

Boletim de Serviço

Nº 36, 08 de setembro de 2015.

**Hospital
Universitário
Cassiano
Antônio Moraes**

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES – EBSERH

HOSPITAL UNIVERSITÁRIO CASSIANO ANTÔNIO MORAES

Av. Marechal Campos, 1355 – Santa Cecília | CEP: 29043-260

Vitória-ES | Telefone: (27) 3335-7100

RENATO JANINE RIBEIRO

Ministro de Estado da Educação

NEWTON LIMA NETO

Presidente

JEANNE LILIANE MARLENE MICHEL

Diretora Vice-Presidente Executiva

CELSO FERNANDO RIBEIRO DE ARAÚJO

Diretor de Atenção à Saúde

GARIBALDI JOSÉ CORDEIRO DE ALBUQUERQUE

Diretor de Administração e Infraestrutura

CRISTIAN DE OLIVEIRA LIMA

Diretor de Controladoria e Finanças

LUIZ ROBERTO MOSELLI

Diretor de Gestão de Pessoas – Substituto

CRISTIANO CABRAL

Diretor de Gestão de Processos e Tecnologia da Informação

LUIZ ALBERTO SOBRAL VIEIRA JUNIOR

Superintendente / Hucam-Ufes

MÁRCIO MARTINS DE SOUZA

Gerente de Atenção à Saúde / Hucam-Ufes

REYNALDO DIETZE

Gerente de Ensino e Pesquisa / Hucam-Ufes

MAROUN SIMÃO PADILHA

Gerente Administrativo / Hucam-Ufes

SUMÁRIO

SUPERINTENDÊNCIA	4
CONSTITUIÇÃO	4
Portaria nº 212 de 14 de agosto de 2015	4
Portaria nº 245 de 01 de setembro de 2015	4
CONCESSÃO	29
Portaria nº 246 de 03 de setembro de 2015	29
GERÊNCIA DE ATENÇÃO À SAÚDE	30
ALTERAÇÃO.....	30
Portaria nº 220 de 24 de agosto de 2015	31
Portaria nº 225 de 24 de agosto de 2015	31
REMANEJAMENTO	32
Portaria nº 241 de 01 de setembro de 2015	32
Portaria nº 243 de 01 de setembro de 2015	33
Portaria nº 244 de 01 de setembro de 2015	33
DESIGNAÇÃO	34
Portaria nº 242 de 01 de setembro de 2015	34
GERÊNCIA ADMINISTRATIVA	34
DESIGNAÇÃO	34
Portaria nº 238 de 01 de setembro de 2015	34
REMANEJAMENTO	34
Portaria nº 239 de 01 de setembro de 2015	35
Portaria nº 240 de 01 de setembro de 2015	35

SUPERINTENDÊNCIA

CONSTITUIÇÃO

Portaria nº 212 de 14 de agosto de 2015

O Constituir a Comissão de Processo de Trabalhos e Referência Técnica do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes – Filial Ebserh, composto pelos representantes das áreas abaixo descritas:

I – Coordenadora:

Prof.^a Léia Damaceno de Aguiar Brotto;

II – Karina Fardin Fiorotti;

III - Laura Pedroza da Silva;

IV – Bianca Silva Oliveira Munaldi;

V – Elisangela Ribeiro Chaves;

VI – Anna Luiza Zandonadi Falchetto Nunes;

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Luiz Alberto Sobral Vieira Junior

Portaria nº 245 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, no uso das atribuições que lhe são conferidas pelo Inciso III, Art. 4º da Portaria nº 125 publicada no Diário Oficial da União de 13 de dezembro de 2013, resolve:

Constituir a Política de Segurança da Informação e Comunicações do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, conforme, anexo:

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Luiz Alberto Sobral Vieira Junior

ANEXO

**Política de Segurança da Informação e Comunicações do
Hospital Universitário Cassiano Antônio Moraes - Hucam-Ufes**



POSIC Versão 1.0

Responsável: Marcelo Marino Mendes Costa

Julho/2015

Histórico de Alterações

Data	Versão	Descrição	Autor
01/07/2015	1.0	Política de Segurança	Marcelo Marino M. Costa

Lista de Aprovadores

Luiz Alberto Sobral Vieira Júnior	
Maroun Simão Padilha	
Márcio Martins de Souza	
Reynaldo Dietze	
Vandré de Castro Tóffoli	

Conteúdo

Glossário.....	5
1. Introdução.....	6
2. Termos e Definições.....	8
3. Objetivos da Política de Segurança e Comunicações.....	10
4. Divulgação e Acesso da Estrutura Normativa.....	11
5. Aprovação e Revisão.....	11
6. Política de Segurança da Estrutura de Informática.....	11
6.1 Política de utilização da rede de dados interna.....	11
6.1.1 Regras Gerais.....	11
6.1.2 Regras para Servidores e Terceirizados.....	12
6.1.3 Regras para Alunos e Estagiários.....	12
6.2 Política do Sistema de Diretórios.....	12
6.3 Política de administração de contas.....	13
6.3.1 Regras Gerais.....	13

6.3.2 Regras para Servidores e Terceirizados.....	13
6.3.3 Regras para Alunos e Estagiários.....	13
6.4 Política de senhas.....	14
6.4.1 Regras Gerais.....	14
6.5 Política de utilização de e-mail.....	14
6.5.1 Regras Gerais.....	14
6.6 Política de acesso à Internet.....	15
6.6.1 Regras Gerais.....	15
6.7 Política de uso das estações de trabalho.....	16
6.7.1 Regras Gerais.....	16
6.8 Política de uso de impressoras.....	17
6.8.1 Regras Gerais.....	17
6.9 Política do uso do serviço de comunicação corporativo.....	17
6.9.1 Regras Gerais.....	17
6.10 Política de uso dos Sistemas de Tecnologia da Informação e Programas de Computador.....	17
6.11 Acesso a rede sem fio.....	18
6.11.1 HUCAM.....	18
6.11.2 HUCAMNET.....	18
6.11.3 PARTNER.....	18
6.12 Política de backup.....	18
7. Política de Segurança Física.....	18
7.1 Política de controle de acesso.....	18
7.1.1 Regras Gerais.....	19
7.2 Política de mesa limpa e tela limpa.....	19
7.2.1 Regras Gerais.....	19
7.3 Política de utilização das salas de Videoconferência.....	19

7.3.1 Regras Gerais.....	19
8. Termo de Compromisso.....	20
9. Verificação da Utilização da Política.....	20
10. Violação da Política, Advertência e Punições.....	20
10.1 Regras para Empregados Públicos.....	21
10.2 Regras para Servidores.....	22
10.3 Regras para terceirizados.....	22

Glossário

ABNT – Associação Brasileira de Normas Técnicas

AGHU – Aplicativo de Gestão para Hospitais Universitários

FTP – File Transfer Protocol - Protocolo padrão da Internet, usado para transferência de arquivos entre computadores

HUCAM – Hospital Universitário Cassiano Antônio Moraes

IMAP – Internet Message Access Protocol - Protocolo de acesso a mensagens eletrônicas.

POSIC – Política de Segurança da Informação e Comunicações

SAME - Serviço de Arquivo Médico e Estatística

SGPTI – Setor de Gestão de Processos e Tecnologia da Informação

SMTP – Simple Mail Transfer Protocol - Protocolo de comunicação usado para troca de mensagens na Internet, via correio eletrônico

SPAM - Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado

TI - Tecnologia da Informação

UFES – Universidade Federal do Espírito Santo

URL - Universal Resource Locator - Endereço de uma página Web, como por exemplo

www.hucam.ebserh.gov.br.

USTI – Unidade de Suporte de Tecnologia da Informação

1. Introdução

A informação é um ativo de grande valor para o Hospital Universitário Cassiano Antônio Moraes, da Universidade Federal do Espírito Santo (Hucam-Ufes). Por conseguinte, deve ser adequadamente utilizada e protegida contra ameaças e riscos.

Sendo assim, a adoção de políticas e procedimentos que visem garantir a segurança da informação devem ser prioridades constantes da instituição, reduzindo os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos do Hucam-Ufes.

A informação pode ser manipulada de diversas formas: por meio de arquivos e mensagens eletrônicas, internet, bancos de dados, meio impresso, verbalmente, em mídias de áudio e de vídeo, etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, são eles:

- 1) Confidencialidade: somente pessoas devidamente autorizadas pela Instituição devem ter acesso à informação;
- 2) Integridade: somente alterações, supressões e adições autorizadas pela Instituição devem ser realizadas nas informações; e
- 3) Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

A proteção da informação não é uma tarefa trivial. Em geral, o sucesso da Política de Segurança da Informação e Comunicações, adotada por uma instituição, depende da combinação de diversos elementos, dentre eles:

- A estrutura organizacional da Instituição;
- As normas e os procedimentos relacionados à segurança da informação; e
- A maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de gestores e colaboradores.

A Política de Segurança da Informação e Comunicações do Hucam-Ufes foi criada para estabelecer regras a serem seguidas pelos usuários dos recursos de informática, de maneira que todos sejam envolvidos e conscientizados da importância da segurança das informações oriundas da Instituição.

Para assegurar um alto padrão de qualidade na prestação dos serviços, fez-se necessária a especificação da POSIC, que visa esclarecer aos usuários a importância da proteção da

informação, tanto ao definir normas e procedimentos para a utilização da rede, quanto da informação que nela trafega.

Todos os usuários dos sistemas ou dos computadores desempenham um papel essencial de apoio efetivo para que a política de segurança possa ser adotada em toda a organização.

Caso os procedimentos ou normas aqui estabelecidos sejam violados, os usuários serão submetidos às penalidades que serão esclarecidas e detalhadas neste documento.

A política de segurança está dividida em:

- Política de segurança da estrutura de informática: contempla políticas, como rede, e-mail, Internet, senhas, entre outras;
- Política de segurança física: aborda o acesso a departamentos, segurança de equipamentos, documentos armazenados fisicamente, entre outros itens.

Dentro de cada uma dessas divisões serão criadas regras gerais, aplicadas a todos. Caso sejam necessárias regras específicas para servidores, alunos ou terceiros serão criadas subdivisões para tais.

A documentação de referência para a elaboração da política de segurança apresentada foi:

- NBR ISO 17799 - código de prática para a gestão da segurança da informação;
- Política de Segurança da Informação e Comunicações (POSIC) – Ufes (Universidade Federal do Espírito Santo);
- Política de Segurança da Informação (PSI) – HUUFMA (Hospital Universitário da Universidade Federal do Maranhão);
- Política de Segurança da Informação (PSI) – HUPAA-Ufal (Hospital Universitário Prof. Alberto Antunes da Universidade Federal de Alagoas);
- Modelo de Política de Segurança, NIC BR Security Office.

2. Termos e Definições

Ativo - qualquer coisa que tenha valor para a organização [ISSO/IEC 13335-1:2004].

Controle - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como um sinônimo para proteção ou contramedida.

Recursos de processamento da informação - qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

Recursos de Tecnologia da Informação e Comunicação - todos os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos setores administrativos e acadêmicos da Hucam-Ufes, tais como: equipamentos de informática de qualquer espécie ou equipamentos de redes e de telecomunicações de qualquer espécie.

Usuários - servidores, prestadores de serviços, estagiários, alunos.

Segurança da Informação - preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Incidente de segurança da informação - um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação [ISSO/IEC TR 18044:2004].

Evento de segurança da informação - ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falta de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Risco - combinação da probabilidade de um evento e de suas consequências [ABNT ISSO/IEC Guia 73:2005]

Política de segurança da Informação e Comunicações - Documentos que oferecem uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Internet - Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

Intranet - Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os servidores possam acessar as informações dos seus respectivos Órgãos Públicos.

Site – Páginas contendo informações, imagens, fotos, vídeos, sons, etc., que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.

Software – Programa de Computador.

Vírus Eletrônico - São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

Download – Baixar um arquivo ou documento de outro computador, através da Internet.

Upload – Envio de um arquivo de seu computador para outro, através da Internet.

Peer-to-Peer (P2P) – É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet.

Administrador – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas.

Correio Eletrônico - Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

Criptografia - Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

Login – Entrada do usuário no sistema.

Logout – Saída do usuário no sistema.

Firewall - É uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo.

3. Objetivos da Política de Segurança e Comunicações

A Política de Segurança da Informação do Hucam-Ufes é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas pela instituição no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

Não obstante, tem por objetivo prestar aos colaboradores, serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional, de forma a evitar falhas de segurança que possam impossibilitar o acesso às informações, sendo que as ações da equipe de TI, no que diz respeito à manutenção de recursos de informática, possam ser justificadas com as regras estabelecidas na política. Para isso, o usuário deve conhecer as regras para utilização da informação de maneira segura, evitando prejudicar o Hospital, os colaboradores ou os alunos.

Por ser a rede do Hucam-Ufes, uma rede interna com conectividade à internet, seu monitoramento, bem como a verificação e a filtragem do conteúdo ajudam a proteger as informações proprietárias, a reduzir a exposição à responsabilidade judicial e a melhorar a produtividade dos aplicativos.

O conteúdo pode ser verificado quanto a informações proprietárias e quanto a palavras ou expressões impróprias para garantir que as normas da política de segurança sejam cumpridas, pode também verificar arquivos com possibilidades de propagação de vírus ou exposição de vulnerabilidade. A filtragem também aumenta a largura de banda ao combater ataques de endereços de e-mail forjados.

Os sistemas de internet e de rede local são propriedade da empresa. Sendo assim, ela pode determinar, legalmente, como e de que forma essa propriedade pode ser usada pelos servidores, terceiros e outros.

4. Divulgação e Acesso da Estrutura Normativa

Esta POSIC deve ser divulgada para todos os colaboradores do Hucam-Ufes e disposta de maneira que seu conteúdo possa ser consultado a qualquer momento.

A Instituição deve certificar-se de que todos os usuários estejam conscientes da importância de cumprir as diretrizes estabelecidas neste documento.

Todos devem estar cientes dos procedimentos de segurança, ter conhecimento da política, se necessário, devem receber treinamentos de como fazer uso correto das informações que nela estão definidas.

5. Aprovação e Revisão

A política deverá ser revisada, no mínimo, anualmente pelo Comitê Gestor de Política da Informação ou pelo Setor de Gestão de Processos e Tecnologia da Informação (SGPTI) do Hucam-Ufes. Entretanto, antes da homologação, a política deve ser revisada e aprovada pelo Conselho Consultivo do Hospital.

6. Política de Segurança da Estrutura de Informática

6.1 Política de utilização da rede de dados interna

Define as normas de utilização da rede interna que abrangem o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

6.1.1 Regras Gerais

- Não serão permitidas tentativas de obter acesso não autorizado, tais como: fraude de autenticação de usuário, fraude de segurança de qualquer equipamento servidor, rede ou conta (também conhecido como “cracking”), acesso aos dados não disponíveis para o usuário,

conectar-se ao equipamento servidor (ou conta) cujo acesso não seja expressamente autorizado para o usuário e colocar à prova a segurança das redes;

- Não serão permitidas tentativas de interferência nos serviços de outro usuário, equipamento servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um equipamento servidor e tentativas de "quebrar" (invadir) um equipamento servidor;
- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, efetuar o logout/logoff ou bloqueio do computador através de senha, evitando o acesso por pessoas não autorizadas;
- Quanto à utilização de equipamentos de informática particulares (notebooks, computadores, impressoras, entre outros) o Hucam-Ufes não fornecerá acessórios, software ou suporte técnico, incluindo assistência para recuperar perda de dados, decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software;
- O acesso a sistemas, como AGHU, deve ser controlado pela identificação do usuário e pelas senhas designadas para usuários autorizados;
- É obrigatório armazenar os arquivos inerentes à instituição no equipamento servidor de arquivos para garantir a cópia de segurança destes;
- Quanto à utilização de equipamentos de informática particulares o colaborador deverá requerer ao seu chefe imediato que solicite ao setor de TI (SGPTI) o uso, apresentando justificativa ao pleito.

6.1.2 Regras para Servidores e Terceirizados

- Quando um servidor ou um terceirizado for transferido entre setores, a chefia que o transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na nova função e informar a equipe de TI qualquer modificação necessária;
- Quando ocorrer a vacância do servidor ou demissão do terceirizado de seu cargo, o chefe responsável deve informar o fato a SGPTI para providenciar a desativação dos acessos do usuário a qualquer recurso da rede. Além disto, o chefe do setor deve alterar todas as senhas de contas de uso coletivo no setor, evitando, assim, o acesso não-autorizado às informações.

6.1.3 Regras para Alunos e Estagiários

- Após o término do vínculo com a instituição, será bloqueado o acesso do aluno ou do estagiário à rede de dados e o conteúdo de suas contas de usuário serão apagados. Portanto o aluno ou o estagiário deve realizar a cópia dos arquivos pessoais antes do final da permanência.

6.2 Política do Sistema de Diretórios

- Materiais de naturezas pornográficas e racistas não podem ser vistos, expostos, armazenados, distribuídos, editados ou gravados nos recursos computacionais do Hucam-Ufes;
- Jogos ou quaisquer tipos de softwares/aplicativos não podem ser gravados ou instalados no computador local e em qualquer outro diretório da rede, restringindo-se apenas àqueles previamente instalados no computador;
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme mostra a Tabela 1:

Tabela 1 – Esquema de armazenamento de arquivos

Compartilhamento Utilização

Diretórios setoriais H: Arquivos do setor em que trabalha

Diretório público T: Arquivos temporários, para todos colaboradores

Diretório Qualidade Q: Arquivos de leitura geral, para todos colaboradores

- A pasta PÚBLICA não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível, devendo ser armazenadas apenas informações comuns a todos, de forma provisória, com objetivo único de transferência de informação entre todos;
- Haverá limpeza semanal dos arquivos armazenados na pasta PÚBLICA, evitando acúmulo desnecessário de arquivos.

6.3 Política de administração de contas

Define as normas de administração das contas que abrange: criação, manutenção e desativação.

6.3.1 Regras Gerais

Desativação da conta:

- À equipe de TI do Hucam-Ufes é reservado o direito de desativar contas de usuário, caso ocorra algum dos critérios abaixo especificados:
 - Incidentes suspeitos de quebra de segurança nas contas dos usuários;
 - Reincidência na quebra de senhas por programas utilizados pela equipe de TI do Hucam-Ufes;
 - Violação das normas de segurança.

6.3.2 Regras para Servidores e Terceirizados

Todo usuário do Hucam-Ufes pode ter uma conta para acesso aos recursos da rede de computadores e acesso a sistemas. Para tanto, a solicitação deve ser feita pelo chefe imediato com apresentação de uma justificativa para a criação da conta do usuário.

- Criação de contas:

- O chefe imediato (onde o servidor/terceirizado está lotado) deve fazer solicitação para criação de conta através de e-mail ou memorando para a Unidade de Suporte de Tecnologia da Informação (USTI) do Hucam-Ufes (usti.hucam@ebserh.gov.br);
- Na solicitação, deve ser informado o número da matrícula, o nome do servidor/terceirizado e o setor ao qual ele pertence, bem como os acessos que serão necessários para este usuário;
- A USTI retornará para o chefe solicitante as informações sobre a conta criada;

- Manutenção da conta.

- As contas serão ser monitoradas pela equipe de TI do Hucam-Ufes com o objetivo de verificar possíveis irregularidades.

6.3.3 Regras para Alunos e Estagiários

O aluno/estagiário poderá ter acesso aos recursos da rede de computadores por meio de usuário e senha.

- Criação de contas:

- A criação da conta do aluno/estagiário se dará através do envio de e-mail ou memorando com o nome, matrícula, início e término da permanência dos alunos/estagiários, pelo setor responsável, a USTI (usti.hucam@ebserh.gov.br);
- A conta do aluno/estagiário será criada pela equipe de TI do Hucam-Ufes com uma senha inicial que deverá ser alterada no momento do primeiro login.

- Manutenção da conta:

As contas serão ser monitoradas pela equipe de TI do Hucam-Ufes com o objetivo de verificar possíveis irregularidades.

6.4 Política de senhas

As senhas são mecanismos de autenticação utilizadas na maioria dos sistemas computacionais. Porém, elas podem ser perigosas, caso o titular escolha-as de forma óbvias e fáceis ou ainda as compartilhe.

6.4.1 Regras Gerais

- Utilize senha com, pelo menos, oito caracteres;

- Inclua, pelo menos, um caractere especial;
- Misture caracteres maiúsculos e minúsculos;
- Misture números, letras e caracteres especiais;
- Utilize um método próprio para lembrar-se da senha, de modo que ela não precise ser escrita em algum local, sob hipótese alguma;
- Utilize senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado;
- Não utilize palavras que estão no dicionário (nacional ou estrangeiros);
- Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc.;
- Não utilize senhas somente com dígitos ou com letras;
- Não anote sua senha em papel ou em outros meios de registro de fácil acesso;
- Não utilize o primeiro nome, o nome do meio ou o sobrenome;
- Não utilize nomes de pessoas próximas, como da esposa (o), dos filhos, de amigos;
- Não utilize senhas com repetição do mesmo dígito ou da mesma letra;
- Não forneça sua senha, por razão alguma;
- A Unidade de Suporte de Tecnologia da Informação pode determinar um tempo de expiração da senha sendo obrigatória a alteração depois do fim do prazo.

6.5 Política de utilização de e-mail

Este tópico visa estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico, no ambiente de Tecnologia da Informação do Hucam-Ufes.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio público que foge do controle da equipe técnica da TI do Hucam-Ufes. As mensagens estão sujeitas a demora de entrega/recebimento e serviços potencialmente não confiáveis.

A maioria da comunicação do dia-a-dia trafega mediante o uso de e-mails. É importante lembrar que, atualmente, grande parte das pragas eletrônicas chegam por esse meio.

Os serviços de e-mail do Hucam-Ufes encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são essenciais. Para isto é importante que algumas regras sejam obedecidas.

6.5.1 Regras Gerais

- Não utilize o e-mail corporativo (@ebserh.gov.br, @ufes.br ou @hucam.edu.br) para fins pessoais;
- É vedada a utilização de e-mails que não estejam em um dos domínios ebserh.gov.br, ufes.br ou hucam.edu.br, para a tramitação de documentos pertinentes à Instituição;
- É obrigatória a utilização de assinatura nos e-mails, seguindo padrão a ser estabelecido pelo Hucam-Ufes;
- O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens;
- O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los. Se for solicitada a interrupção do envio, a solicitação deve ser acatada e o envio não deverá acontecer;
- É proibido o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta não autorizada, como: publicidade, comercial, anúncios e informativos ou propaganda política;
- É proibido reenviar ou, de qualquer forma, propagar mensagens em cadeia independentemente da vontade do destinatário de receber tais mensagens;
- Não é recomendável, o envio de e-mail para mais de 10 (dez) pessoas de uma única vez;
- É proibido o envio de e-mail mal-intencionado, tais como mail bombing ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail;
- Para certificar-se que a mensagem foi recebida pelo destinatário, deve-se, se necessário, utilizar procedimentos de controles extras para verificar a chegada da mensagem. Pode ser solicitada notificações de “recebimento” e “leitura”, por exemplo;
- Não execute ou abra arquivos anexados por remetentes desconhecidos ou suspeitos;
- Não abra arquivos anexados com as extensões, *.bat, *.exe, *.src, *.lnk, se não tiver certeza que solicitou este e-mail;
- Evite anexos muito grandes;
- Não devem ser enviadas, para fora da Instituição, mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito ao Hucam-Ufes.

6.6 Política de acesso à Internet

Este tópico define as normas de utilização da Internet que engloba desde a navegação a sites até downloads e uploads de arquivos.

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos usuários do Hucam-Ufes. Não é permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

6.6.1 Regras Gerais

- O Hucam-Ufes monitora e bloqueia automaticamente sites de pornografia, pedofilia e outros contrários à lei ou a esta política. O acesso a esses sites é terminantemente proibido, mesmo ocorrendo falhas no mecanismo de bloqueio;
- O Hucam-Ufes possui mecanismo de autenticação, que determina a titularidade de todos os acessos à Internet feitos por seus usuários;
- É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;
- Usuários com acesso à Internet não podem efetuar upload de qualquer software licenciado ao Hucam-Ufes ou de dados de propriedade do Hucam-Ufes sem a autorização expressa do Setor de Gestão de Processos e Tecnologia da Informação;
- Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades, desde que observado os termos de licença de uso e registro desses programas;
- A Internet, no âmbito do Hucam-Ufes, é uma concessão e não um direito. Portanto, sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho. Caso o usuário necessite utilizar à INTERNET para atividades não relacionadas com os negócios da organização deverá fazê-lo, fora do horário do expediente;
- Haverá geração de relatórios gerenciais dos acessos por usuários num determinado período. Os chefes poderão, mediante solicitação, ter acesso a essas informações a qualquer tempo;
- O usuário deve utilizar a Internet observando a conformidade com as leis vigentes e a ordem pública;
- O usuário não pode utilizar a Internet com objetivo ou meio para a prática de atos ilícitos, proibidos pelas leis vigentes e pela presente Norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;
- O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso (conta de rede);

- Os usuários que desejarem utilizar outras conexões, além daquelas já estabelecidas, deverão obrigatoriamente informar a Unidade de Suporte da Tecnologia da Informação do Hucam-Ufes;
- A utilização da ferramenta SPARK, para comunicação instantânea, é autorizada;
- É vedado o uso de demais softwares de comunicação instantânea, salvo expressa autorização do SGPTI;
- Não é permitido a utilização de software peer-to-peer (P2P);
- Não é permitido o acesso a sites de relacionamento, como Facebook e afins, salvo expressa autorização do SGPTI;
- Não é permitido acesso ao conteúdo da Internet utilizando Proxy Virtual.

6.7 Política de uso das estações de trabalho

Cada estação de trabalho possui códigos internos que permitem a identificação na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que se ausentar, certifique-se de que tenha efetuado logoff ou bloqueio da estação de trabalho.

6.7.1 Regras Gerais

- Não utilize nenhum tipo de software/hardware sem autorização da equipe técnica;
- Não é permitido gravar, reproduzir e compartilhar nas estações de trabalho MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;
- Mantenha nas estações de trabalho somente o que for indispensável e pessoal;
- Todos os dados relativos ao Hucam-Ufes devem ser mantidos no servidor, onde existe rotina de backup;
- Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários autorizados. Portanto, não se pode garantir sua integridade e disponibilidade, pois poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário que acessar a estação;
- É proibida a abertura do equipamento para qualquer tipo de reparo. Caso seja necessário, será realizado exclusivamente pelo setor técnico na USTI;
- É proibida a transferência física do equipamento para outra área. Caso seja necessário, será realizado exclusivamente pelo setor técnico na USTI.

6.8 Política de uso de impressoras

Define as normas de utilização racional de impressoras em todos os setores do Hucam-Ufes, garantindo os serviços de impressão a toda a comunidade e proporcionando economia na manutenção e aquisição de impressoras e suprimentos (cartuchos e toners). Para tanto, deverão ser utilizados todos os recursos e serviços propiciados pela rede de computadores.

6.8.1 Regras Gerais

- Antes de reenviar documento para impressão, verifique na impressora se o que foi solicitado já está impresso;
- Se a impressão do documento apresentou erro e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve-o para sua mesa. Se o papel não for mais útil a organização, este deverá ser destruído;
- Não é permitido deixar impressões erradas na mesa das impressoras e/ou nas mesas das pessoas próximas a ela;
- Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;
- Utilize a impressora apenas para impressão de trabalhos da instituição;
- Todo e qualquer documento institucional que não possua mais valor para a organização deve ser destruído mediante o uso de fragmentadora/trituradora de papel.

6.9 Política do uso do serviço de comunicação corporativo

Define a política de uso do sistema de comunicação corporativo adotado pela instituição.

6.9.1 Regras Gerais

- As conversações de ofício e aquelas de mero expediente entre setores do Hucam-Ufes serão realizadas, preferencialmente, mediante a utilização do Serviço de comunicação corporativo disponibilizado pela Unidade de Suporte de Tecnologia da Informação;
- Os chefes diligenciarão no sentido de que os clientes de acesso ao Serviço de Comunicação Corporativo dos usuários estejam sempre conectados durante o expediente.

6.10 Política de uso dos Sistemas de Tecnologia da Informação e Programas de Computador

- Os sistemas de tecnologia da informação do Hucam-Ufes são constituídos de programas de computador desenvolvidos pela equipe do SGPTI para uso dos setores, cabendo à USTI o seu controle, desenvolvimento, manutenção e melhoria tecnológica;
- Os setores são responsáveis pela alimentação e atualização das informações que lhes competirem nos sistemas de tecnologia da informação, devendo manter a precisão e a correção dos dados informados;

- Nos casos de alteração ou remoção de informação existente na base de dados, a USTI preservará os dados anteriores, mediante a criação de cópia de segurança para fins de auditoria;
- O Hucam-Ufes utilizará, preferencialmente, Software Livre ou de Código Aberto;
- Fica definido com padrão o sistema operacional Linux, na distribuição CentOS;
- A instalação e a utilização de programas de computador de código proprietário (“software pago” ou de “código proprietário”) no Hucam-Ufes obedecerão aos seguintes requisitos:

I - Existência de licenças de uso pertencentes ao Hospital em quantidade suficiente;

II - Conformidade com as atividades do Hucam-Ufes;

III - Compatibilidade com os demais programas utilizados e adequação aos recursos computacionais disponíveis.

- Os setores poderão submeter pedido de homologação de programa de computador ao Setor de Gestão de Processos e Tecnologia da Informação para uso em suas atividades;

- O SGPTI publicará, na Intranet, a listagem de programas homologados, onde constarão os nomes, as versões, os tipos de licenças de uso e os setores autorizados a utilizá-los.

6.11 Acesso a rede sem fio

O Hucam-Ufes disponibilizará, em áreas onde houver dispositivos de rede sem fio, acesso à internet e a rede local. Este recurso está dividido em 3 (três) redes identificadas pelo seu SSID (Service Set Identifier).

6.11.1 HUCAM

Rede sem fio sem autenticação para acesso público à internet com restrição e filtragem elevadas de conteúdo. Monitoramento constante de seu tráfego.

6.11.2 HUCAMNET

Rede sem fio com autenticação para acesso corporativo e à internet, obedecendo as regras da POSIC. A senha de acesso deve ser solicitada na USTI.

6.11.3 PARTNER

Rede sem fio com autenticação para acesso à internet e a rede local dos terceiros, obedecendo as regras da POSIC. A senha de acesso deve ser solicitada na USTI.

6.12 Política de backup

- Todos os backups devem ser automatizados por sistemas de agendamento para que sejam executados fora do horário comercial;

- As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro e distante do Data Center;
- O tempo de vida e o uso das mídias de backup devem ser monitorados e controlados;
- Testes de restore devem ser executados periodicamente e documentados;

7. Política de Segurança Física

O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da Instituição. A segurança física dos equipamentos de informática e das informações devem ser protegidas de possíveis danos. Será abordada a segurança física dos ambientes de informática, dos equipamentos em geral e procedimentos.

7.1 Política de controle de acesso

Existem áreas que demandam maior atenção quanto ao controle da entrada de pessoas, por conterem informações ou equipamentos a serem protegidos, por exemplo: sala de servidores, superintendência, setor financeiro, setor de documentação, recursos humanos, sala de reuniões, entre outras.

Em instalações desenvolvidas para fins especiais, por exemplo o CDC (Contêiner Data Center), que abrigam equipamentos importantes, serão utilizadas maiores proteções que o nível normalmente oferecido.

7.1.1 Regras Gerais

- Apenas pessoas autorizadas e com crachás podem acessar as instalações;
- Setores que tratem informações confidenciais (SAME, áreas financeira e de pesquisa, etc) terão acesso permitido somente a pessoas autorizadas;
- A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos;
- Em caso de perda de chave, a chefia responsável deve ser informada imediatamente para solicitação de troca da fechadura.

7.2 Política de mesa limpa e tela limpa

A política de mesa limpa deve ser utilizada pelos usuários do Hucam-Ufes, de modo que papéis e mídias removíveis não fiquem expostos.

A política de tela limpa considera que, caso o usuário não esteja utilizando a informação ela não deve ficar exposta, de modo a reduzir o risco de acesso não autorizado, perda e danos à informação.

7.2.1 Regras Gerais

- Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados. Devem ser guardados de maneira adequada, preferencialmente em gavetas ou armários trancados;
- O ambiente dos setores deve ser mantido limpo, sem caixa ou qualquer outro material sobre o chão de modo a facilitar o acesso de pessoas que estejam no setor;
- Caso não esteja utilizando o computador não deixe nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas;
- Agendas, livros ou quaisquer materiais que contenham informações sobre a instituição, que não sejam de domínio público, devem ser guardados em locais fechados, evitando o acesso;
- Chaves de gavetas, de armários, de portas de acesso, devem ser guardadas em lugares adequados.

7.3 Política de utilização das salas de Videoconferência

Para utilização das salas de videoconferência e equipamentos de informática, algumas regras devem ser cumpridas para que possa ser feito o uso correto das instalações evitando danos aos equipamentos.

7.3.1 Regras Gerais

- O acesso às salas de videoconferência será controlado, somente sendo permitido o uso das mesmas com um técnico responsável;
- É de responsabilidade do professor/servidor ao utilizar a sala, zelar pela ordem das instalações. Sendo necessário qualquer tipo de manutenção a equipe técnica deverá ser informada;
- Os equipamentos devem ser trancados e guardados em segurança quando deixados sem supervisão;
- Nenhum equipamento pode ser conectado aos sistemas ou rede sem aprovação prévia e, se necessário, sob supervisão;
- As chaves de acesso as salas devem ficar guardadas em locais que o acesso seja controlado e não seja permitida a entrada de pessoas não autorizadas;
- A reserva para utilização das salas deverá ser feita por telefone (ramal da USTI) ou Intranet (intranet.hucam).

8. Termo de Compromisso

O termo de compromisso é utilizado para que os servidores, alunos e estagiários se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento.

No termo de compromisso, Anexo I, são reforçados os principais pontos da política de segurança e comunicações. O mesmo deve ser assinado por todos os usuários e renovado sempre que necessário.

9. Verificação da Utilização da Política

Para garantir as regras mencionadas acima o Hucam-Ufes se reserva o direito de:

- Implantar softwares e sistemas para monitorar e gravar o histórico de utilização do acesso à Internet através da rede e das estações de trabalho da Instituição;
- Inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas pastas compartilhadas, visando assegurar o rígido cumprimento desta política;
- Monitorar a rede interna e garantir a integridade dos dados e programas, implantando firewall como primeira, mas não a única barreira entre a rede interna e a Internet;
- Incluir a divulgação da POSIC como parte do programa de integração de novos servidores, terceirizados, estagiários, bem como do programa de integração de novos alunos (ao início de cada ano letivo);
- Realizar treinamentos de reciclagem para os servidores e terceirizados mais antigos.

10. Violação da Política, Advertência e Punições

Ações que violem a POSIC ou que quebrem os controles de segurança da informação e comunicações são passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isolada ou cumulativamente.

Os empregados públicos estão sujeitos as sanções previstas na CLT. Os servidores públicos civis da União, estão sujeitos a Lei no 8.112/1990. Para o caso de servidores de empresas terceirizadas, deve estar previsto no contrato o afastamento dos servidores envolvidos, sem prejuízo de outras sanções legais.

No caso de alunos, resoluções específicas devem ser aprovadas para que membros do corpo discente sofram punições em caso de violação das normas de segurança de informação. As

penalidades devem variar de advertência ao desligamento da Universidade, sem prejuízo de outras sanções legais.

Ao recebimento de denúncia ou a detecção da violação da POSIC, as ações a serem seguidas são:

I- Diagnosticar o motivo da violação:

- a. Negligência;
- b. Acidente;
- c. Erro;
- d. Desconhecimento da política; e
- e. Intencional

II- Determinar as circunstâncias da violação;

III- Bloqueio do acesso ou o cancelamento da conta do usuário

As penalidades devem ser gradativas e de acordo com a ação:

- Uso indevido;
- Disseminação de material proprietário;
- Uso de material não adequadamente licenciado;
- Produção e disseminação de material obsceno, racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva;
- Quebra de sigilo;
- Alteração de informações (falsidade ideológica).

Em todos os casos aplica-se o previsto no Código Penal e no Código Civil, bem como as normas e resoluções internas do Hucam-Ufes.

As penalidades listadas abaixo serão aplicadas de acordo com o Regime Jurídico de cada colaborador, a saber:

- I. advertência;
- II. suspensão;
- III. demissão;
- IV. cassação de aposentadoria ou disponibilidade;
- V. destituição de cargo em comissão;

VI. destituição de função comissionada.

10.1 Regras para Empregados Públicos

- Caso seja necessário advertir o empregado público, será informada a Divisão de Gestão de Pessoas para providências de competência da Divisão;
- O não cumprimento, pelo empregado público, das normas estabelecidas neste documento seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, a abertura de sindicância, ou aplicações de punições como Comunicação de descumprimento, Advertência ou suspensão, Demissão por justa causa conforme itens previstos na CLT;
- Comunicação de descumprimento: Será encaminhado ao empregado público, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a Divisão de Gestão de Pessoas na respectiva pasta do empregado;
- Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade;
- Demissão por justa causa nas hipóteses previstas no artigo 482 da Consolidação das Leis do trabalho, conforme Anexo II.

10.2 Regras para Servidores

- Caso seja necessário advertir o empregado público, será informada a Divisão de Gestão de Pessoas para providências de competência da Divisão;
- O não cumprimento, pelo servidor, das normas estabelecidas neste documento seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, a abertura de sindicância, ou aplicações de punições como Comunicação de descumprimento, Advertência ou suspensão, Demissão por justa causa conforme itens previstos na Lei 8.112/90;
- Comunicação de descumprimento: Será encaminhado ao servidor, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a Divisão de Gestão de Pessoas na respectiva pasta do servidor;
- Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade;
- Demissão por justa causa nas hipóteses previstas na Lei 8112/90.

10.3 Regras para terceirizados

- Caso seja necessário advertir o terceirizado, será informado gestor do contrato para adotar as medidas contratuais cabíveis.

ANEXO I – TERMO INDIVIDUAL DE RESPONSABILIDADE

Pelo presente instrumento, eu, _____, matrícula/identidade nº _____, perante o Hucam-Ufes, na qualidade de usuário dos recursos de processamento da informação do Hucam-Ufes, declaro estar ciente e concordar com a Política de Segurança da Informação e Comunicações composta por suas Diretrizes Gerais, Normas, Procedimentos e Instruções.

Declaro, também, estar ciente de que os acessos por mim realizados à internet, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico corporativo são monitorados automaticamente.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas normas da Política de Segurança da Informação e Comunicações e que, a não observância desses preceitos, implicará na aplicação das sanções previstas nesta Política.

Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança da Informação e Comunicações e com as Normas e Padrões vigentes.

Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.

Não revelar fora do âmbito profissional, fato ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico.

Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.

Manter cautela quando a exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos.

Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.

Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha, através dos quais posso efetuar operações a mim designadas nos recursos computacionais que acesso, procedendo a:

- a. Substituir a senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível;
- b. Não divulgar a minha senha a outras pessoas;

- c. Nunca escrever a minha senha, sempre memorizá-la;
- d. De maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outras pessoas;
- e. Somente utilizar o meu acesso para os fins designados e para os quais estiver devidamente autorizado, em razão de minhas funções;
- f. 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 da minha senha ou das transações a que tenho acesso;
- g. Reportar imediatamente ao superior imediato ou ao Setor de Gestão de Processos e Tecnologia da Informação em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.
- h. Solicitar o cancelamento de minha senha quando não for mais de minha utilização.
- i. Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação dos sanções disciplinares cabíveis.

Vitória, _____ de _____ de _____.

Nome:

Matrícula:

ANEXO II – ARTIGO 482 da CLT

Art. 482 – Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

- a) ato de improbidade;
- b) incontinência de conduta ou mau procedimento;
- c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço;
- d) condenação criminal do empregado, passada em julgado, caso não tenha havido suspensão da execução da pena;
- e) desídia no desempenho das respectivas funções;
- f) embriaguez habitual ou em serviço;
- g) violação de segredo da empresa;

h) ato de indisciplina ou de insubordinação;

i) abandono de emprego;

j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas, nas mesmas condições, salvo em caso de legítima defesa, própria ou de outrem;

k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem;

l) prática constante de jogos de azar.

Parágrafo único. Constitui igualmente justa causa para dispensa de empregado a prática, devidamente comprovada em inquérito administrativo, de atos atentatórios contra a segurança nacional.

** Parágrafo único acrescentado pelo Decreto-lei nº 3, de 27 de janeiro de 1966.

Luiz Alberto Sobral Vieira Junior

CONCESSÃO

Portaria nº 246 de 03 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando as diretrizes estabelecidas pelo Grupo de Trabalho da sede e aprovadas pelo Colegiado Executivo da EBSEH que serviram de orientação para a revisão do LTCAT dos Hospitais Federais;

Considerando a aprovação do Colegiado Executivo do Hospital Universitário Cassiano Antônio Moraes- Filial EBSEH, referente aos percentuais estabelecidos no Laudo Técnico de Condições do Ambiente de Trabalho - LTCAT revisados em 2015, considerando o que consta no processo nº 23068.305464/2015-22 onde foi revisado o laudo técnico pela equipe do SOST resolve:

Art.1º Conceder aos empregados celetistas da EBSEH-Filial HUCAM, abaixo relacionados lotados na Unidade Materno Infantil (posto de trabalho–Centro Obstétrico) e Unidade de Atenção à Saúde da Mulher (posto de trabalho – Centro Obstétrico), após revisão do Laudo Técnico de Condições do Ambiente de Trabalho- LTCAT, o adicional de insalubridade no percentual de 40% (quarenta por cento–grau máximo).

Nome	Cargo	Admissão	SIAPE
Unidade Materno Infantil (posto de trabalho – Centro Obstétrico)			
Grazelia Barreto Silva	Enfermeira	04/08/2014	1131233

Maximiniana A. dos Reis Fonseca	Enfermeira	04/04/2015	2213092
Marcia F.F. de Almeida	Técnica em Enfermagem	04/08/2015	2148927
Patricia Paulino Bianchini	Técnica em Enfermagem	12/05/2014	1464232
Geisa Silva Trancoso	Técnica em Enfermagem	12/05/2015	2121310
Mirian de Melo Rozario	Técnica em Enfermagem	04/08/2014	2148935
Elediane Garbeloto Tricano	Médico- Ginecologia e Obstetrícia	12/05/2014	2121248
Anna Carolina Machado Dettino	Médico- Ginecologia e obstetrícia	01/10/2014	1519892
Juliana José Fernandes	Médico- Ginecologia e obstétrica	04/08/2014	1757676
Aline Forattine Garcia	Médico- Ginecologia e obstetrícia	01/10/2014	2137239
Emanuele de Angeli Endrinder	Médico- Ginecologia e obstetrícia	03/03/2015	18400064
Fabiana Patrão	Médico- Ginecologia e obstetrícia	07/07/2015	2237614
Ana Rachel Farranha Santana Daltron	Médico- Ginecologia e obstetrícia	03/03/2015	2203855
Unidade de Atenção à Saúde da Mulher (posto de trabalho – Centro Obstétrico)			
Janine Martins Machado	Mastologia	12/05/2014	1348541
Carolina L.P Ferruchi	Médico- Ginecologia e obstetrícia	03/11/2014	3602131
Layza Merizio Borges	Médico- Endoscopia Ginecológica	03/02/2015	2188026

Art.2º Determinar a Divisão de Gestão de Pessoas providência relativa ao pagamento do adicional de insalubridade as empregadas.

Art.3º Esta portaria entra em vigor na data de sua assinatura.

Luiz Alberto Sobral Vieira Junior

GERÊNCIA DE ATENÇÃO À SAÚDE

ALTERAÇÃO

Portaria nº 220 de 24 de agosto de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, no uso das atribuições que lhe são conferidas pelo Inciso III, Art. 4º da Portaria nº 125 publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando as designações constantes da Portaria nº 155/2015 de 23 de junho de 2013, resolve:

Art.1º Alterar os membros do Colegiado Gestor Unidade de Cirurgia RPA e CME do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes – Filial Ebserh, composto pelos representantes das áreas abaixo descritas:

I – Coordenadora (provisória):

Lais Rubert Machado – Enfermeira Especialista - Responsável Técnica Centro Cirúrgico;

II - Dr. Fernando Antonio Martins Bermudes – Chefe do Setor de Apoio Terapêutico;

III – Lidice Peruch Fundão – Enfermeira;

IV – Dr. José Carlos Binda – Anestesiologista - APSA;

V – Dr. Carlos Eduardo B. e Almeida – Anestesiologista - EBSEH;

VI– Secretário (provisório):

Marcelo Costa Vicente – Enfermeiro Especialista - Centro - Cirúrgico Matutino;

VII – Regina Maria Nazareth – Enfermeira Assistencial – Centro Cirúrgico Vespertino;

VIII – Marcela Sizenando Soares de Oliveira – Enfermeira – Centro Cirúrgico - UFES;

IX – Raquel Silva Paiva – Enfermeira Assistencial – Centro Cirúrgico - Oftalmologia;

X – Thiago Costa Freitas – Tec. de Enfermagem – Centro Cirúrgico Matutino;

XI – Ester Laureano Oliveira – Téc. de Enfermagem Vespertino;

XII – Fausto Onofre Umar – Téc. de Enfermagem – Centro Cirúrgico – UFES;

XIII – Liliane Karine Santos – Instrumentadora - Centro Cirúrgico – UFES;

XIV – Cidnéia Maria Murelli Stein – Téc. de Enfermagem – CME;

XV– Christiane Rodrigues – Farmacêutica – Farmácia Satélite;

XVI – Fernanda Souza Paranhos – Recepcionista – Almoarifado Satélite;

XVII – Carlos Alberto Simões da Silva – Recepcionista – Central de Remoção Intra Hospitalar;

XVIII – Jildevan Rodrigues Mota - Recepcionista – Central de Remoção Intra Hospitalar;

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Marcio Martins de Souza

Superintendente em Exercício Hucam/Ebserh

Portaria nº 225 de 24 de agosto de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, no uso das atribuições que lhe são conferidas pelo Inciso III, Art. 4º da Portaria nº 125 publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando as designações constantes da Portaria nº 163/2015 de 30 de junho de 2015. Resolve:

Art.1º Alterar os membros do Colegiado Gestor Unidade da Unidade de Oncologia/Hematologia do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes – Filial Ebserh, composto pelos representantes das áreas abaixo descritas:

I – Coordenador:

Dr. Guilherme Santos Crespo;

II – Dr. Alex Bruno de Carvalho Leite;

III –Dr.^a Aurenívea Cuerci Cazzotto;

IV –Dr. Marcos Pretti Araújo;

V –Dr.^a Prisces Amélia S. Bitencourt Amorim Matos;

VI–Dr. Renato Pretti;

VII - Dr. Volmar Belisario Filho;

VIII- Secretária:

Maria Adelaide Costalonga Monjardim - Enfermeira;

IX – Ivy Alcoforado Felisberto - Farmacêutica;

X – Dedalmira Ferreira Ramos – Téc. de Enfermagem;

XI – Maria Helena da Silva Santos – Assistente Social;

XII – Queila Cássia Corrêa Guimarães – Psicóloga;

XIII – Ravena Santos Raulino – Fisioterapeuta.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Marcio Martins de Souza

Superintendente em Exercício Hucam/Ebserh

REMANEJAMENTO

Portaria nº 241 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação constante no Formulário de Solicitação de Remanejamento, de 21 de agosto de 2015, resolve:

Art. 1º Remanejar a enfermeira terapia intensiva pediátrica **Andreia Braga de Souza Ribeiro**, empregada celetista, matrícula Siape nº 2203869, da Unidade de Atenção à Saúde da Criança e Adolescente, da Divisão de Gestão do Cuidado, para a Unidade de Terapia Intensiva e Semi Intensiva Pediátrica e Neonatal, do Setor de Apoio Terapêutico, da Divisão de Apoio Diagnóstico e Terapêutico, ambas da Gerência de Atenção à Saúde do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, a partir de 21 de agosto de 2015.

Luiz Alberto Sobral Vieira Junior

Portaria nº 243 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação constante no Formulário de Solicitação de Remanejamento, de 31 de agosto de 2015, resolve:

Art. 1º Remanejar o enfermeiro assistencial **Tiago Santos da Silva**, empregado celetista, matrícula Siape nº 2148781, da Unidade do Sistema Cardiovascular, da Divisão de Gestão do Cuidado, para o Setor de Urgência e Emergência, da Divisão de Gestão do Cuidado, ambas da Gerência de Atenção à Saúde do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, a partir de 05 de setembro de 2015.

Luiz Alberto Sobral Vieira Junior

Portaria nº 244 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação constante no Formulário de Solicitação de Remanejamento, de 31 de agosto de 2015, resolve:

Art. 1º Remanejar a técnica enfermagem **Mônica dos Santos Pimentel**, empregada celetista, matrícula Siape nº 2237662, da Unidade do Sistema Urinário, da Divisão de Gestão do Cuidado, para a Unidade de Terapia Intensiva e Semi Intensiva Pediátrica e Neonatal, do Setor de Apoio Terapêutico, da Divisão de Apoio Diagnóstico e Terapêutico, ambas da Gerência de Atenção à Saúde do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, a partir de 31 de agosto de 2015.

Luiz Alberto Sobral Vieira Junior

DESIGNAÇÃO

Portaria nº 242 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação contida no Memo nº 77/2015 – UASCA/Ebserh, de 25 de agosto de 2015, resolve:

Art. 1º Designar a chefe da Divisão Médica **Aparecida das Graças Carvalho Gomes**, matrícula Siape 654676, para responder pela Chefia da Unidade de Atenção a Saúde da Criança e Adolescente, da Divisão de Gestão do Cuidado, da Gerência de Atenção a Saúde do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, no período de 09/09/2015 a 23/09/15, em decorrência das férias da chefe titular **Rita Elizabeth Checon de Freitas Silva**, matrícula Siape nº 298169.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Luiz Alberto Sobral Vieira Junior

GERÊNCIA ADMINISTRATIVA

DESIGNAÇÃO

Portaria nº 238 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação contida no Memo nº 003/2015 – UPD/Hucam/Ebserh, de 27 de agosto de 2015, resolve:

Art. 1º Designar o assistente administrativo **Luiz Carlos Pereira de Assis**, matrícula Siape 2166327, para responder pela Unidade de Pagamento da Despesa, do Setor de Orçamento e Finanças, da Divisão Administrativa Financeira, da Gerência Administrativa do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, no período de 09/09/15 a 18/09/15, em decorrência das férias do chefe titular **Israel Thompson Rufino**, matrícula Siape nº 295911.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Luiz Alberto Sobral Vieira Junior

REMANEJAMENTO

Portaria nº 239 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação constante no Formulário de Solicitação de Remanejamento, de 24 de agosto de 2015, resolve:

Art. 1º Remanejar o analista administrativo administração **Leonardo Ferreira Viana**, empregado celetista, matrícula Siape nº 2213075, do Setor de Administração, da Divisão Administrativa Financeira, para a Unidade de Contratos, do Setor de Administração, da Divisão Administrativa Financeira, ambas da Gerência Administrativa do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, a partir de 01 de setembro de 2015.

Luiz Alberto Sobral Vieira Junior

Portaria nº 240 de 01 de setembro de 2015

O Superintendente do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, filial da Ebserh, no uso das atribuições que lhe são conferidas pelo Inciso III do Art. 4º da Portaria nº 125, publicada no Diário Oficial da União de 13 de dezembro de 2013, considerando a solicitação constante no Formulário de Solicitação de Remanejamento, de 24 de agosto de 2015, resolve:

Art. 1º Remanejar a assistente administrativa **Aline Alves Silva Pandolfi**, empregada celetista, matrícula Siape nº 2172824, do Setor de Hotelaria Hospitalar, da Divisão de Logística e Infraestrutura Hospitalar, para a Unidade de Contratos, do Setor de Administração, da Divisão Administrativa Financeira, ambas da Gerência Administrativa do Hospital Universitário Cassiano Antônio Moraes – Hucam-Ufes, a partir de 01 de setembro de 2015.

Luiz Alberto Sobral Vieira Junior