Norma Operacional n.º 8, de 6 de Julho de 2017

Normatiza os procedimentos de segurança relativos ao uso do serviço correio eletrônico no âmbito do Hospital de Clínicas da Universidade Federal do Triângulo Mineiro (HC-UFTM).

O Superintendente do Hospital de Clinicas da Universidade Federal do Triângulo Mineiro e, considerando

a Norma Brasileira (NBR) *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC) 27001:2013 - Sistema de Gestão de Segurança da Informação**;**

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

a Norma Complementar n.º 1 Instrução Normativa/Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (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;

a Norma Complementar n.º 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 (APF), direta ou indireta;

a Norma Complementar n.º 7/IN01/DSIC/GSIPR, (Revisão 1), que estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da APF, direta e indireta;

a POSIC da Ebserh, resolve:

Art. 1.º Editar a presente Norma Operacional que versa sobre os procedimentos de segurança relativos ao uso do serviço correio eletrônico no âmbito do Hospital de Clínicas da Universidade Federal do Triângulo Mineiro (HC-UFTM).

Art. 2.º Para fins desta Norma entende-se por:

I – e-mail: correio eletrônico que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

II - caixa de correio: conjunto de pastas (caixa de entrada, itens enviados, rascunhos, etc.) e as próprias mensagens do correio eletrônico;
III - cavalo de troia: programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogos, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário;
IV - endereço de correio eletrônico: identificação do proprietário de um correio eletrônico;
V - correio eletrônico institucional: conta de correio eletrônico mantido pelo HC-UFTM e/ou Ebserh;
VI - correio eletrônico particular: conta de correio eletrônico mantido por terceiros (Gmail, Hotmail, Yahoo, etc.);
VII - correntes: é considerado um tipo de *spam*. Geralmente é apresentado em um texto que pede para que o destinatário repasse a mensagem um determinado número de vezes ou, ainda, "para todos os amigos" ou "para todos que ama", sendo que o texto pode contar uma história antiga, descrever uma simpatia (superstição) ou, simplesmente, desejar sorte;
VIII - lista de distribuição: uso de um e-mail para o envio de mensagens (unidirecional) aos membros de um grupo;
IX - provedor de e-mail externo: fornecedor de serviços de e-mail provido por terceiros (Gmail, Yahoo, Hotmail, etc.);
X - spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
XI - *software* - sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas e também pode ser definido como os programas que comandam o funcionamento de um computador;
XII - *spyware*: termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros, geralmente utilizadas de forma não autorizada e maliciosa;
XIII - vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.
XIV - agente público: toda aquela pessoa física que presta serviço à Administração Pública e às pessoas jurídicas da administração indireta, seja transitoriamente ou sem remuneração.

Art. 3.º Para que seja permitido o acesso e a criação de contas, o agente público terá direito a uma única conta de e-mail que o identificará.

Art. 4.° A conta de correio eletrônico institucional, disponibilizada ao agente público quando de sua admissão, é pessoal e intransferível e deve ser utilizada somente para os interesses da instituição, sendo seu titular o único e total responsável pelo seu uso e suas consequências, sendo vedada sua divulgação.

Art. 5.° Ao utilizar correio eletrônico particular, o agente público não deverá exceder os limites da ética, bom senso e razoabilidade, sendo o mesmo responsável pelo conteúdo trafegado e seus eventuais riscos.

§ 1.º O HC-UFTM não se responsabiliza em fornecer suporte técnico ao correio eletrônico particular.

§ 2.º É proibido o uso do correio eletrônico particular para o envio ou recebimento de informações de mensagens e/ou documentos institucionais.

Art. 6.° Em relação ao cancelamento, bloqueio, suspensão ou desbloqueio do correio eletrônico:
I - cabe à Divisão de Gestão de Pessoas comunicar ao Setor de Gestão de Processos e Tecnologia da Informação (SGPTI) o desligamento dos agentes públicos do HC-UFTM para que a conta de correio eletrônico do agente público seja desativada;
II - no caso de afastamento do agente público, o acesso ao seu correio eletrônico será suspenso.

Art. 7.º Do uso do correio eletrônico:
I - as caixas de correio eletrônico institucional possuem tamanho limitado, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo do SGPTI definir esses limites;
II - todo agente público do HC-UFTM, antes de enviar mensagens pelo correio eletrônico institucional, deve levar em conta a classificação da informação, conforme legislação vigente;
III - o uso da conta de correio eletrônico institucional em listas de distribuição deve se limitar aos casos de necessidade do trabalho ou atividade desempenhada no HC-UFTM;
IV - o correio eletrônico institucional não deve ser utilizado para fim particular, como cadastro de comércio eletrônico, por exemplo.

Art. 8.º É vedada a utilização do correio eletrônico institucional para:

I - praticar crimes e infrações de qualquer natureza;

II - realizar spam;

III - contribuir com a continuidade de correntes de mensagens eletrônicas;

IV - utilizá-lo com objetivos político-partidários, religiosos, entre outros;

V - receber, armazenar ou enviar de forma consentida, mensagens com:

a) vírus de computador, cavalo de Troia, *spyware* e outros *softwares* maliciosos;
b) material pornográfico, atentatório à moral e aos bons costumes ou ofensivos;
c) conteúdo criminoso, ilegal, ou que façam sua apologia;
d) conteúdo discriminatório (racial, religioso, etc.) ou de incitação à violência;
e) conteúdo que desrespeite os direitos autorais.

Art. 9.º De forma a preservar o funcionamento do serviço de correio eletrônico institucional, o agente público deve:

I - eliminar, periodicamente, as mensagens desnecessárias de sua caixa de correio, inclusive as existentes nas pastas personalizadas, na lixeira, rascunho e enviados, de forma a não exceder o limite de tamanho da caixa de correio;

II - evitar clicar em *links* de acesso às páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem iniciar a instalação de *softwares* maliciosos ou direcionar o agente público para um *site* falso, possibilitando a captura de informações;

III - evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência, solicitando ajuda do SGPTI no caso de suspeita de irregularidade na mensagem.

Art. 10. Quanto ao monitoramento do uso do serviço correio eletrônico:

I - o correio eletrônico institucional pode ser monitorado e restringido pelo SGPTI, quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados);

II - nos casos de suspeita de infração à POSIC, o SGPTI poderá acessar a caixa postal institucional do respectivo agente público através de ato administrativo ou judicial.

Art. 11. Os agentes públicos devem comunicar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao SGPTI

Art. 12. Em caso de quebra de segurança da informação por meio de recursos de TIC o SGPTI deve ser imediatamente notificado a fim de adotar as providências necessárias.

Art. 13. Os incidentes de segurança, quebra de segurança e denúncias de descumprimento à POSIC e suas normas podem ser encaminhadas através do e-mail sgpti.hctm@ebserh.gov.br.

Art. 14. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da POSIC da Ebserh Sede, estendida para suas filiais.

Art. 15. Esta norma entra em vigor a partir da data de sua publicação.