC-UFTM qualquer equipamento de informática que não pertença à instituição sem prévia autorização e/ou homologação pelo SETISD.
- Não é permitida qualquer mudança física de equipamentos de TIC:
  - ✓ Caso haja necessidade, deve ser solicitado formalmente ao SETISD para avaliação e execução.

5.3 Uso de dispositivos portáteis

- Os dispositivos portáteis do HC-UFTM, sempre que não estiverem sendo utilizados, devem ser guardados em local seguro, onde o responsável por estes possa garantir a segurança patrimonial, inclusive a não utilização por pessoas não autorizadas.

5.4 Política de mesa e tela limpas

- Os documentos devem ser classificados em conformidade com a Política de Classificação De Informação, Sigilo e Temporalidade da Ebserh.
- Os documentos sigilosos não devem ser deixados à vista na ausência do agente público e devem ser guardados em local seguro e com controle de acesso.
- O agente público deve bloquear o acesso à estação de trabalho ou computador portátil que lhe foi confiado sempre que dele se ausentar.

5.5 Descarte de informações

- As informações não mais utilizadas pelos agentes públicos, em meio eletrônico ou não, devem ser apagadas ou destruídas conforme regras da legislação vigente.

6. DISPOSIÇÕES FINAIS

- Os agentes públicos devem comunicar os incidentes que afetam a segurança do patrimônio ou o descumprimento desta Norma ao SETISD.
- Em casos de quebra de segurança da informação por meio de recursos de TIC, o SETISD deve

ser imediatamente notificado a fim de adotar as providências necessárias.

- Os incidentes de segurança e denúncias de descumprimento desta Norma, da POSIC e de suas regulamentações devem ser encaminhados ao SETISD, pelo e-mail setisd.hc-uftm@ebserh.gov.br.
- Ao autor de infração a esta Norma, serão aplicadas as sanções cabíveis, conforme previsto no item "Penalidades" da Política de Segurança da Informação e Comunicações da Ebserh.

7. LEIS E REGULAMENTOS APLICÁVEIS

1. Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

2. Norma Brasileira (NBR) ISO/IEC 27001:2013 - Sistema de Gestão de Segurança da Informação.

3. NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação.

4. Norma Complementar nº 1 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.

5. Norma Complementar nº 3 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações - POSIC nos órgãos e entidades da Administração Pública Federal, direta ou indireta - APF.

6. Norma Complementar nº 20 IN01/DSIC/GSI/PR, de 15 de julho de 2014, que estabelece diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal, direta ou indireta – APF.

7. Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.

8. Portaria nº 1054, de 02 de agosto de 2011, que institui a Política de Segurança da Informação e Comunicações no Ministério da Educação.

9. Decreto-Lei 2.848, de 07 de dezembro de 1940.

10. Lei 8.112, de 11 de dezembro de 1990.

11. Política de Segurança da Informação e Comunicações da Ebserh (PoSIC).

12. Política de Classificação De Informação, Sigilo e Temporalidade da Ebserh.

13. Política de Proteção de Dados Pessoais da Ebserh.

14. Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais.

14. Lei 8.429 de 2 de junho de 1992 – Lei da Improbidade Administrativa

8. HISTÓRICO DE ELABORAÇÃO/REVISÃO

VERSÃO	DATA	DESCRIÇÃO DA AÇÃO/ALTERAÇÃO
3	10/6/2022	

Elaboração – versão 1 Freud Antonio Martinelli Gomes, chefe do Setor de Gestão de Processos e Tecnologia da Informação (SGPTI) **Registro e análise inicial** Alice Prudente Borges, assistente administrativo da Unidade de Planejamento **Registro, análise, formatação e revisão final** Ana Paula Corrêa Gomes, chefe da Unidade de Planejamento **Aprovação** Colegiado Executivo	Data: 10/7/2017
Revisão – versão 2 Rodrigo Ferretti Silva, chefe do SGPTI **Registro, análise, formatação e revisão** Ana Paula Corrêa Gomes, chefe da Unidade de Planejamento **Validação** Rodrigo Ferreti Silva, chefe do SGPTI **Aprovação** Colegiado Executivo	Data: 1º/6/2020
Revisão – versão 3 Rodrigo Ferretti Silva, chefe do SETISD Sergio de Oliveira, Analista de Tecnologia da Informação/SETISD Marcela Valente de Sousa, Assistente Administrativo do SETISD **Registro, análise, formatação e revisão** Ana Paula Corrêa Gomes, chefe da Unidade de Planejamento, Gestão de Riscos e Controles Internos **Validação** Rodrigo Ferreti Silva, chefe do SETISD **Aprovação** Colegiado Executivo	Data: 16/8/2022

9. ANEXO A

Hospital de Clínicas

TERMO DE RESPONSABILIDADE DE USO DE RECURSOS DE TIC E CONFIDENCIALIDADE

Eu **nome, nacionalidade, cargo, SIAPE 0000000, inscrito (a) no CPF sob o nº** 000.000.000-00, declaro ter ciência da obrigatoriedade, a partir desta data, quanto ao cumprimento das regulamentações descritas na Política de Segurança da Informação e Comunicação (POSIC) do Hospital de Clínicas da UFTM, publicada por meio da Portaria nº 35, de 6 de março de 2017, da EBSERH, instituída por meio da Resolução Conselho Consultivo nº 70, de 6 de julho de 2017 do Hospital de Clínicas da UFTM. Comprometo-me ainda a cumprir o dever de agente público em salvaguardar a informação sigilosa e a pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal. (Norma Complementar 20/IN01/DSIC/GSIPR).

Por este termo de responsabilidade e confidencialidade, comprometo-me a:

1. Não utilizar informações **sigilosas (protegidas por legislação específica) ou pessoais** a que tiver acesso, para lograr benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros. Estas informações nos diversos formatos (impresso, magnético ou digital) devem ser tratadas com absoluta reserva em qualquer condição e não podem ser divulgadas ou dadas a conhecer a terceiros não autorizados, inclusive aos próprios usuários (servidores públicos, estagiários, prestadores de serviço ou terceirizados) do Hospital de Clínicas da UFTM, sem a autorização do proprietário da informação;

2. Não efetuar gravação ou cópia da documentação sigilosa ou pessoal a que tiver acesso para fins diversos não relativos à função ou cargo;

3. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

4. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador, bloquear estação de trabalho, garantindo assim a impossibilidade de acesso indevido por terceiros;

5. Não revelar minhas senhas a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

6. Alterar minha senha regularmente e sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

7. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

8. Não navegar em sites pornográficos, defensores do uso de drogas, de pedofilia ou sites de cunho racistas e similares ou realizar qualquer atividade tipificada como crime, bem como não fazer download de material protegido por direitos autorais ou com conteúdo impróprio;

9. Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

10. Informar imediatamente ao Setor de Tecnologia da Informação e Saúde Digital (SETISD) do HC UFTM a respeito de qualquer incidente de segurança da informação ou violação, intencional ou não, das regras descritas na Política de Segurança da Informação e normativas correlacionadas.

De acordo com o Código Penal Brasileiro (Decreto-Lei 2.848, de 1940) constitui infração inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

O não cumprimento deste Termo implicará, para os que estiverem envolvidos na violação do sigilo e uso das informações do Hospital de Clínicas da UFTM, sem prejuízo da responsabilidade civil e criminal, nas seguintes sanções: Para Servidores: sanções internas, variando de simples advertência à demissão por justa causa, conforme Art. 132, inciso IX da Lei 8112/90. Para parceiros, estagiários, prestadores de serviço ou terceirizados: variando de advertência à rescisão do respectivo contrato de prestação de serviço, com aplicação de todas as multas nele previstas por inadimplemento.

Nestes Termos, as seguintes expressões são assim definidas:

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal.
Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
Informação pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem, como: resultado de exames médicos; lista de nomes,

e-mail dos servidores ou colaboradores do Hospital de Clínicas da UFTM e respectivos dados, armazenados sob qualquer forma; Informações referentes a salários e benefícios dos servidores.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo, tais como: Sigilos Decorrentes de Direitos de Personalidade: Sigilo Fiscal, Sigilo Bancário, Comercial, Sigilo Empresarial, Sigilo Contábil; Sigilos de Processos e Procedimentos: Acesso a Documento Preparatório, Sigilo do Procedimento Administrativo Disciplinar em Curso, Sigilo do Inquérito Policial, Segredo de Justiça no Processo Civil, Segredo de Justiça no Processo Penal; Informação de Natureza Patrimonial: Segredo Industrial, Direito Autoral e Propriedade Intelectual de Programa de Computador, Propriedade Industrial.

Incidente de segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que seja ameaça á integridade, autenticidade ou disponibilidade de qualquer ativo de TI do Hospital de Clínicas da UFTM.

Proprietário da informação: refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação.

Uberaba, _____ de _____ de 20___.

_____

Nome do Agente Público