

PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Teresina, março de 2018

DISTRIBUIÇÃO E VIGÊNCIA

Este documento consiste na Política de Segurança da Informação – PSI do Hospital Universitário da Universidade Federal do Piauí HU-UFPI, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades. No entanto destaca-se que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da instituição.

Esta versão pode ser alterada a qualquer momento, uma vez que os pontos apontados para mudanças sejam informados e discutidos com os demais colaboradores da mesma. Contudo a versão da PSI deve ser revisada a cada ano, considerando a data de sua aprovação.

CICLO DE APROVAÇÃO

Destacam-se as principais fases da **Política de Segurança da Informação**:

Elaborador	Data
Analista de Segurança	

Revisor e Aprovador	Data

Aprovador Final	Data

CONTROLE DE VERSÕES

Versão	Data	Responsável	Controle das Modificações
1.0	01/03/2014	Mychel Rosa	Criação do documento
1.1	20/06/2017	Madson Santos	*Segurança Do Ambiente Físico *Uso Das Estações De Trabalho (Item 12 – Pag.19) *Segurança Do Ambiente De Ti (Pag.23-24) *Da Equipe De Resposta A Incidentes Em Redes
1.2	18/09/2017	Mychel Rosa	*Retirada do Projeto de Controle de Acesso Físico do Hospital
1.3	22/09/2017	Mychel Rosa	*Revisão do documento

SUMÁRIO

GLOSSÁRIO

INTRODUÇÃO

OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POR QUE OS COLABORADORES DEVEM SE PREOCUPAR COM
SEGURANÇA?

ALTA DIREÇÃO

CLASSIFICAÇÃO DAS INFORMAÇÕES

DAS RESPONSABILIDADES

UTILIZAÇÃO DA REDE

POLÍTICA DE SENHAS

CORREIO ELETRÔNICO

USO DAS ESTAÇÕES DE TRABALHO

USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

USO DE IMPRESSORAS

SEGURANÇA DO AMBIENTE DE TI

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES
COMPUTACIONAIS

VIOLAÇÃO DA POLÍTICA E PENALIDADES

CONSIDERAÇÕES FINAIS

ANEXO I – TERMO DE COMPROMISSO

ANEXO II – TERMO DE RESPONSABILIDADE DE USO DE NOTEBOOK
PARTICULAR NA REDE CORPORATIVA

GLOSSÁRIO

Ativo: Algo que tenha valor para a organização.

Evento: Acontecimento que acarrete na mudança do estado atual de um processo.

Incidente: Evento que traz prejuízos à organização.

Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos.

Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização.

Malwares: O nome malware vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador.

SPAM: É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Phishing: Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar sua identidade.

Mail bombing: Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível.

INTRODUÇÃO

A presente Política de Segurança da Informação – PSI está baseada nas recomendações da norma ABNT NBR ISSO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, além de estar de acordo com o Decreto nº3505 de 13/06/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, e outras leis vigentes.

A informação é um ativo de grande valor para o Hospital Universitário do Piauí – HU-UFPI, por isso necessita ser adequadamente protegida.

“Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT NBR ISO/IEC 17799:2005).

Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

- Confidencialidade: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
- Integridade: Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;
- Disponibilidade: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

O HU-UFPI faz o acompanhamento do ciclo de atendimento dos pacientes através do sistema Aplicativo de Gestão para Hospitais Universitários – AGHU, tornando essencial para o negócio que as informações sejam confiáveis e estejam devidamente protegidas. Assim, é imprescindível a criação de uma política que normatize e direcione os procedimentos necessários para garantir a segurança das informações e a consequente excelência no atendimento ao paciente, sendo este o caráter do documento ora apresentado.

OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

“A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados” (ABNT NBR ISO/IEC 17799:2005).

A Política de Segurança da Informação tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

- A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;
- O compromisso da empresa com a proteção das informações de sua propriedade e/ou sob sua guarda;
- A participação e cumprimento por todos os colaboradores em todo o processo.

POR QUE OS COLABORADORES DEVEM SE PREOCUPAR COM SEGURANÇA?

“Uma corrente é tão forte quanto seu elo mais fraco”. Não adianta a área da Tecnologia da Informação impor controles e medidas técnicas se não existir a participação dos colaboradores, por exemplo, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico se um funcionário que tem acesso legítimo a determinada área restrita, resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área.

A área de Tecnologia da Informação é a responsável pela salvaguarda dos dados da organização, mas o processo de segurança da informação deve envolver todos os colaboradores, independente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada.

Diante do exposto, a Política da Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.

ALTA DIREÇÃO

A efetividade Política de Segurança da Informação depende estritamente do comprometimento da alta direção. É essencial que os responsáveis por liberar recursos, aplicar sanções, criar regras e portarias, apoiem a PSI e demonstrem seu comprometimento para que os colaboradores se sintam motivados a cumpri-la.

A ordem expressa e o exemplo de cumprimento das cláusulas da PSI pela alta direção possibilitarão:

- A inexistência de exceções à regra;
- Que a PSI seja um ativo estratégico;
- Que a PSI componha a legislação interna do HU-UFPI;
- Que a PSI tenha ampla divulgação;
- Que a PSI seja incluída no processo de contratação de novos funcionários.

Caso esta premissa não seja cumprida, a Política de Segurança da Informação se tornará apenas um documento obsoleto, existente na teoria e não adotado na prática.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

- Pública;
- Interna;
- Confidencial;
- Confidencial restrita.

1 – Pública

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

São exemplos de informação pública:

- Editais de licitação;
- Rotinas e agendas médicas;
- Campanhas de promoção à saúde.

2- Interna

São informações disponíveis aos colaboradores do HU-UFPI para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

São exemplos de informações internas:

- Memorandos, Portarias, Padrões, Políticas e Procedimentos internos;
- E-mails e lista telefônica internos;
- Avisos e campanhas internas;

3 – Confidencial

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.

São exemplos de informações confidenciais:

- Exames e diagnósticos de pacientes;
- Processos judiciais;
- Dados cadastrais de funcionários.

4 – Confidencial restrita

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas ao superintendente, gerentes e funcionários cujas funções requeiram conhecê-las.

São exemplos de informações confidenciais restritas:

- Atas de reunião da governança com a presidência da EBSERH;
- Indicadores e estatísticas dos processos de negócio do HU-UFPI;
- Resultado de auditorias internas.

DAS RESPONSABILIDADES

1 – Colaboradores

Será de inteira responsabilidade de servidores, funcionários, terceirizados e demais colaboradores do HU-UFPI:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação do Hospital Universitário do Piauí;
- Buscar o Setor de Gestão de Informação e Informática para esclarecimentos de dúvidas referentes à PSI;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pelo HU-UFPI;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo HU-UFPI;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Comunicar prontamente à chefia imediata qualquer violação a esta política, suas normas e procedimentos.

2 – Gestores de Pessoas e/ou Processos

Em relação à segurança da Informação, cabe aos gestores de pessoas e/ou processos:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI do HU-UFPI;
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Elaborar, com o apoio do Setor de Gestão de Processos e Tecnologia da Informação, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

- Tomar as decisões administrativas referentes aos descumprimentos da PSI do HU-UFPI.

3 – Subcomitê Gestor de Segurança da Informação

Cabe ao Subcomitê Gestor de Segurança da Informação:

- Propor melhorias, alterações e ajustes da PSI;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Avaliar incidentes de segurança e propor ações corretivas;

O Subcomitê de Gestão de Segurança da Informação deverá ser composto por, no mínimo, um colaborador das seguintes áreas:

- Representante da Governança;
- Setor de Gestão de Processos e Tecnologia da Informação;
- Unidade de Gestão da Informação;
- Unidade de Suporte de TI;
- Divisão de Gestão de Pessoas;
- Assessoria Jurídica;

O CGSI reunir-se-á, ordinariamente, uma vez a cada seis meses e extraordinariamente sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o HU-UFPI.

4 - Setor de Gestão de Processos e Tecnologia da Informação

Cabe ao Setor de Gestão da Informação e Informática:

- Definir as regras para instalação de software e hardware no HU-UFPI;
- Homologar os equipamentos pessoais (smartphones e notebooks) para uso na rede do HU-UFPI;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Mediante informações da DivGP, manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;

- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades, etc.;
- Promover, com o envolvimento da DIVGP, palestras de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio do HU-UFPI;
- Analisar criticamente incidentes de segurança em conjunto com o Subcomitê Gestor de Segurança da Informação;
- Manter comunicação efetiva com o Subcomitê Gestor de Segurança da Informação sobre possíveis ameaças e novas medidas de segurança;
- Buscar alinhamento com as diretrizes da organização.

UTILIZAÇÃO DA REDE

O ingresso à rede interna do HU-UFPI deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados. Assim, é preciso que sejam instauradas algumas regras, listadas a seguir:

- 1) A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade do HU-UFPI, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores neste hospital;
- 2) A Internet sem fio deverá ser segregada, garantindo o isolamento da rede interna do hospital, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; poderá ter outras redes com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam/podem ter acesso aos dados internos. A definição de qual rede o usuário deverá ingressar ficará a cargo do SGPTI após análise dos requisitos de acesso;
- 3) A concessão de acesso à rede sem fio para acesso apenas à Internet se dará através de preenchimento de formulário disponível na página <http://sisah.ufpi.br>, aba “Suporte Técnico”, opção “Solicitação de Acesso WiFi. O usuário deverá preencher o formulário e encaminhá-lo impresso ao SGPTI, devidamente assinado pelo chefe do setor/unidade. Ficam estabelecidos os seguintes períodos de acesso: 1 ano para colaboradores, 6 meses para estudantes e 1 semana para visitantes;
- 4) A DivGP ficará responsável por notificar formalmente o SGPTI sobre desligamentos de colaboradores, para que os acessos dos mesmos sejam revogados;
- 5) O HU-UFPI reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;
- 6) Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade do HU-UFPI, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.
- 7) A Internet disponibilizada pelo HU-UFPI aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada pelo chefe e não prejudique o andamento dos trabalhos nos setores/unidades;
- 8) Apenas colaboradores devidamente autorizados a falar em nome do HU-UFPI para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica, etc.;

- 9) É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;
- 10) Os colaboradores com acesso à Internet só poderão fazer o download programas necessários às suas atividades no HU-UFPI e deverão providenciar a licença e o registro necessário desses programas, desde que autorizados pelo SGPTI;
- 11) O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo SGPTI;
- 12) Os colaboradores não poderão em hipótese alguma utilizar os recursos do HU-UFPI para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
- 13) Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
- 14) Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
- 15) Os colaboradores não poderão usar os recursos do HU-UFPI para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;
- 16) Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, µtorrent e afins);
- 17) Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, uploaded, bitshare, depositfiles, etc;
- 18) Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall;
- 19) Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando o SGPTI deverá estar devidamente ciente e concedido autorização para tal;

- 20) Os arquivos inerentes ao HU-UFPI, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;
- 21) Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;
- 22) Haverá geração de relatórios de sites e downloads acessados por usuário.

POLÍTICA DE SENHAS

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

- 1) A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
- 2) A senha inicial só será fornecida ao próprio colaborador, pessoalmente. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
- 3) É proibido o compartilhamento de login para funções de administração de sistemas;
- 4) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);
- 5) As senhas deverão seguir os seguintes pré-requisitos:
 - Tamanho mínimo de oito caracteres;
 - Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
 - Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc).
- 6) O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

- Desligamento do colaborador;
 - Mudança de função do colaborador;
 - Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
- 7) Para os cancelamentos acima mencionados, a Divisão de Gestão de Pessoas ficará responsável por informar prontamente o SGPTI acerca dos desligamentos e mudança de função dos colaboradores.

E-MAIL

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

- 1) O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;
- 2) Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;
- 3) É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;
- 4) É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
- 5) É proibido enviar qualquer mensagem por meios eletrônicos que torne o HU-UFPI vulnerável a ações civis ou criminais;
- 6) É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- 7) Produzir, transmitir ou divulgar mensagem que:
 - Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
 - Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
 - Vise obter acesso não autorizado a outro computador, servidor ou rede;
 - Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Vise burlar qualquer sistema de segurança;
 - Vise vigiar secretamente ou assediar outro usuário;
 - Vise acessar informações confidenciais sem explícita autorização do proprietário;
 - Tenha conteúdo considerado impróprio, obsceno ou ilegal;
 - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
 - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
- 8) O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:
- Não contrariar as normas aqui estabelecidas;
 - Não interferir, negativamente, nas atividades profissionais individuais ou na de outros colaboradores;
 - Não interferir, negativamente, no HU-UFPI e na sua imagem.

USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

- 1) É de responsabilidade do colaborador do equipamento zelar pelo mesmo, mantendo-o em boas condições;
- 2) Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;
- 3) É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe do SGPTI;
- 4) As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas.
- 5) É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do SGPTI;
- 6) É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do SGPTI;

- 7) As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;
- 8) Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
- 9) Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
- 10) É proibido o uso de estações de trabalho para:
 - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
 - Burlar quaisquer sistemas de segurança;
 - Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
 - Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
 - Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- 11) O SGPTI não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição;
- 12) As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo do HU-UFPI é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, contando com todos os recursos de equipamentos disponíveis, mas não pode deixar de considerar os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade do HU-UFPI ou particular com prévia aprovação e permissão pelo SGPTI, como: notebooks, smartphones e pendrives.

Todas as regras do tópico “Estações de Trabalho” se enquadram nesta seção, adicionalmente a:

- 1) Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna do HU-UFPI mediante autorização do chefe imediato via memorando e prévio cadastro e liberação do SGPTI;
- 2) O uso de notebooks e dispositivos móveis para fins de acesso à rede de Internet do HU-UFPI será realizado mediante cadastro de usuário através do endereço <http://sisah.ufpi.br> e autorização do chefe imediato (Ver item 3 – Utilização da Rede);
- 3) O SGPTI deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. Aplicativos peer to peer, farejadores de tráfego, softwares que possam gerar carga excessiva na rede, que não estejam de acordo com a legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem HU-UFPI não serão permitidos. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;
- 4) O SGPTI tem o direito de, periodicamente, auditar os equipamentos utilizados no HU-UFPI, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados no HU-UFPI;
- 5) É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo SGPTI;
- 6) É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook;
- 7) Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
- 8) É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam ao HU-UFPI não podem ser armazenados no disco rígido do notebook ou em dispositivos de armazenamento móvel (ex: pendrive), sem a autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados no servidor de compartilhamento destinado para tal;
- 9) Mesmo nos computadores portáteis fornecidos pelo HU-UFPI, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento;
- 10) É proibida a inclusão de smartphones na rede corporativa do HU-UFPI. Estes equipamentos deverão ter seu acesso restrito à rede de Internet;

USO DE IMPRESSORAS

O uso de impressoras no HU-UFPI deve seguir algumas regras:

- 1) É proibida a impressão e xerox de documentos de cunho pessoal e/ou ilegal;
- 2) A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica do SGPTI;
- 3) A instalação das impressoras deverá ser realizada através do servidor de impressão “CUPS”. É proibida a instalação por vias diretas através da rede;
- 4) O chefe de cada setor / unidade será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões/xerox excessivas;
- 5) As impressoras devem estar ligadas na energia através dos seus transformadores e serão proibidas intervenções desta natureza por parte de qualquer colaborador que não seja do SGPTI.

BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer. Assim, estabelecem-se as regras:

- 1) Todo sistema ou informação relevante para a operação dos negócios do HU-UFPI deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;
- 2) As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar o SGPTI sobre a necessidade de backup dos mesmos, sugerindo o tempo de retenção destas cópias;
- 3) Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;
- 4) As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;
- 5) Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;

- 6) O SGPTI deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;
- 7) Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

SEGURANÇA DO AMBIENTE DE TI

Estrutura Física do Data Center

As máquinas (servidores) que armazenam sistemas do HU-UFPI estão em área protegida – Data Centers localizados neste hospital.

Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do Data Center;

A entrada aos Data Centers tem acesso devidamente controlado e monitorado.

As permissões de acesso físico às áreas restritas do Data Center devem ser mensalmente revisadas;

As áreas do Data Center devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado;

A porta do Data Center deve permanecer fechada, com mecanismo de autenticação individual quando possível.

O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de Segurança e mediante supervisão.

O acesso ao Datacenter sem as devidas identificações só poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Caso haja necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a mesma deve ser autorizada pelo Subcomitê Gestor de Segurança da Informação.

Estrutura Lógica do Data Center

Na política de segurança da Informação estabelecida pelo HU-UFPI, define-se que os analistas de TI, mediante ciência do Subcomitê Gestor de Segurança da Informação, devem ser os únicos a terem permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

O objetivo da segurança lógica no Data Center é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados;

Somente os colaboradores credenciados e autorizados pelo Subcomitê Gestor de Segurança da Informação podem ter acesso aos dados armazenados;

Os logs dos ativos de rede devem ser monitorados constantemente afim de evitar acessos indevidos.

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (Resolução nº 1 de 30/06/2010 / MTE - Ministério do Trabalho e Emprego - D.O.U. 02/07/2010)

Objetivo

A missão da ETIR é zelar pela segurança das informações e comunicações do HU-UFPI, prevenindo e tratando incidentes de rede, em cumprimento à Política de Segurança da Informação deste hospital.

A atividade principal da ETIR é o tratamento de incidentes de segurança em rede, que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de vulnerabilidades.

Diretrizes

Modelo de Implementação

O modelo de implementação a ser utilizado, inicialmente, pela ETIR será o modelo Centralizado. Neste modelo existirá uma ETIR central composta por empregados públicos com dedicação não exclusiva às atividades de tratamento e resposta aos incidentes no ambiente computacional do HU-UFPI;

O Gestor de Segurança da Informação será responsável por criar as estratégias, gerenciar as atividades e executar as tarefas, além de ser o responsável;

A atuação da ETIR se dará por ações reativas e proativas;

As ações reativas incluem recebimento de notificações de incidentes, orientação no reparo a danos, e análise de sistemas comprometidos buscando causas, danos e responsáveis;

Estrutura Organizacional

O Gestor de Segurança da Informação será responsável por designar no mínimo 3 (três) integrantes do SGPTI, com a competência de coordenar as atividades de tratamento e resposta a incidentes.

Para cada integrante será indicado e designado o respectivo substituto.

As atividades reativas da ETIR terão prioridade sobre aquelas designadas pelos chefes.

A participação nas atividades da ETIR não enseja remuneração de qualquer espécie, sendo consideradas serviço público relevante.

A execução das atividades de tratamento e resposta a incidentes poderá ser apoiada por colaboradores e prestadores de serviço, desde que supervisionadas por pelo menos um membro da ETIR.

A ETIR terá como competências:

- Coordenar, executar e acompanhar as atividades de tratamento e resposta a incidentes na rede corporativa do HU-UFPI;
- Coordenar, executar e acompanhar a análise dos sistemas comprometidos buscando, causas, danos e responsáveis;
- Coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa do HU-UFPI;
- Coordenar, executar e acompanhar a análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes no HU-UFPI;
- Desenvolver um Plano de Conscientização em segurança da informação e comunicações afim de que todos os servidores no HU-UFPI tenham ciência do assunto;
- Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes da rede corporativa do HU-UFPI;
- Participar da definição e acompanhar os indicadores de incidentes na rede corporativa do HU-UFPI;
- Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicações;
- Participar na proposição de recursos necessários às ações de segurança da informação e comunicações; e
- Executar outras atividades correlatas que lhe forem demandadas.

Tratamento de Incidentes

Serviços Reativos: Tratamento de Incidentes de Segurança em Redes Computacionais; Tratamento de Artefatos Maliciosos; Tratamento de Vulnerabilidades.

Serviços Proativo: Detecção de Intrusão.

Todo e qualquer servidor deve estar ciente que o tratamento de incidentes visa minimizar os impactos de um incidente nos processos em curso no HU-UFPI, sendo

assim voltado à redução e contenção dos efeitos causados por eventos técnicos indesejáveis e seu monitoramento;

Quaisquer falhas, anomalias, ameaças ou vulnerabilidades observadas devem ser notificadas o mais rápido possível através do e-mail: <abuse-hupi@ebserh.gov.br> ;

Cabe a ETIR obter informações quantitativas acerca dos incidentes ocorridos que descrevam: sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes. Tais informações servem como indicadores da eficácia das políticas e da relação custo-benefício dos controles de segurança;

Após o levantamento dos dados do incidente a ETIR deverá tratá-lo e documentá-lo, visando manter um histórico dos incidentes e ainda uma cultura acerca dos mesmos;

Os serviços proativos, reativos e de gerenciamento de qualidade prestados pela ETIR serão detalhados e revisados pelo Gestor de Segurança da Informação.

A ETIR terá autonomia compartilhada, trabalhando em conjunto com outras unidades no processo de tomada de decisão sobre quais medidas devem ser adotadas quanto aos riscos e incidentes identificados.

Em caso de conflito ou divergência entre a ETIR e a outra unidade envolvida no processo de tomada de decisão, a questão será encaminhada ao Gestor de Segurança da Informação que poderá arbitrar perante o conflito.

VIOLAÇÃO DA POLÍTICA E PENALIDADES

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

- Advertência verbal

O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação do HU-UFPI e será recomendado à leitura desta Norma;

- Advertência formal

A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida.

A segunda notificação será encaminhada para a chefia imediata do infrator.

CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas à Governança para avaliação e decisão.

Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Governança, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

Teresina, de 2017.

ANEXO I – TERMO DE COMPROMISSO

NOME:	
CPF:	E-MAIL:
VÍNCULO:	SIAPE/MATRÍCULA:
LOTAÇÃO:	TELEFONE:

Comprometo-me a:

- 1) Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes;
- 2) Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações;
- 3) Não revelar, fora do âmbito profissional, fatos ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico;
- 4) Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico;
- 5) Manter cautela quanto à exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos;
- 6) Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha;

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação de sanções disciplinares cabíveis.

Teresina, _____ de _____ de _____.

Assinatura do Colaborador

**ANEXO II – TERMO DE RESPONSABILIDADE DE USO DE NOTEBOOK
PARTICULAR NA REDE CORPORATIVA**

NOME:	
CPF:	E-MAIL:
VÍNCULO:	SIAPE/MATRÍCULA:
LOTAÇÃO:	TELEFONE:

1. O presente termo objetiva a cessão de acesso à rede corporativa do HU-UFPI ao colaborador acima identificado;
2. O presente instrumento vigorará imediatamente a partir da assinatura deste;
3. O colaborador ficará responsável por:
 - Obedecer às normas vigentes da Política de Segurança da Informação;
 - Toda e qualquer manutenção/despesa que for necessária para o pleno funcionamento do equipamento;
 - Possuir um aplicativo Antivírus devidamente atualizado;
 - Instalar apenas aplicativos com licença de livre distribuição, ou que o mesmo tenha adquirido a sua licença;
 - Não copiar, reproduzir ou distribuir documentos, arquivos, programas ou qualquer informação que forem de direito do HU-UFPI;
 - Todo e qualquer prejuízo que, por sua culpa, na utilização do equipamento, vier causar a terceiros, durante o tempo de vigência deste Termo.

Teresina, ____ de _____ de _____.

Assinatura do Colaborador